Evaluating Access Controls Over Data

Logical access controls have become a vital part of IT audit, both in IT reviews by internal auditors and by external auditors in the IT audit portion of a financial attest engagement. This focus is rational given the inherent risk associated with logical access controls to applications, data and systems in general.

This article offers some basic guidance to IT auditors in evaluating the access controls over relevant data files. In doing so, management may be able to gather ideas on how to better secure not only accounting data, but other data assets as well.

ACCESS METHODS TO DATA

The obvious method of access to data is via the applications that create, edit, maintain and report data; however, there are other methods through which one can get to data. They include the network operating system (NOS), primary server, database (and database administrator [DBA]) and operating system (OS). Each of these data-related components has its own risk and its own role in securing data.

Generally speaking, access to data is available through the “front door” and the “back door.” “Front door” refers to access via legitimate applications and their functionality. That is, through normal activities of the application, users are able to gain access to data from many of the programs.

“Back door” refers to a different kind of access. Certain staff members or positions in IT, and possibly other functional areas, have the ability to access raw data by going around the application and accessing data files directly with some tool other than the application. These positions can include system administrator, server administrator, network administrator, DBA and OS administrator (some of these will likely overlap in small and medium-sized enterprises [SMEs]). These positions are at risk because they are able to gain unauthorized access rather easily, without adequate controls.

In addition, there is likely to be at least one person who has “keys to the kingdom.” When the previously mentioned positions overlap and a single person performs all of those functions, when access rights are read-write (RW) universally, or when “root” access rights to servers are granted, that person has keys to the kingdom and is a high risk in terms of data security.

DATA STATES

Conventional wisdom identifies data as being in one of three states of being: at rest, in transit or in process. “At rest” refers to data storage when data are simply located on a storage device with no current activity related to those data. “In transit” refers to data that are being transmitted across some communication lines, such as the data’s own network or the Internet. “In process” refers to data that are being created, modified or otherwise managed via applications. Each of the states is affected by one or more methods (figure 1).

<table>
<thead>
<tr>
<th>Method</th>
<th>At Rest</th>
<th>In Transit</th>
<th>In Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Network/NOS</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Database Management System (DBMS)</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>DBA</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

One common control for data at rest or in transit is encryption. For instance, for credit card data that are stored on a server connected to the Internet, the data file should be encrypted in all states. Protocols and secured connectivity are also important for data in transit, especially over the Internet. Tools such as Secure Sockets Layer and virtual private networks provide mitigating controls for the security of data in transit.
Data that are in process need controls in the application to help protect their integrity. The perimeter, NOS, server, OS and DBMS all provide means to increase or decrease the risk associated with data security. The following discussion provides some procedures to assess the level of risk for a particular entity at a particular time.

IT AUDIT IMPLICATIONS FOR DATA SECURITY
The IT auditor needs to assess the risk associated with each of the venues as it relates to the particular audit objectives. In order to properly audit the security of data, IT auditors will need to consider people, processes, IT, control—including access controls—and the state of the data. Therefore, assuming the constraint of access controls, the following sections present an illustrative description of the types of procedures the IT auditor should consider.

General Rules for Access Control/Passwords
Logical access controls related to login credentials, and especially passwords, overlap several of the components and methods related to data security. Therefore, the password principles that follow are used repeatedly in the procedures described in further sections. Passwords are considered more reliable if they follow these guidelines.

The first guideline relates to the ease of guessing or hacking passwords based on their length. The shorter the length of a password, the easier the password is to guess and the less time it takes for a hacker to crack a password with hacker tools. The general consensus is that a password should have a minimum of eight characters in order to be protected from being cracked and to protect unauthorized access to data assets.

The second guideline is a related one—the strength of the password. “Strength” means the complexity of the characters used to create a password; passwords should not be words in the dictionary, easy-to-guess names or only lowercase letters of the alphabet. To increase the strength of the password, a mix of lowercase letters, uppercase letters, numbers (at least one) and special characters (at least one) introduce a sufficient level of complexity to cause that password to become fairly difficult to guess or hack.

The third guideline aims to prevent unauthorized access via “piggy-backing,” in which an authorized user walks away from a workstation without logging off and a fellow employee uses that system to conduct unauthorized activities. Because the authorized user is logged on, the coworker is able to gain unauthorized access to the system and potentially some access to the underlying data in the DBMS. To prevent this kind of unauthorized access, reliable systems provide for automatic logoff of sensitive accounts after some amount of time of inactivity by the user (also referred to as a “timeout”). The IT auditor should verify that an auto logout is in place for users who have access to sensitive data.

The fourth guideline deals with the response of the access control system to a failed login attempt. That is, when someone inputs login credentials that are incorrect, how does the system respond to that attempt? Best principles designate that the system should lock out the account after three successive failed attempts—the assumption being that there may be a malicious attempt to hack or guess the password.

The fifth guideline is associated with the duration of lockouts. Systems usually allow a system administrator to set the length of time before allowing anyone another attempt to log in once a user has been locked out. That should be something other than zero; 60–90 minutes will probably successfully frustrate hacker attempts. It could also be indefinite for more sensitive accounts/access, forcing a user who forgets login credentials to reestablish credentials.

The sixth access control principle involves terminated employees. For whatever reason, many entities fail to remove the login credentials of terminated employees. There should be sound policies and procedures to ensure that the credentials of terminated employees are removed in a timely manner.

Enjoying this article?

- Read IS Auditing Guideline G38 Access Controls. www.isaca.org/guidelines
- Read Identity Management Audit/Assurance Program. www.isaca.org/research-deliverables
- Learn more about, discuss and collaborate on access controls, application controls and OS/400 in the Knowledge Center. www.isaca.org/knowledgecenter
The share function allows folders and files to be shared with previously apply to the server.

The password principles outlined the server and NOS have multiple risk factors related to data rights from Active Directory in Microsoft SQL Server). The application may inherit user access rights from the network. That is, applications that are RW give the user access to the underlying data, those applications should be restricted to users who need the ability to read and write. Put another way, no all users should have access to all applications, especially those with RW capability. Some applications provide their own access controls. The IT auditor needs to gain an understanding of the application and whether it has its own access controls and, if so, if they are independent of or subservient to the network. That is, the application may inherit user access rights from the network (e.g., Microsoft Dynamics can inherit users, groups and access rights from Active Directory in Microsoft SQL Server). The objective is to restrict access to those applications, regardless of how the application assigns the access rights.

Applications
The procedures for applications involve logical access controls. Because the applications that are RW give the user access to the underlying data, those applications should be restricted to users who need the ability to read and write. Put another way, not all users should have access to all applications, especially those with RW capability. Some applications provide their own access controls. The IT auditor needs to gain an understanding of the application and whether it has its own access controls and, if so, if they are independent of or subservient to the network. That is, the application may inherit user access rights from the network (e.g., Microsoft Dynamics can inherit users, groups and access rights from Active Directory in Microsoft SQL Server). The objective is to restrict access to those applications, regardless of how the application assigns the access rights.

Server and NOS
The server and NOS have multiple risk factors related to data security. First, there are access rights that are established for users and administrators. The password principles outlined previously apply to the server.

In addition to logical security, “shares” should be examined. The share function allows folders and files to be shared with various users or groups. The key is to prohibit the sharing of critical data except to a few authorized users or one group. For instance, if a spreadsheet is used in the financial reporting process (which is often the case), that file should not be shared with users other than the person authorized to use it, the person authorized to review it, etc. In fact, restricting the file/folder is one way to mitigate the risk associated with using a spreadsheet.

In general, shared permissions for data access should be used sparingly and judiciously.

The next risk is that of the users who have access to the server. Those users and groups should be established in such a way as to minimize access rights, using restricted rights for each user and each group. One good policy is to establish group rights and then add users to the appropriate group, limiting the number of individual users who have specific access rights—usually unique rights. Thus, the IT auditor should review the access rights file to see who has access and what kind of access. Usually, the OS will provide a tool to view that information. Terminated employees should be tested as well.

Sometimes, the server vendor will ask for access to the server to maintain, debug and solve problems that occur. These accounts must be guarded carefully. Auditors should ensure that any access is read-only (RO) and should even consider setting up a temporary vendor account when needed, which can be removed or disabled until it is needed again.

Servers come with default settings for users and groups, and sometimes, those accounts are not established in a secure manner. For instance, sometimes, access is granted to “everyone.” Sometimes, the administrator credentials are “admin” (username) and “admin” (password) and, thus, easy to guess. Likewise, the database system administrator default is sometimes “sa” and “sa,” which is also easy to guess. Therefore, at first use, any default accounts should be examined and changes made where appropriate. The IT auditor should look for these default accounts to ensure that they have been “sanitized.”

The IT auditor should test the process of adding, removing and modifying users and groups in regard to access rights. For instance, the add process should be tested to see whether it picks up the password policies correctly. The removing process should be tested to ensure that access is truly removed. The IT auditor should gather evidence of any breach, violation or abuse of password policies and procedures—and internal password policy settings/configuration. Any intrusions from outside of the system should also be determined and evaluated.
Firewalls
Firewalls can allow or disallow access to external users, and can lead to unauthorized access to data. Therefore, the firewall should be tested for appropriate access controls for users who enter the system externally.

Here, too, the default settings from the manufacturer can be troublesome. The default setting for access should be to deny the credentials “any” and “any,” which forces the system to verify each external user against some access rights established for users and groups.

Change controls and updates/patches are risk factors that can lead to data being susceptible to misuse, theft or unauthorized access. Therefore, the IT auditor should test change controls and update/patch controls to ensure that the firewall is being properly managed to mitigate the risk of unauthorized access. SoD applies in the same way here as it does for passwords.

OS and Network Administrators
OS and network administrators, by the nature of their functions, have back-door access to data. Thus, when IT auditors examine password policies and review users and groups, the IT auditors should see a limited number of people with OS or network server administrator rights. That is, a firm with 10 staff members in the IT department does not need all 10 to have OS administrator, server administrator or network administrator rights. In SMEs, two or three people are probably sufficient to manage and perform the administrator functions. Thus, the IT auditor should see a reasonably limited number of administrators. Also, the rights granted need to be least-privilege access.3

DBA
In the same manner as administrators, the DBA has an unusual amount of risk related to the data. Unlike OS, server and network administrators, the DBA knows more about the data, data structures and data files than anyone else in the entity. Therefore, the DBA is not only able to access data via the back door, he/she can also conduct any number of malicious or deleterious activities related to the data and potentially hide that unauthorized activity for a long time—after all, this person is the oversight and manager of the DBMS.

Also in the same manner as administrators, the DBA should have rights assigned at the least-privilege level. The DBA should also be segregated from all other IT- and data-related functions. On the organizational chart, the DBA should appear similar to an island, with no connection to other functions and no oversight of the people who do them. Also in the same manner as administrators, there should be a reasonably limited number of DBAs. Obviously, the more DBMSs that exist, the more DBAs are needed, but for any one DBMS, the number should be limited to just a few.

In addition, the DBMS often comes with default users, and sometimes, the access granted to these accounts is too broad or risky. The IT auditor should look for those accounts and ensure that they have been changed or removed, if necessary, for data security.

SAMPLE IT AUDIT PROCEDURES FOR DATA SECURITY
The previously mentioned guidelines provide a benchmark for the procedures and for evaluation of evidence in IT audit procedures that are related to passwords and access control. The venues and possible procedures and IT audit objectives are compiled in figure 2.

CONCLUSION
Data security has become a vital need for almost all entities due to the expansion of data stored, technical standards and increased malicious activities. There are some basic principles for auditing data security, including auditing password policy, administrative rights and other aspects of logical access. While logical access is not the only IT audit procedure for data security, it is generally considered a key one, and a basic one applied to audits and reviews of all types. This article provides some basic IT audit procedures for security over data, including logical access over the front door (e.g., applications) and the back door (e.g., DBAs, administrators), and access to the database in general.

ACKNOWLEDGEMENT
A special thanks to my colleague at Carr Riggs & Ingram, David Mills, for his invaluable input into this article and for his encouragement.
ENDNOTES

1 One such tool is DumpSec, which can gather password access rights and policies and “dump” them to a printout or screen. See SystemTools.com, SomarSoft Utilities, www.systemtools.com/somarsoft/?somarsoft.com. Another tool is Netwrix, which can examine lockouts, password configurations/settings, changes to passwords and more. It works on a number of servers such as Active Directory, SQL Server and Microsoft Exchange. See Netwrix Corp., USA, 2011, www.netwrix.com.

2 The exact default accounts depend on the server, but usually the IT auditor should be able to determine the pertinent information by doing a web search for the server manufacturer and model and “default accounts.”

3 US Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, USA, 1985, affectionately known as the “orange book,” is a commonly accepted standard for computer and data security. It defines “least privilege” as “a principle that requires each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks.”