IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12578

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

A Risk-Based Approach to Auditing Relational Databases

Wendy S. Walker, Miami University, 12221 Madison Avenue, Urbandale, IA 50323 , 515-314-1517, Walkerws@muohio.edu

Jeffrey W. Merhout, PhD, Miami University, 311 Upham Hall, Oxford, Ohio 45056, USA, 513.529.8340, merhoujw@muohio.edu

ABSTRACT

With the increased focus on risks and controls since the passing of the Sarbanes-Oxley Act in the U.S., security has been an increasingly hot topic among IT professionals. As a result, risk assessment has become an important measure for designing controls. Assessing the risks associated with relational database design could result in various controls being proactively implemented to help prevent security breaches. Some controls available to prevent security violations include: access and authorization controls, specifically discretionary and mandatory access control; encryption, including full database and partial database encryption; and monitoring controls.

INTRODUCTION

In our ongoing research, we have been reviewing various techniques and controls used by companies for assessing and minimizing risks related to relational database security. In this presentation we briefly describe the necessity of controlling risks, in light of the increased focus from recent Sarbanes-Oxley (SOX) legislation. Through previous work experience as an IT Audit intern at a Big Four international accounting firm, the first author has experience with the auditing of a few different controls implemented for Oracle, including access, authorization, and program change control. We will draw upon these experiences in addition to reviewing the information assurance literature.

OVERVIEW FOR THE USE OF A RISK-BASED APPROACH

Our research is most easily divided into three sections: risk, controls, and tools used to test relational database security. With an increased awareness of risks stemming from SOX legislation and implementation, a focus on risk is maintained throughout. In addition, controls for database security risks are discussed, specifically the following: authorization and access, encryption, and monitoring techniques.

RISK-BASED APPROACH

Risk management is the foundation for any IT environment. The risk of unauthorized access to information "without appropriate authority" (ITGI, 2005, p. 9) is an important factor for an organization during the development of controls. By assessing where an organization's vulnerabilities lie, implementing appropriate controls can help minimize the risks of unauthorized access. As for any application, database risk assessment is a necessary first step when planning controls for a relational database. There are three types of controls necessary for access: limitation, data encryption, and monitoring. In the following paper, each type will be discussed as applied to a relational database.

ACCESS CONTROL

The first control we will discuss is access control. By controlling access to the database, the risk of an unauthorized access by a user is minimized. Limitation of access is primarily broken into two categories: discretionary and mandatory. Discretionary access is generally categorized by 'group' privileges, which in most cases, makes it easier to grant privileges to a user. Because each person assigned to the particular group is granted the same level (same rights) of access, this assignment "allows users to grant access to portions of data they control to other users" (Davidson, 1995, p.2).

Discretionary User Access

Discretionary user access can separate system versus object privileges, such as the use of CREATE table versus UPDATE table (system privileges authorize a user to perform an operation while object privileges grant the user "the ability to perform an operation on a specific database object" (Davidson, 1995, p.2). A group of users may have access to the payroll tables for example; however, Users A, B, and C may have the privilege 1, which allows them to create the tables in the database, while Users D, E and F, may only have privilege 2, which allows them only to update the tables. Furthermore, Users G and H may only be allowed to view the tables and not to update or create them at all, which may be privilege set 3. While this is an easier method for assigning, it easily allows members of a group to have access to too many rights or privileges, which may be unnecessary for their job function (or perhaps too few privileges for some job functions). Additionally, while this access control is initially a good form of protection for assigning roles within a database, it does not prohibit one user from copying information and disseminating it further to other users. For example, if User A was allowed to view payroll information, there is no protection against User A copying the information from the payroll table for User B.

Benefits of using discretionary user access controls include not only assigning user access roles but "can also limit access to information" (Davidson, 1995, p.3). The benefit of discretionary user access controls is multifunctional (limitations of roles and information) flexibility that this control provides to the company. Not only does discretionary access limit the areas of the database a user can access but also the information the user can access.

Mandatory User Access

Mandatory access is described as a more complex segregation of privileges, by assigning labels to each type of data according to its level of sensitivity. Access is assigned not based on protecting the security of the information, which differs from discretionary (discretionary access is based on task). In this case, each person is assigned a level of privileges to which they are allowed to view. Organizations would have to assess the level of risk and determine the best access level control to mediate their risk. A level would be defined by the sensitivity of the information within each category. In a multilevel organization, the data in the system are assigned a level according to the level of sensitivity. A level of clearance is then assigned to each user, and the level of clearance "denotes the range of labels that a user is authorized to access" (Davidson, 1995, p.4). The level of clearance gives the user certain areas of sensitive information that they are allowed to access but nothing further beyond their level of clearance.

Depending on which type of user access can minimize the level of risk associated with unauthorized access, would determine which type should

be implemented in the organization. For example, if level of sensitivity is a more appropriate risk mitigating control, than mandatory access would be more appropriate than discretionary access, and should be implemented into the organization.

ENCRYPTION

An additional control for protection of the data within the database is to utilize a form of encryption. Using one or more types of encryption would provide an additional safeguard to the database by placing a limit on what is visible to various users. Full database encryption encrypts the entire database, which places a limit on the readability of the database files (Davidson, 1995). Full database encryption places a limit on who can view the data within the database. For example, an administrator may be able to view who has access to the information but not what the information actually looks like (i.e. could approve access to payroll, but would not be able to view payroll information). For example, in Oracle, "user passwords are maintained in an encrypted format" (Mehta, 2004, p.43) this prevents an administrator from viewing the actual password. This control is generally used in conjunction with logical access controls, and can aid in increasing speed (when compared to full encryption). Similar to full encryption, partial encryption of the database should not limit the user's access to necessary information used in their everyday work.

Depending on the level of security needed to properly mitigate the risks associated with a breach of security into the database files, encryption may not be necessary given proper use of discretionary access controls or mandatory access controls. "Little additional security provided within the data base itself from full data base encryption," (Davidson, 1995, p.5) if discretionary or mandatory access controls are utilized properly. An obvious drawback to full database encryption is the need to periodically (weekly, monthly, quarterly) to change the encryption key. Depending on the size of the database, this could take an extensive period of time, due to the decrypting and re-encrypting of the entire database (Davidson, 1995). Because of this, partial database encryption may be utilized to protect especially sensitive data. Like full database encryption, this should not be configured in a way that will "limit access by users who are otherwise cleared to see the data" (Davidson, 1995, p.6). Partial database encryption will still require the periodic changing of encryption key; however, because only parts of the data will be encrypted, decryption and re-encryption time will be much less than full database encryption.

MONITORING

Another control which is used to track users is the use of monitoring. A record of activity is a good control to use in risk minimization. In many relational database programs, there is an audit trail or logging function, that when activated, can produce a list of what users logged in, when, what areas of data they accessed, etcetera (Mehta, 2004). Before implementing logging, it is important to decide which activities should be logged to achieve the most effective monitoring control. By reviewing the log, administrators can review the list of users who have accessed information to look for users who have been terminated, new users, or unauthorized users. This control keeps users accountable for their actions because their access is being monitored for access.

One control a company may utilize would be to review a list of user access monthly or quarterly to look for access which is not authorized. Auditors may select a sample of terminated users, for example, and compare these selected terminated users and compare their user names against the log of access to check that their access was first, terminated, and second, that they did not access the database.

For logging to be most effective, it is important to remember not to log everything. Thus, for each organization, it is important to assess the data/information risks for the organization, and determine which areas are important to log. Some key areas to focus on may be logging into the operating system, connecting to the database, and administrator-level access. Access denied may also pose a problem, such as instances when a user's access is denied multiple times in a certain time period.

CONCLUSION

As more and more companies use relational databases, assessment of enterprise risk associated to the databases use is a growing concern. By presenting a risk based approach, companies can cater their controls to what their company would specifically need. We believe our IRMA Conference presentation on our continuing research of database risk assessment and control methods will be valuable because of the relevancy related to Sarbanes-Oxley compliance.

REFERENCES

Davidson, M.A. (1995), Security in an Oracle Data Base Environment. *Information Systems Security*, 3(4), 59-68.

IT Governance Institute (ITGI) (2005), Information Risks: Whose Business Are They? Retrieved from www.itgi.org.

Mehta, R. (2004), Oracle Database Security. *Information Systems Security*, 12(6), 40-52.