

## Supporting SOX 404 Remediation with Identity And Access Management

**Philip Chukwuma**  
September 06, 2006

### **Introduction**

In the last two years Sarbanes-Oxley (SOX) law has made many companies aware of information security because executive management is now being held responsible for providing “due-care” in the support and security of systems that are material to SOX. The result of the first year of testing of section 404 of SOX produced one common theme; and that is that identity and access management (IAM), at many organizations, is deficient. Majority of the findings are about deficient identity and access management processes and procedures. In order to be compliant, companies will have to remediate IAM related findings through improvements in the process and the supporting systems. Specifically, companies have to address account management, password management, termination process, segregation of duties issues, etc.

### **Major findings in SOX Reviews**

As mentioned earlier, after the first year of SOX 404 testing, it was immediately apparent that identity management is the #1 issue facing many companies. Some of the issues identified in the first year of testing are as follows:

- Terminated employee user accounts are not disabled or deleted
- Users can obtain accounts without proper authorization
- Some user accounts do not require passwords
- There is no access control or access control methodology
- There are no policies, standards, and guidelines driving user account and password management
- Passwords are very easy to break
- Lack of segregation of duties
- “Super User” accounts used by many people in their daily work functions
- No proper control of “Super User” accounts
- Lack of documentation including identity management process
- Lack of logging, auditing, and review of events including identity management activities

#### **Sarbanes-Oxley**

In 2002 Congress passed a Law to address all the failure arising from publicly traded companies such as Enron. The magnitude of these failures and the associated executive malfeasances were the impetus for the law. The Sarbanes-Oxley, in effect, makes company executives responsible for any material weakness and requires the executive management to assert to the soundness of their financial report and the associated systems, policies, processes, and procedures. SEC was given the responsibility to monitor companies for compliance to SOX law.

While the above is not a full list of findings from SOX 404 testing in the first year, it is apparent that these need to be addressed to be SOX compliant. A more comprehensive list is included in Appendix A (“After First Year of SOX”).

### **Identity Management**

*Identity and access management* – is a mega process and solution employed to manage user accounts, passwords, and access rights. The users can be employees, contractors, customers, or business partners. The key aspects of identity management are the processes and the automated systems. Identity management is made of several other inter related, but independent, processes that provide service and security in the management of resources. These include provisioning and de-provisioning, user authentication, password management, employee self service, and access management. Access management includes the granting and restriction of access to a user, role, or group to a resource.

Access management requires that all the resources are cataloged and classified. The classification of the resource will determine who should have access to the resources and what type of access should be granted. For an example, if the resource is a table in a financial database, the classification should first identify the table as *Sensitive* or *Critical* and then define the types of access as *Read*, *Write*, *Delete*, etc.

*Provisioning* - Using our sensitive database example above, the provisioning process is used to administer, authorize, and document access to the database. The provisioning process will include documenting and providing all the required authorizations from the data owner, application owner, or business owner before access is granted. The provisioning process can use an automated workflow to move access request from request to actual creation or deletion of the account.

Provisioned resources may go beyond user accounts. It may include all resources that the company uses in the performance of its business function including SOX material functions. As such, such things as computers, laptops, blackberries, cell-phones, office phones, may be provisioned to an employee. The provisioning records also become a way to log and track all resources that have been assigned to an employee. This makes the de-provisioning process quicker and less expensive because all the system accounts associated with the user can be quickly identified and disabled. Also, all the resources assigned to the user can be quickly identified and collected.

*Policies, Standards, & Guidelines* - Policies, standards, and guidelines provide support to identity management. These include such things as developing a naming standard for user

#### **Segregation of Duties**

Segregation of duties is defining mutually exclusive functions and assigning permissions to those functions so that user can only perform one of those functions. Segregation of duties requires proper resource identification, catalogue, and classification.

accounts, servers, directories and shares. It also includes a definition of what constitutes a proper password, length, and age of password. The policies and guidelines should be used to determine how to format and manage user accounts. Policies and procedures, approved by upper management, are the driving force for an effective identity management process.

### **Addressing SOX 404 Issues with Identity Management**

Given the list of identified issues with SOX 404, IAM can address majority of these issues, through different mechanisms. Some of the mechanism employed were discussed above and include policies, provisioning of resources and access, proper identification and authentication, logging, tracking, and review of user account activities.

*Policies and Standards* - Resolving identity management issues will go a long way in addressing compliance issues for SOX 404 and any other regulations. This requires a good foundation embedded in corporate information security polices that address identity management. Such industry standard as ISO 17799 is a very good start in identifying required policies and formulating such policies. These policies should be supported by corporate standards and procedures that the respective platform Systems Administrator and/or application owner can use. The policy may state that all systems classified as *Sensitive* must use encryption in the transmission and storage of data. An internal encryption standard is then developed that specifies such things as the key length, and key management. The procedures will then define how the encryption is applied. These documented policies will provide some of the documentations required by SOX 404.

Security standards should also be developed for all available platforms (UNIX, Windows, etc). These security standards should be built into the configuration standard for each respective platform. The standard should also include the following:

- Password composition
- Password length
- Password aging
- Account expiration
- Third-party access
- Dormant accounts
- Unattended computers and screen savers
- Account review

In the case of such platforms as Windows, registry settings that provide additional security should be included. These standards should be applied on the respective platforms and will also be the standard to measure deviations both for SOX and for internal host reviews. Identity management will help companies identify those policies, standards, and guidelines that should be in place to support IAM processes.

*Data Classification and Segregation of Duties* - Defined data classification and roles are essential to access control and proper enforcement of segregation of duties. Segregation of duties is one of the major areas were issues were found with many companies. As

stated above, to properly determine the type of access to grant to users, data resources need to be counted and categorized on their importance, criticality, or sensitivity. Based on the classification, access is defined. Users are granted access based on user classification and also using the principle of 'least privilege'. 'Least privilege' gives users the minimum amount of access required to perform their jobs and as such ensures that no single user is given too much access.

Part of SOX testing is to look into user roles and determine if a user is performing conflicting functions or has the rights to perform conflicting functions. With a properly implemented segregation of duties, users do not have too many rights and are not allowed to performing conflicting functions. Identity management can be used to define roles and segregate functions by given the users only those permissions required to perform their jobs. Segregation of duties needs to be automated to be effective. The automatic review of user access will flag those roles that are mutually exclusive. A full definition of user roles while essential may not be required. However, a grouping of user activities is needed to properly implement segregation of duties. Access control is applied to the users or the group and segregation of duties implemented by defining the user's job and providing access to those things that will not amalgamate user rights and permissions. In some organizations, people that have been there the longest tend to have too many rights. This is because as the users are promoted or transferred their previous access is not revoked resulting in unintended 'Super Users'. In our database example, the business/data owner will be given permissions that define him/her as the data owner and as such any attempt to also give him/her administrative permissions will be flagged and logged.

Another issue with segregation of duties is the use of 'modeling' by some organizations in creating user accounts. Modeling occurs when a new user is hired by an organization and their user account is modeled against an existing employee's account. The problem with this is that if the existing employee has accumulated permissions over the years across different functional groups, the permissions are given to the new hire. With IAM, roles are defined and assigned to the user, thus resolving this SOX issue.

*Authorization and Provision* - How the whole process of obtaining access, maintaining access, and removing access is managed is essential to identity management and SOX 404 testing. This is the provisioning and de-provisioning process. The provisioning process is important to SOX because it is important to know who is requesting access; who authorized the access; who created the access; what access was requested and what access was granted? The de-provisioning process is important because we need to determine how quickly access is removed when no longer needed. It is not uncommon to find terminated employees who have access to systems in their former place of employment 12 months after they have been gone. And of course the accounts are still active.

The provisioning and de-provisioning process reduces the time required to create or remove an account. It also provides a mechanism to obtain the required authorizations

before a user account is created and access is granted or modified. This mechanism is the workflow that is used to automate the movement of access request from one point to another until the access is granted or denied. It becomes a means to document access requests and authorizations, and management reports can be generated from such records. Using this information, a comparison can be made quickly between requested access and actual access. This effort will help reduce the amount of time required for SOX testing for future years.

*User Identification and Authentication* - For users of resources that have been defined as being relevant or material to SOX, there needs to be a way to identify these users. Identity management provides such mechanism for identification of user. The framework could start with a security policy that requires each person that needs access to a company's IT resources to have a valid userid and a password, and have an active relationship with the company. This will eliminate the user of general use accounts and create an environment where the user account name is the same on every system. With the userid the user is identified and with the password the user is authenticated to the system before access is granted. All system permissions are then granted to the user based approved roles.

As such, the question "Who has access to System A?" (where System A is a SOX material application) can be easily answered by generating a list of all current users. A dump will also provide the level of access for each user in the system. These lists are reviewed periodically to verify the legitimacy of the user and the appropriateness of the level of access.

*Auditing and Reporting* – The interpretation of SOX for the first year requires that access to SOX material data is logged and the logs reviewed frequently. To support this requirement, account creation, deletion, and modification have to be logged, as well as changes to user access. The authorization of the access also needs to be logged so that issues concerning segregation of duties can be identified and reported. It is not enough that activities are logged, but in order to meet SOX requirements, these logs must be reviewed regularly. These logs can be forwarded to a central log server, managed by the Information Security group.

IAM provides a means to document activities that occur during the account management. The provisioning system, with its workflow, can provide a logging and tracking mechanism that will record all user administration activities. The access control system can also log all activities on monitored IT resources. This provides an audit trail that answers the questions who changed what, when, and how?

## Conclusions

It will be safe to draw two conclusions from the information above and one of those is that "*Effective implementation of identity management will lead to better security*". This is possible because an effective identity and access management system will result in a better user administration and access management process and system. It will result in an

efficient provisioning and de-provisioning process, and provide automated tracking, auditing, and reporting of activities.

The second conclusion is that “Effective identity management implementation will lead to compliance with current and future regulations”. SOX 404 interpretations will continue to evolve and produce new requirements. Many regulations are pending in Congress today addressing information security. It will be safe to say that we will see new regulations in the future addressing information security in general and identity protection and management in particular. A sound implementation of identity and access management that addresses items identified above will provide favorable compliance results for organizations. These favorable compliance results will include SOX 404 in its current form, future interpretations, and will also support and address future regulations.

## **Appendix A - After First Year of SOX**

- Lack of security policies.
- Lack of security standards especially governing user account management.
- Lack of an effective monitoring process and tools.
- Lack of segregation of duties.
- Employees who have been in a company for a long time tend to accumulate system permission even after they change department
- Account policies differ from one system to the other.
- Resource classifications are not done.
- Full access is granted in many systems.
- Password policy is either weak or not implemented.
- Production systems are implemented with default configurations and password.
- System passwords are in clear-text.
- System accounts do not have any password.
- No formal process for new account creation, modification, and deletion.
- Terminated employee accounts are not disabled or deleted.
- User accounts do not require passwords.
- Account lockout is not implemented.
- Users can obtain accounts without proper authorization.
- “Super User” accounts are used by administrators in their daily work activities.
- Use of “Super User” accounts is not logged.
- Lack of trained personnel. Some companies that will like to perform 404 remediation internally do not either have people to perform remediation task or have the right skill-set in-house. Some companies do not have the personnel that understand and can implement segregation of duties, provisioning, or the essentials of Information Security.
- 3<sup>rd</sup> Party users are not categorized.
- 3<sup>rd</sup> Party user accounts do not have any expiration date.
- 3<sup>rd</sup> Party user access are not logged.
- Periodic review of user accounts is not performed.
- Inadequate vulnerability testing.
- Lack of a robust change management process and tools.
- Lack of an effective user awareness program.
- Deficient general access control mechanisms. It is not uncommon to find companies where the group “Everyone” for example is has full access to every directory.
- Lack of a proper remediation plan.
- Lack of Resources.
- Lack of a testing environment for SOX 404 remediation.
- Lack of proper system documentation.
- Under-estimation of Remediation effort.