

Testing User Access Control For SOX Compliance: Lessons Learned

By Nalneesh Gaur

The rush to comply with the Sarbanes-Oxley (SOX) regulation has placed an inordinate burden on publicly traded companies. American companies have criticized the SOX regulation as too onerous and expensive.

I have been personally involved with a SOX compliance effort with focus on the IT components of SOX. SOX requires testing of internal controls to identify material weaknesses as it relates to financial reporting. Section 302 and 404 of SOX are the key emphasis areas for information technology. SOX looks at the nature and characteristics of a company's use of IT in its information system that affects the company's internal control over financial reporting. Elements such as income tracking, purchasing, payroll, and reporting are reviewed. Organizations must ensure that appropriate controls (including IT controls) are in place. They must also provide their independent auditors with documentation supporting management's assessment. This includes design documentation and the documented results of the test procedures.

User Access (UA) testing is a key component of SOX testing. The external auditors will test UA for financially relevant applications at the Database, Application and Operating System Levels. This article draws upon my experience and outlines test preparation, lessons learned and recommendations to automate some of the UA testing activities for the future.

What is Tested?

External Auditors will test the effectiveness of controls for a specified period of time as defined by executive management. The focus of SOX is on financially relevant applications, the supporting databases and the underlying operating systems. Internal testing of controls (by internal audit, risk management or other such groups) is an ongoing activity prior to external auditor testing. It is not sufficient that controls exist; they must be documented. The external auditor tested SOX compliance in four broad areas, namely:

1. User Access
2. IT Operations
3. Change Management
4. Systems Development Life Cycle (SDLC)

The scope of SOX testing is depicted in Figure 1. Overall the SOX testing effort can be represented as:

$$\text{SOX testing effort} = N_{\text{FRA}} \times N_{\text{TA}}$$

You can probably surmise that testing more often and/or increasing the number of financially relevant applications will increase the SOX testing

effort. I have seen N_{TA} vary from four to twelve times a year. I have heard of the N_{FRA} number reaching as high as 60.

In UA testing it is not sufficient to determine whether the user should have access. You must also determine whether or not the privileges granted to a given user are appropriate. UA testing includes:

- ▲ Generation of User Access Reports (UARs): This report contains details about the user and their access.
- ▲ Investigation of Malicious Activity: This involves investigating terminated users for malicious activity: For this access, logs and intrusion detection reports must be consulted.
- ▲ Remove unnecessary access privileges and users: Where there is excess privilege, it should be removed.

Such testing needs to be performed on a periodic basis. In my case, we tested on a monthly basis. For every period the UA testing will need to be certified by Business Owners, Application Owners, Business Relationship Managers, and IT must certify users as applicable. Corrective actions such as locking/removing user IDs or change in privileges as a result of the internal testing will need to be documented.

How to Prepare

Internal controls can be tested any time prior to filing for 10K. External auditors are specifically prohibited from relying on management's test results. However, early testing will make you aware of the deficiencies in internal controls before your auditor finds them. The SOX UA testing boils down to answering a basic question: "Who has access to what at a given time?" The three-step process outlined below provides an approach to SOX UA testing:

I. Define scope of UA testing: First and foremost, it is essential to identify the financially relevant applications. Once these are identified, then the corresponding database and operating system dependencies must be identified. The resulting list of systems, applications, and database will constitute the scope of the UA testing effort. It is paramount that the process of identifying the UA scope be started months in advance before the end of the financial year. Right sizing the scope is crucial. Too much scope will result in increased effort and too little scope could result in nasty last-minute surprises or compliance deficiencies.

II. Generate User Access Reports: For all elements in the UA testing scope, we need to generate User Access Reports (UAR). Keep in mind that it is not necessary to generate electronic UARs. In some cases, if you have documented procedures for generating paper-based UARs, then

those reports should suffice. The UAR consists of the following details for each user:

- A. Unique user identifier: This defines the “who” of the access and in some cases could be just the user ID. But as you review users across multiple systems, you may determine that a user ‘jsmith’ on one system is not the same as ‘jsmith’ on another. During the course of my project, I came across situations where an individual was rehired (in some cases more than once.) The unique user identifier may be a combination of user ID, full name, employee ID and account creation date.
- B. Access privilege: This defines the “what” of the access and will vary across different scope elements.
- C. Termination date: This is used primarily to ensure that the terminated user’s access was revoked. If the user ID was terminated, then a termination date needs to be recorded. The HR database should be consulted to capture the terminate date.
- D. Current status: Most systems and your corporate policy may lock out a given user upon termination rather than delete the account. Possible value for this field can be “Locked” or “Active.”

III. Certify UAR: The process of access certification and documentation can be both time- and resource-consuming. To put it in perspective, let us say you have identified 25 financially relevant applications. You determine that there are 5 back-end databases supporting the applications and that there are a total of 75 operating systems that support the applications and databases. In this case, you will need to capture 105 (75+25+5) UARs. What makes it complicated is that some of the applications may be out-sourced and that it is sometimes not easy to locate an asset owner. Further, for users who no longer need access to a system (due to termination, or transfer), malicious activity will need to be investigated.

Lessons Learned

In the middle of my project there was no turning back, however, I tried to imagine how simple the whole effort would have been in a centralized mainframe type environment as compared to the distributed computing environment. But since that’s not the world we live in any more, here are the lessons that I learned.

1. The scope and effort may not be fully understood: As I mentioned earlier in the text, the scope is a function of frequency of testing and the number of financially relevant applications. Adding/removing financially relevant applications can result in increased or wasted effort. In my case, we were still finalizing the list of financially relevant applications even as we neared the end of the fiscal year. As a result, we were challenged both by the changes to the list of financially relevant applications as well as the fast-approaching time limit (end of fiscal year).
2. Communications can be fast and furious: Faced with a time limit and as yet undefined list of financially relevant applications, the communication back and forth between all stakeholders, internal audit, and application owners caused unnecessary confusion. Once in the midst of the effort, there is simply no time to redefine the communication rules.
3. Restoration from backup tapes may be required: For the past month’s UARs, we had to go back in time and certify users. This required that we request backup tapes and restore user access

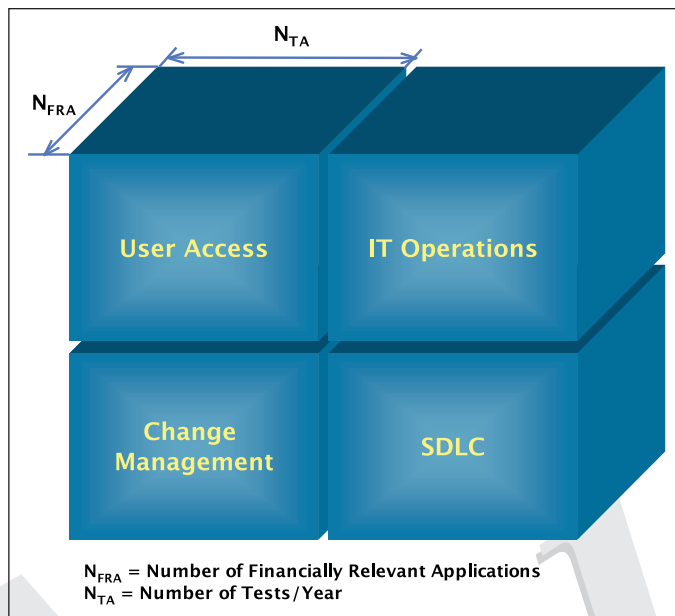


Figure 1: SoX testing scope

information and logs in a non-production restoration environment. Identifying spare hardware for restoration and locating backup tapes is not a trivial task and can slow you down significantly.

4. Anticipate the volume of UARs for each period: The sheer volumes of UARs that are generated can be overwhelming. Our hypothetical 25 financially relevant application scenario 105 UA reports would need to be extracted and signed off on a periodic basis. To ensure report consistency, we provided all application owners with a template that listed all required fields. Next for each period, we tracked report status from generation to sign-off and archival by OS, application and database.
5. Expect Orphan IDs: At sign-off many orphan user IDs could result. Orphan IDs are those that neither a Business nor an Application owner is ready to sign-off on. In our case, after investigating malicious activity, we took one of two actions: 1) Lock/Remove or 2) Reassign the orphan ID. Both are not easy actions to take because either action could disrupt operations.
6. It may be impossible to investigate malicious activity by terminated transferred users: It is challenging to investigate malicious activity for terminated/transferred users when audit, log or any host-level intrusion detection information is lacking. This to me is a dead end and may require management accepting the risk and signing-off on the user.
7. Expect severe resource constraints: Companies that have their financial year ending in December will find it challenging to coordinate resources due to holidays and personnel vacation plans. During such times, it is likely that your sense of urgency is not shared by others. Internal testing will more than likely continue over weekends. At some point, employee morale may need to be addressed.

Recommendations

1. Clearly define the scope and communication plan: If the scope is not defined properly, it has a cascading effect on the SOX UA testing effort. The scope should also be a key input into the


communication plan. The communication plan will address the stakeholders, internal auditors and application/business owners.

2. Start months in advance: I would echo that which has been repeated in several SOX preparation articles: Start at least 4-6 months in advance. Pay special attention if your financial year ends in December. Both November and December are holiday months and it is difficult to locate resources when they are away on holiday or vacation.
3. Standardize on the UAR format: Standardization will help you quickly review access and will also make it easier for your auditor to review your work (even if they don't rely on it).
4. Regularly review UARs: Business and Application owners should set up a process to regularly review and sign-off on UARs.
5. Automate: Organizations that have implemented components of an Identity and Access Management (I&AM) system will find it much easier to perform UA testing than those that haven't. An I&AM solution consists of processes, people and technologies that control who has access to resources in the enterprise. Components of a full-blown I&AM solution are listed below:
 - a. **Identity Management** provides users with the capability to register their identities and manage their passwords and profiles.
 - b. **Access Control** provides user identification, authentication, secure session management, and authorization services to applications and resources within the enterprise.
 - c. **Provisioning and De-Provisioning** automates the administration of user access to systems, applications, and resources.
 - d. **Identity Repositories/Directories** provide consolidated storage of user identities, policies and audit log information. Centralized repositories feed provisioning engines and provide the foundation for authentication and access control services.

Please be aware that an I&AM implementation is not a two-week long project. Depending on your environment, plan at least 4-6 months prior to implementing the proposed I&AM solution components.

Conclusion

SOX requires the testing of internal controls to identify material weaknesses as it relates to financial reporting. The SOX test effort is proportional to the number of financially relevant applications and the number of times the controls are tested per year. The User Access testing component of the internal controls testing requires months of planning and can be quite a burden on resources. Much thought should be given in structuring the scope of the SOX UA testing and subsequently developing a communication plan.

To automate the UA testing process, consider implementing an I&AM system. Planning and improving internal process as well as implementing parts of an I&AM system will greatly reduce the burden on SOX UA testing. If you are unable to implement an I&AM system, then you will need to create and communicate the manual process in the short term. 

Nalnees Gaur is a CISSP, BS 7799 Lead Auditor, and a Manager with Diamond Cluster International.