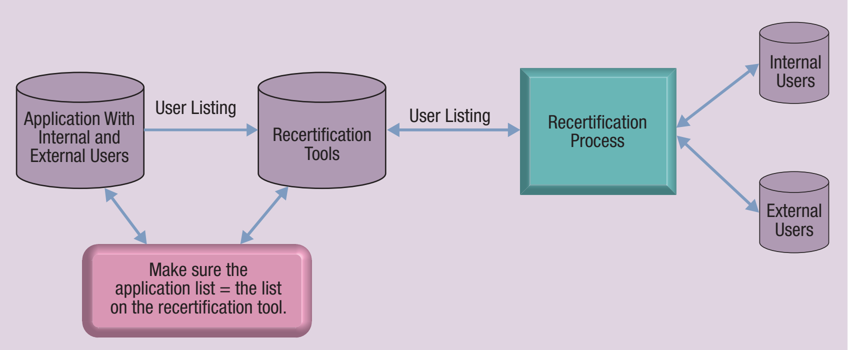
Importance of Recertification Completeness in the Control Environment

Owners of critical business data need to ensure that all application and database user entitlements and privileges are recertified on a periodic basis to make sure that only authorized individuals have access to the enterprise's data. This article assumes the enterprise has a periodic recertification process in place for their applications and databases. It also emphasizes the need for each enterprise to have a completeness check to validate this key control. Depending on the impacted applications, a gap in this control may have a negative impact on an enterprise's US Sarbanes-Oxley Act 2002 (SOX) compliance audit or Statement on Standards for Attestation Engagements (SSAE) 16 audit.

Application Layer Recertification

Many enterprises have internal and external (client) application users. The process of recertifying internal users and external users can be different, depending on the application. Management must ensure that a process is in place to correctly distinguish external users from internal users. The enterprise must establish and communicate standards for recertifying its clients as external users in addition to recertifying internal users. The standards should include the client's responsibility for the accuracy and completeness of user access. A designated client contact must periodically review the client user and entitlement list and confirm the list is accurate and complete.

Figure 1—Application Recertification Using a Recertification Tool


Application With Internal and External Users
User Listing
Recertification Tools
User Listing
Recertification Process
Internal Users
External Users
Make sure the application list = the list on the recertification tool.

Source: K. Martin. Reprinted with permission.

For internal users, management must ensure that a consistent methodology is executed regularly for recertification. At a minimum, the recertification should be performed on an annual basis, but could be more frequent based on the nature of the application and the sensitivity of the data. Larger enterprises use recertification tools (**figure 1**) to rely on the data inputs from business applications. Many applications have existed for years, and the feeds to the recertification tool may not have been revisited to accommodate changes to the application or the recertification tools. If this type of situation occurs, the enterprise may be at risk for not recertifying all user IDs.

To ensure that all users and entitlements at the application layer are recertified, management should perform a completeness check by comparing a user listing of the entitlements on the application to a user listing of corresponding entitlements on the recertification tool. Management must ensure that the two files reconcile. If they do not, the enterprise may have issues with the data feeds or the entitlement process, or just have timing differences.

Without being able to confirm that the source application and recertification tool data reconcile, management can be assuming risk of users who have not been recertified and, therefore, may be unauthorized. The unauthorized individuals may have retained logon IDs after being transferred or retained entitlements or privileges that they no longer need.

Database Layer Recertification

Most database users are database administrators and, by the very nature of their jobs, need to have access to the enterprise databases. However, there could be situations when either not all database

Kathleen Martin, CISA, CRISC
Is currently employed by Santander Bank as a director of risk infrastructure controls. Previously, she worked for ING, CitiSreet and JPMorgan Chase.

users are recertified or not all of their entitlements or privileges are recertified. Management should pay particular attention to how functional IDs are used and if those IDs are recertified in the management recertification process. If a functional ID is not recertified, anyone with access to that ID may be able to make changes, resulting in unauthorized access to the database.

> **“If the data are recertified at a very low level, it is quite possible that the control will be viewed as an administrative exercise and not be taken seriously.”**

Entitlements or privileges at the database layer can also present a challenge. User roles or privileges at the application layer, in most cases, can be straightforward and easy to interpret. Depending on the database type, several lower-level entitlements may or may not need to be recertified. Management needs to assess the entitlement level required to perform a reliable recertification. For example, entitlements may be provisioned at a table level. However, recertifying at a table level may be too onerous and may not be performed appropriately. If the data are recertified at a very low level, it is quite possible that the control will be viewed as an administrative exercise and not be taken seriously. Therefore, recertifying at the correct level of role or privilege not only helps to facilitate a completeness check (by not having to reconcile all lower-level entitlements), but the check should be more meaningful because the manager can understand the access the user is retaining.

After the recertification completeness checks are performed, management should execute one last step. Management should confirm that every user who no longer needs access has been removed from the system. It is possible for management to perform all of the prior steps but not actually remove the IDs or entitlements that are no longer needed. If they are not removed, additional risk is placed on the enterprise for allowing defunct IDs to continue to allow access. Depending on the password security strength, other internal users may be able to compromise the defunct IDs.

Recertification of user IDs and their entitlements has been a standard control for many years. Management should continue to be diligent to ensure a completeness check for application-level and database-level user IDs and entitlements.

Author’s Note

The opinions expressed in this article are the author’s own and not those of her employer.