FEATURE

Rethinking User Access Certifications

They go by different names. Some people call them user-access reviews, others call them access certifications and still others call them periodic access reviews (PARs). This article refers to them as access certifications. Access certification involves a manager or system owner reviewing users' entitlements (access) to a system or systems to ensure that the users have access to only what they need.

Access certification has been around for as long as users have been granted access to systems, and numerous standards and regulations require them. Over the last couple of decades, access control technologies and system advances have necessitated rethinking how access certifications are used as a control and at what frequency.

This article lays out several risk factors for determining how critical access certifications are in an enterprise's environment. It also discusses the certification metrics and automation possibilities that should be considered when designing and monitoring access control processes. It will help enterprises align time, effort and cost by focusing critical controls on identity and access management systems where possible.

Risk Factors

Are the enterprise's access control processes more manual or automated? This risk factor is important when designing access review controls. The more manual an access provisioning and deprovisioning process is, the more likely access certifications will be of value. Likewise, the more automated the process, the less likely access certifications are to provide value, or the cost to perform the certification will exceed the benefit received from it. For example, at one time, the only way to approve access to a system was through a paper form. A system administrator would then provision the access approved on the form. A typical scenario for removing access was the system administrator receiving a form or a report from the human resources (HR) department indicating that the user had left the enterprise or had a new position. **Figure 1** and **figure 2** illustrate the differences between manual and automated processes.

Manual processes created greater opportunities for errors, which could be corrected during the user certification process. As a result, user certification played a prominent part in the control structure. It was a common occurrence to find users who no longer worked for the company to still have access to systems or to find users who had excess access from positions they no longer held.

Fast forward to today, and a user's access to a system is more likely to be tied to an identity and

Vincent J. Schira, CISA, CIPT, CISSP, CPA, PCI-ISA
Is an information security compliance program leader at Domino's. Responsible for compliance with a wide variety of regulations, his focus includes consumer data privacy, Payment Card Industry Data Security Standard compliance and identity management. Before joining Domino's, he held leadership positions in accounting, materials and logistics management, and internal audit within the automotive industry. Schira has presented to the National Restaurant Association and the Institute of Internal Auditors on key audit and security concepts. He also works part time as a firefighter and emergency medical technician for the city of Novi, Michigan (USA).

Figure 1—Manual Provision Process

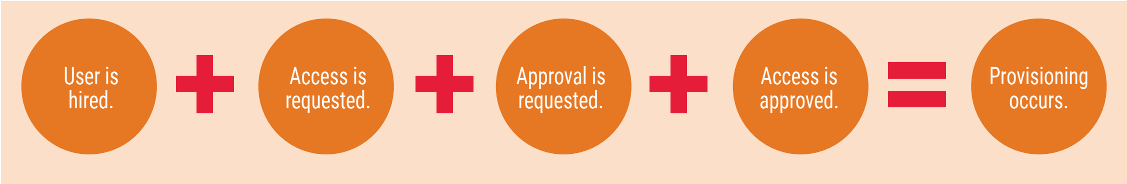
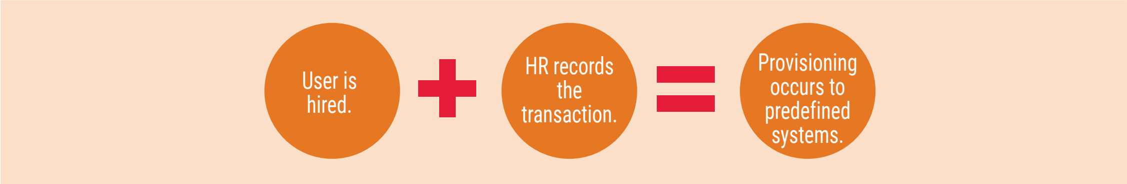


Figure 2—Automated Provision Process


User is hired.
+
HR records the transaction.
=
Provisioning occurs to predefined systems.

access management (IAM) system. The IAM system is updated through an interface from the enterprise's HR system and automatically provisions access according to the user's identity and role(s). In addition, when a user is terminated or changes positions, the HR system sends this transaction to the IAM system to perform the deprovisioning for all the systems in the user's role that are no longer needed. In these instances, it is likely to find the access certification to be less valuable, and the access certifications produce relatively clean results. This is because the user's access has been linked to his/her position and identity. Other than maintenance of linkages, there is no manual human intervention required to adjust or terminate access. The argument can be made that the access certification has been transformed from a manual control to an automated application control. The IAM system continually checks the system in question for users who should not have access.

Figure 3 and **figure 4** illustrate the differences between manual and automatic deprovisioning processes.

> “THE IAM SYSTEM CONTINUALLY CHECKS THE SYSTEM IN QUESTION FOR USERS WHO SHOULD NOT HAVE ACCESS.”

How does the enterprise control segregation of duties? Assessing this risk factor is another indicator of how critical access certifications are in

Figure 3—Manual Deprovisioning Process

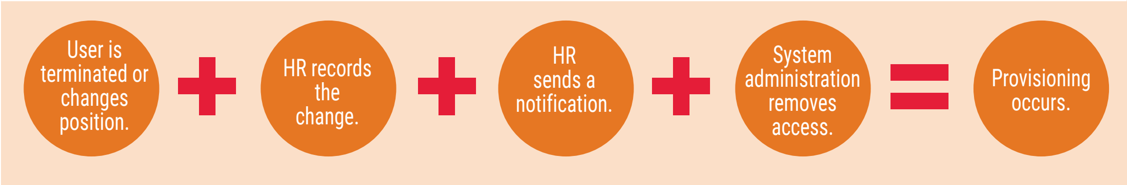
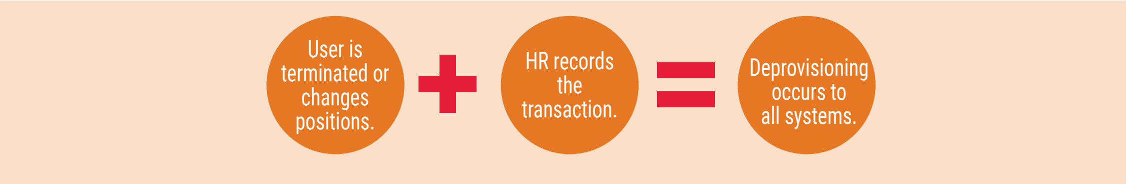

User is terminated or changes position.
+
HR records the change.
+
HR sends a notification.
+
System administration removes access.
=
Provisioning occurs.

Figure 4—Automated Deprovisioning Process


User is terminated or changes positions.
+
HR records the transaction.
=
Deprovisioning occurs to all systems.

the control structure. A purpose of the traditional access certification is that system owners look for segregation-of-duties violations (the pairing of two conflicting transactions). This was necessary because a manual review was the only way to check for such violations. Today, the process for identifying violations is often automated through an IAM or governance, risk and compliance (GRC) application. The IAM and GRC applications continually search across multiple systems for violations and notify the appropriate personnel so the access can be corrected.

Is the enterprise centrally managing decentralized facilities or systems (i.e., is an application administered at a headquarters location, but the users are distributed at operations facilities in different regions or even countries), or are systems managed locally? Historically, IT systems were managed by system administrators who worked in the data center. With the advances in technology, many systems can now be managed by end-user departments. This eliminates the breakdowns in communication that can occur between the administrators and owners of a system, which can lead to the need for more frequent access certifications. The end-user department can manage access directly based on the needs of its team. **Figure 5** lists indications for access certification frequency.

Automation and Metrics

There are times where an access certification is appropriate. For these instances, an IAM application is invaluable. Most IAM applications have many options for configuring certifications.

> “MANY IAM AND GRC APPLICATIONS HAVE THE CAPABILITY TO APPLY A RISK RANKING TO USERS BASED ON THEIR ACCESS.”

Many IAM and GRC applications have the capability to apply a risk ranking to users based on their access. The risk calculation is based on parameters configured in the application. This is an excellent way to focus on high-risk users and to maximize the time individuals assigned to certify the access have. For example, certifications can be designed to review high-risk transactional access quarterly and read-only access annually.

Figure 5—Indications for Access Certification Frequency

+

Indications that access certifications need to be done on a frequent basis:

- There is a large user population.
- No monitoring is in place.
- Users are geographically dispersed.
- System or data owners are separate from the administrators of the system and the user population.
- There is high user turnover.
- Past certifications yielded many high-impact adjustments.
- The system provides direct access to data or transactions (not through a user interface).

−

Indications that access certifications need to be done on a less frequent basis:

- The user population is a small team or department.
- Automated monitoring through a GRC or IAM is in place.
- Users are centrally located.
- Access is managed by the team who owns the system or data.
- There is low user turnover.
- Past certifications yielded few adjustments.

In addition, access certifications can be configured to occur when changes in roles or entitlements are detected by the IAM application. Any access not reviewed during a change can be configured to be certified in a fixed interval review. This is an excellent way to spread certification activity in smaller increments. This is opposed to the traditional certification where all access is certified at a fixed interval, which can often overwhelm a reviewer and lead to a less thorough review.

The access certification functionality of IAM applications also provides useful metrics on how much access is adjusted during a certification event. These metrics can be used to further justify or modify the certification frequency. If certifications are yielding a high number of unexplained and impactful access adjustments, it is important to consider conducting certifications more frequently. If certifications have few access adjustments or adjustments are not significant, it is important to consider lowering the frequency of certification. The metrics are also useful to identify problems in the upstream provisioning or deprovisioning processes. **Figure 6** and **figure 7** illustrate two must-have metrics for an IAM program.

Figure 6—Percent of Entitlements Removed

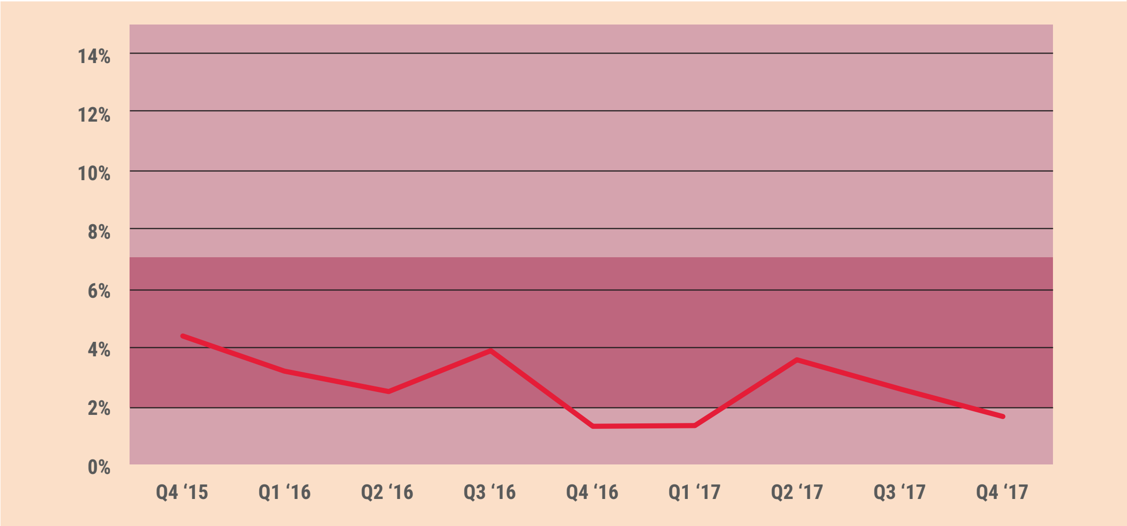


Figure 7—Percent of Users Adjusted

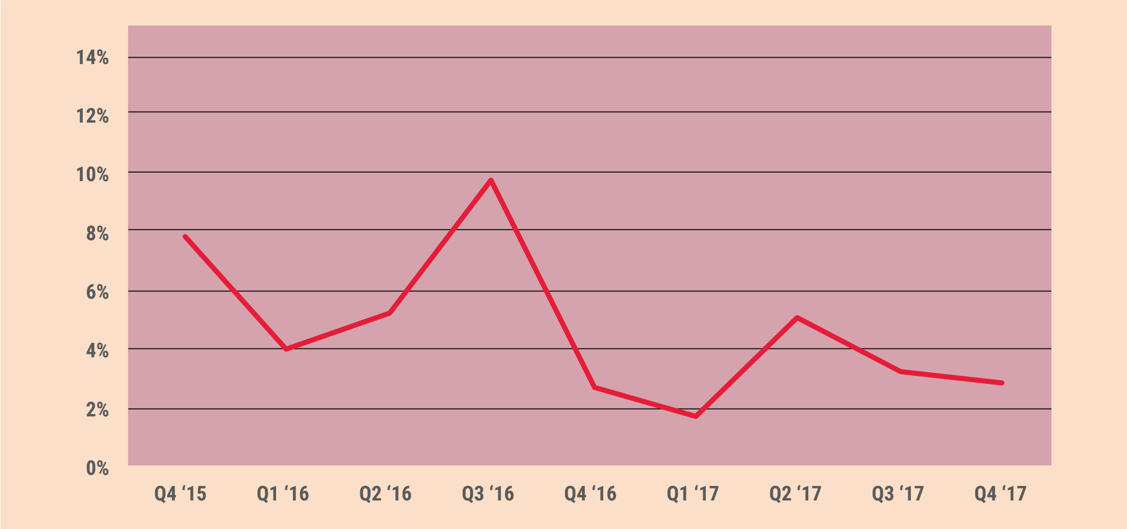


Figure 6 shows the percentage of entitlements removed during access certification for a given period. An entitlement is defined as the fine-grain access that is used to execute IT access policies to data, devices or services. They are also called authorizations, privileges, rights or permissions. For example, if there are five users who each have five entitlements, there is a total of 25 entitlements. If, during an access review, two of these entitlements were removed, 8 percent of entitlements (2/25) were removed.

> “OVER TIME, THE ENTERPRISE WILL BE ABLE TO DEVELOP A BASELINE OF WHAT IS NORMAL BASED ON THE PROVISIONING AND DEPROVISIONING CONTROLS IN PLACE.”

Over time, the enterprise will be able to develop a baseline of what is normal based on the provisioning and deprovisioning controls in place. Significant increases in the number of entitlements removed means access is being overprovisioned or deprovisioning controls are broken. A number dropping too low could indicate extremely good controls or possible reviewer fatigue, and there are more entitlements that should be removed.

Figure 7 shows the percentage of users adjusted (the percentage of users who had one or more entitlements removed) during the access certifications for a given period.

Looking at Both Percentage Charts Together

A high percentage of users adjusted and a low percentage of entitlements adjusted means just one or a low number of entitlements are being removed from many users. This can mean that one entitlement is being overprovisioned to a large population of users.

A low percentage of users adjusted and a high percentage of entitlements removed means that many entitlements are being removed from a low number of users. This can mean that entire users are being removed, indicating a possible problem with the terminations process.

If an enterprise decides to place more emphasis on the automation provided by the IAM application and the metrics it can track, it is important to ensure that the IAM application has the appropriate controls in place. The following concepts are critical to ensure the integrity of the IAM application and processes:

- Change controls over the configurations and functionality in the application.
- Control overprivileged access to who can make critical changes to the application.
- Maintain operational controls to ensure that the data in the IAM are current and accurate.

Conclusion

Using these criteria and metrics to conduct a risk assessment and facilitate a discussion with auditors is a useful way to rightsize the access certification program and add more reliance on the IAM application. In addition, for enterprises without an IAM or GRC application, this article provides some of the benefits and cost reductions that can be used to justify a purchase. Following these points will allow an enterprise to match the cost with the benefit of access management controls.