Access Certification: Reducing Risk with the Right Information and the Right Processes

Abstract

To comply with internal policies and industry regulations, managers need to regularly attest that their employees need the access they have. This is a crucial task for organizations in health care, organizations that accept credit cards as forms of payment, government departments, financial institutions and any publically traded company. Failing to ensure proper access rights can be incredibly costly, resulting in negative public perception, a drop in stock price, and fines, as well as criminal and civil lawsuits. This paper explains the challenges related to access certification and how to address them.

Introduction

How attestation usually works

In most organizations, access certification is a boring, intensively manual task that requires staff to review lists on spreadsheets to determine whether staff are still with the organization and whether they should still have the access rights they possess. In most cases, managers have no idea what access each employee has, and so must simply assume that, if the person is still employed and still on their team, the access rights must be ok. To pour a little fuel on the fire, often the list includes a "check all" box, which saves the manager a great deal of time: All he or she has to do is just click that box and, right or wrong, be finished.

Is there a problem with this "blind attestation"—that is, managers attesting to access rights without knowing whether those rights are still needed? I mean really, what's the worst that could happen? You don't want to find out firsthand: The consequences can range from negative public perception, fines, and a drop in stock price to criminal and civil lawsuits.

Here's something close to a worst-case example: In October of 2010, former Societe Generale trader Jerome Kerviel was convicted to three years in a French jail and ordered to repay 4.9 billion euros. Evidence showed that Kerviel used old passwords from former job roles within the company to perpetrate rogue trades on his own without any oversight.

Something like this could happen at your organization as well if your managers blindly attest that their employees should maintain their current access rights simply because they are still employed there. What about the employee who just transferred in from another department? Does he still have access to a file share that his former role required? Is that in violation of the compliance regulations your organization must adhere to?

All too often, managers who are asked to review employee access do not have a full picture of what they are attesting to.

The root of the problem

Problems related to attestation often stem from three causes:

- Lack of information
- Lack of understanding of the information you do have
- Lack of defined processes in
- how to certify access

Lack of information

All too often, managers who are asked to review employee access do not have a full picture of what they are attesting to. They can verify that everyone is still in their department or is still employed at the organization, but usually they don't have details about what access rights each employee has. Therefore, managers cannot reliably attest to whether employees should retain their current access rights. Instead, they must make a big assumption that the status quo is OK.

Some organizations have shifted attestation tasks to the application owners, but application owners who are asked to perform access certification usually lack the same details about access rights as business managers, and may also lack information about each employee's current role and access needs. For example, an application owner might have granted access to a given employee a couple of years ago in response to an email request. Now the application owner can only look up the employee's name in the HR spreadsheet of employees (or perhaps the email Global Address List) and see that this person is still employed with the organization; the application owner likely has no information on the individual's current role and whether their current duties still require the same access. Perhaps they were promoted recently into a new role or department and no longer need the same access.

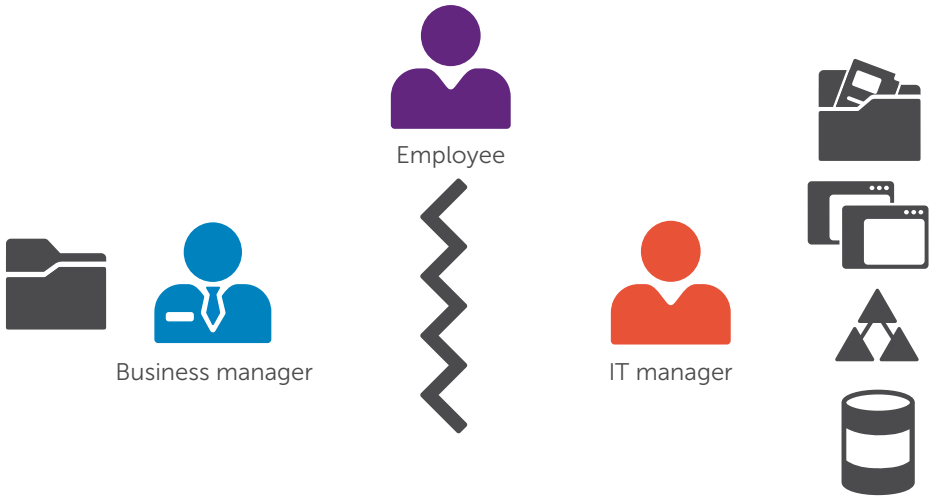

Figure 1: Usually, the business manager sees only that the employee is on their team and understands their current role but can't get a clear view of what specific access entitlements they have. Conversely, the IT manager can see which systems and applications can be accessed by the employee, but doesn't understand the employee's role nor which access entitlements are necessary for that role.

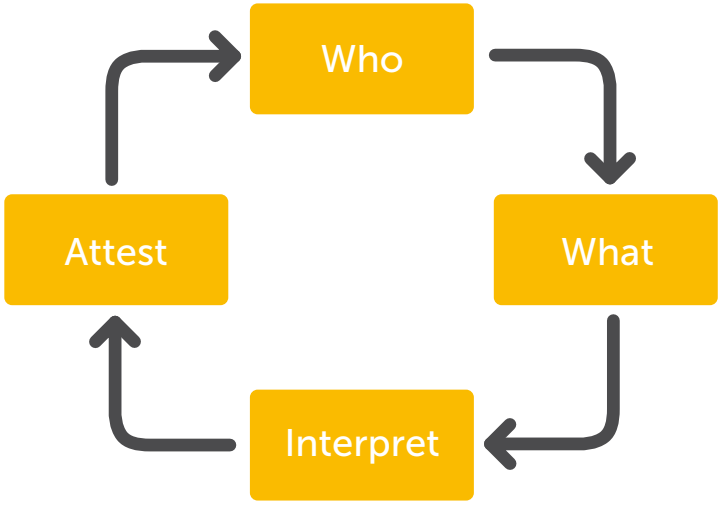

Figure 2: The pieces to solving the challenge of access certification.

The disconnect here, regardless of whether it's the application owner or the business manager doing the access certification, is a lack of information.

Lack of understanding

Some organizations do provide business managers with a list of the entitlements meaning all the access rights associated with each employee (perhaps generated by a home-grown program to help with access certification). Unfortunately, more often than not, the entitlements are not easy to understand. A business manager might be able to see that employee John Smith has access to \\DC7\C$\, but would the manager understand what that means? Possibly, but it's more likely that the manager won't know what server or share that is, whether John can access everything on it, what else is on that server, and so on. It's just not clear.

The IT manager has the opposite lack of understanding: He or she easily understands what \\DC7\C$\ is, but doesn't know what role John Smith has

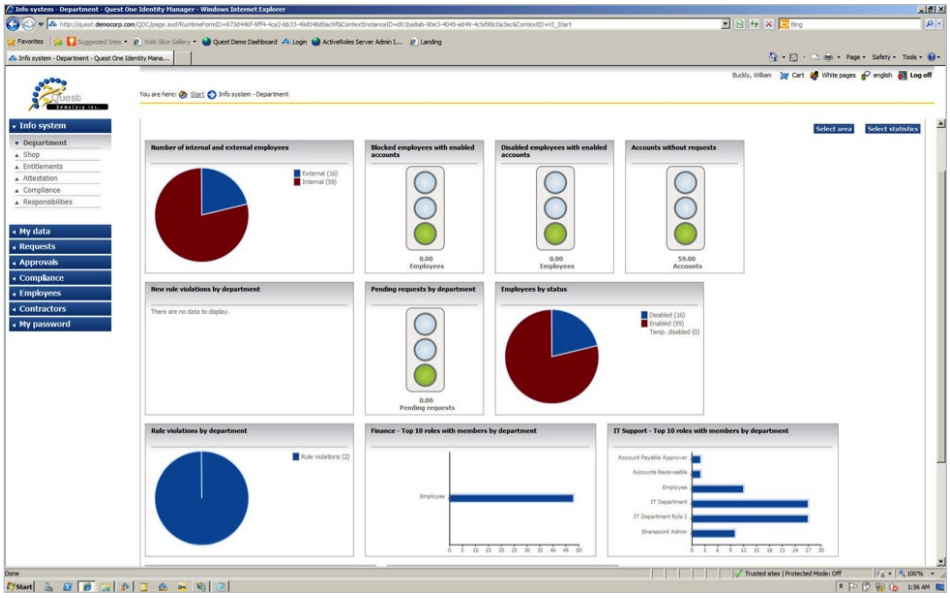

Figure 3: A manager's dashboard display can quickly show the number of employees, roles, and whether there are any concerns, through the use of 'traffic light' graphics.

Some organizations have shifted attestation tasks to the application owners, but application owners who are asked to perform access certification usually lack the same details about access rights as business managers, and may also lack information about each employee's current role and access needs.

Many organizations rely on provisioning to address the challenges of access certification. However, the reality is that this doesn't work. Users inevitably get access to new programs and applications, but there's a lack of follow-through on removing that access.

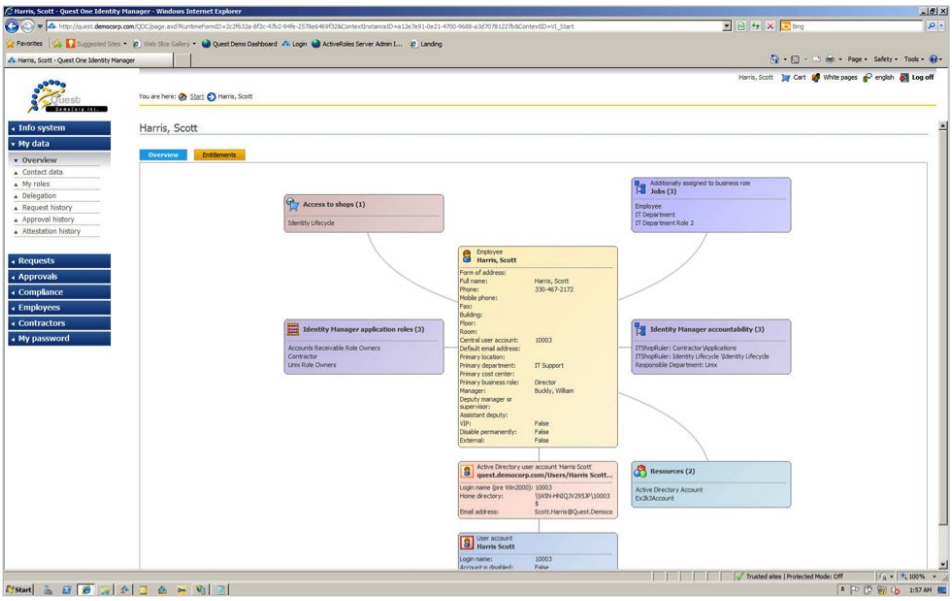

Figure 4: The entitlements screen displays a 360-degree view of all of an employee's entitlements.

in the organization and whether he truly needs access to \\DC7\C$\.

Lack of defined process

Many organizations rely on provisioning to address the challenges of access certification. Having a proper provisioning system in place to grant access and then remove it when an employee leaves, they reason, should eliminate the need for regular access certification. However, the reality is that this doesn't work. Users inevitably get access to new programs and applications, but there's a lack of follow-through on removing that access. The classic example is when an employee transfers within the company, as we saw earlier in the case of the Societe Generale trader; often an employee who changes roles within

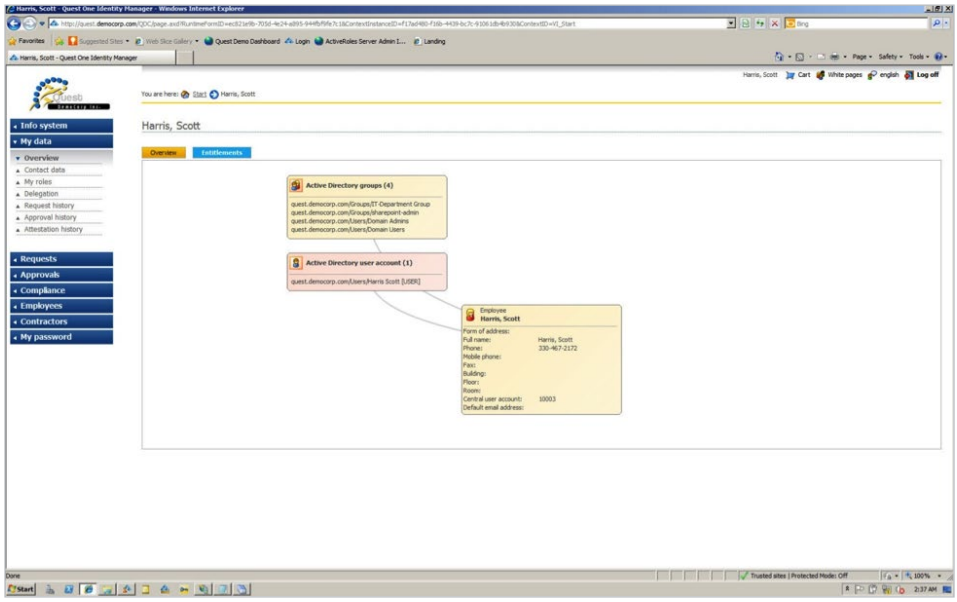

Figure 5: Details clearly show that employee Scott Harris is in the IT group, a SharePoint admin, a domain admin and domain user.

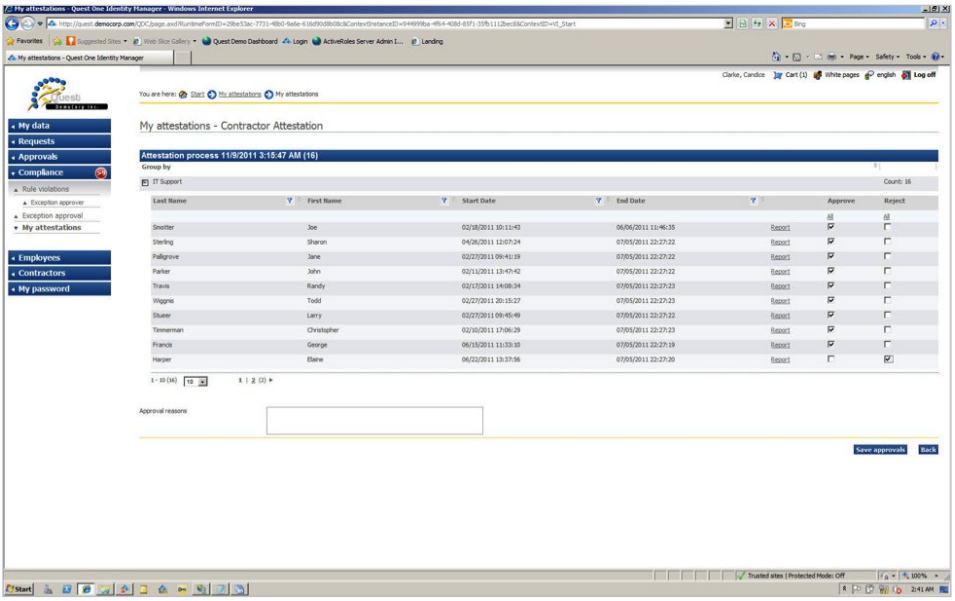

Figure 6a: The above example shows that manager Candice Clark is attesting to the fact that Elaine Harper is no longer a contractor on her team.

the organization retains his or her old access rights because no one even considers removing them. They are still an employee; what's the threat, right?

What is missing is a clearly defined, collaborative process between IT staff, who can see and understand the access rights of each employee, and the business managers, who are in a position to understand each employee's current role in the organization.

How to tackle the challenges of access certification

Every problem has a solution if you break it down into pieces. For access certification, the pieces are the following:

What is missing is a clearly defined, collaborative process between IT staff, who can see and understand the access rights of each employee, and the business managers, who are in a position to understand each employee's current role in the organization.

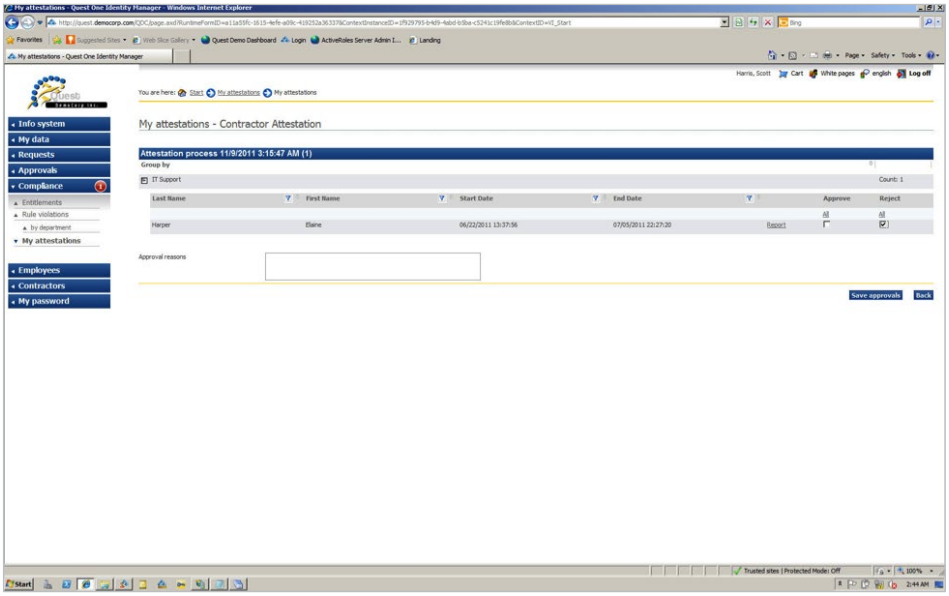

Figure 6b: Once Candice Clark attests that Elaine Harper is no longer a contractor, administrator Scott Harris receives an action to approve Elaine's removal. Once approved, this kicks off a workflow that immediately deprovisions Elaine's access.

The first step is to ensure you are conducting your access certification with an up-to-date employee list. If an employee no longer works for the organization, you can bet that HR was involved and will have ensured that he or she is no longer being paid, so the HR list should be the master list of current employees.

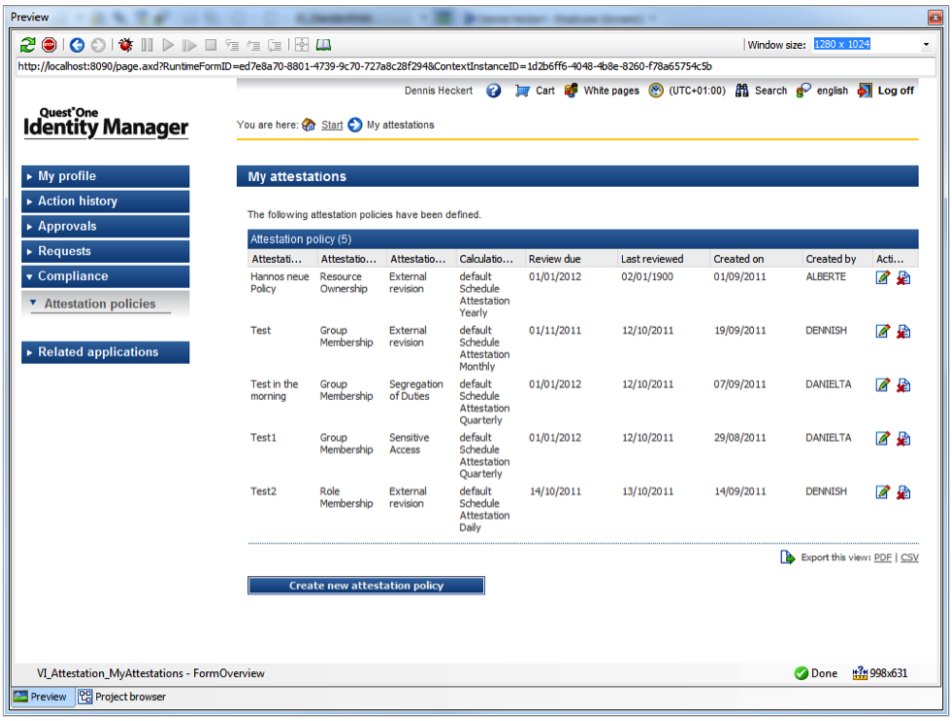

Figure 7: Auditors can establish regular attestation policies to occur on a regular basis.

Who: identify the organization's employee population

The first step is to ensure you are conducting your access certification with an up-to-date employee list. If an employee no longer works for the organization, you can bet that HR was involved and will have ensured that he or she is no longer being paid, so the HR list should be the master list of current employees. HR will also have a breakdown of the reporting structure to identify the managers for attestation purposes as they should be the ones doing the attestation because they understand the employee's role.

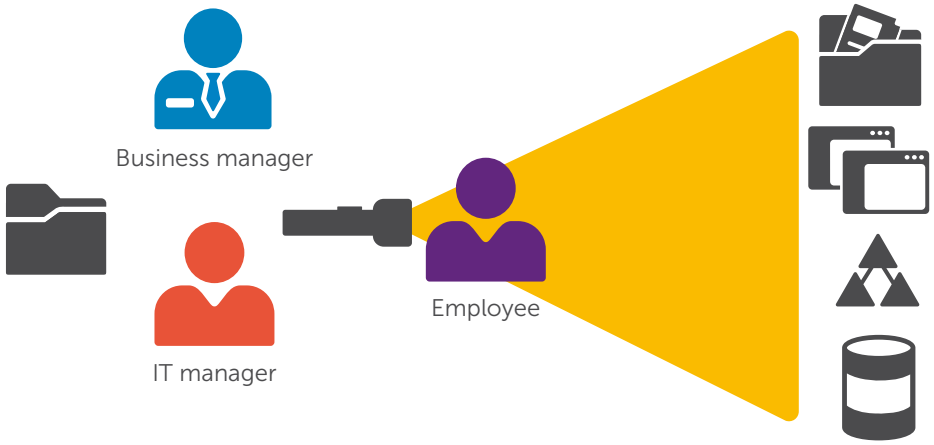

Figure 8: With the right tools, both the business manager and the IT manager can have a clear view of what each employee has access to and can make informed decisions about access certification.

What: identify the entitlement descriptions

The next step is to identify all of the potential entitlements in your environment. You'll need a detailed listing of each entitlement, along with a list of which employees have access to each. For many, this can be a time-consuming process as you will need to have each administrator responsible for each application, file share, etc. produce a list of all the entitlements and employees who have access for each. You may also have entitlements assigned by role or department; if so, this will need to be taken into account.

Interpret: 'translate' the entitlements into English

This is one of the most crucial steps to preventing blind attestation. As discussed earlier, a manager might be able to see that an employee has a particular entitlement, but doesn't understand the entitlement code. Instead of just assuming the entitlement is OK, the manager needs to understand the access being granted.

Attest: determine whether the user should have access

With a clear picture of who is being certified, what the current access rights are, and what each entitlement means (not just a code on a spreadsheet), the certifier is in a position to determine whether to attest to the current access or request modifications to suit the user's current role.

Conclusion

Access certification is a challenge at most organizations because of a lack of information, understanding and well-defined process: Business managers understand employees' roles but not their access rights; IT managers understand employees' access rights but not their legitimate access needs; and no process is available to facilitate collaboration between them. Since the blind attestation that usually results exposes the organization to serious risks, these challenges need to be addressed.

Dell One Identity solutions can address the divide and provide a clear, 360-degree view of employees and their access in a format that's easy to understand. With a clear process and the proper tools in place, organizations can save time completing their access certification reviews and ensure a more secure and compliant environment.

To learn more about Dell One Identity solutions for identity and access management visit software.dell.com/solutions/identity-and-access-management.

Dell One Identity solutions can address the divide and provide a clear, 360-degree view of employees and their access in a format that's easy to understand.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.