WHITE PAPER

8 Best Practices for Identity and Access Management

Introduction

Identity and access management (IAM) isn’t something you do once and then forget about. It’s an ongoing process, a critical part of your infrastructure that demands continuous management. Even if you have a fully implemented directory, it’s never too late to take advantage of best practices to help continuously manage this crucial part of your environment.

A key insight about identity and access management is beginning to emerge in our industry: contrary to common practice, IT should not be heavily involved in identity management. Too often, IT is placed in the role of “gatekeeper” simply because only IT has the tools needed to manage identity. But with the right identity management tools in place, IT maintains the tools and infrastructure, and the business controls the actual identities.

Here are eight key practices, gathered from years of experience and informed by this key insight, that will help you improve your identity management system to ensure better security, efficiency and compliance.

Eight best practices for IAM

1. Define your workforce

Your organization’s workforce is managed by your personnel or human resources department. They also have to manage information about people who are not employees, such as contractors and consultants.

ONE IDENTITY

Most of these people require access to company resources.

The first best practice is to use your HR systems as much as possible as an authoritative source of data for your identity and access management system. This will help you avoid repetitive work, errors, inconsistencies and other problems as the IAM system grows. Ideally, you'll provide some kind of managed front-end, such as a web- based interface that can be used to verify the quality of the imported data, revise data as needed and so on.

2. Define identities

The next best practice is to implement a single, integrated system that provides end-to-end management of employee identities and that retires orphaned or unneeded identities at the appropriate time. This is where IT responsibility formally begins in the identity management lifecycle. Typically, you'll identify the following:

- A primary directory service (often Active Directory)
- A messaging system (such as Exchange Server or Lotus Notes)
- A primary Enterprise Resource Planning (ERP) system (such as SAP)

Once identified, these crucial systems are integrated into the overall identity management architecture. Why focus on these three kinds of systems? Primarily because they deliver a "quick win," providing identity integration across the most-visible and most-used resources that users interact with on a daily basis. More systems can be integrated later.

In reality, each disparate system will continue to have its own user accounts. Your integrated system simply maps identities to these accounts, and you'll often use a web-based front-end to manage that mapping process. There will be invariably a few identities that can't be automatically mapped, and the front-end will allow those to be handled on an exception basis.

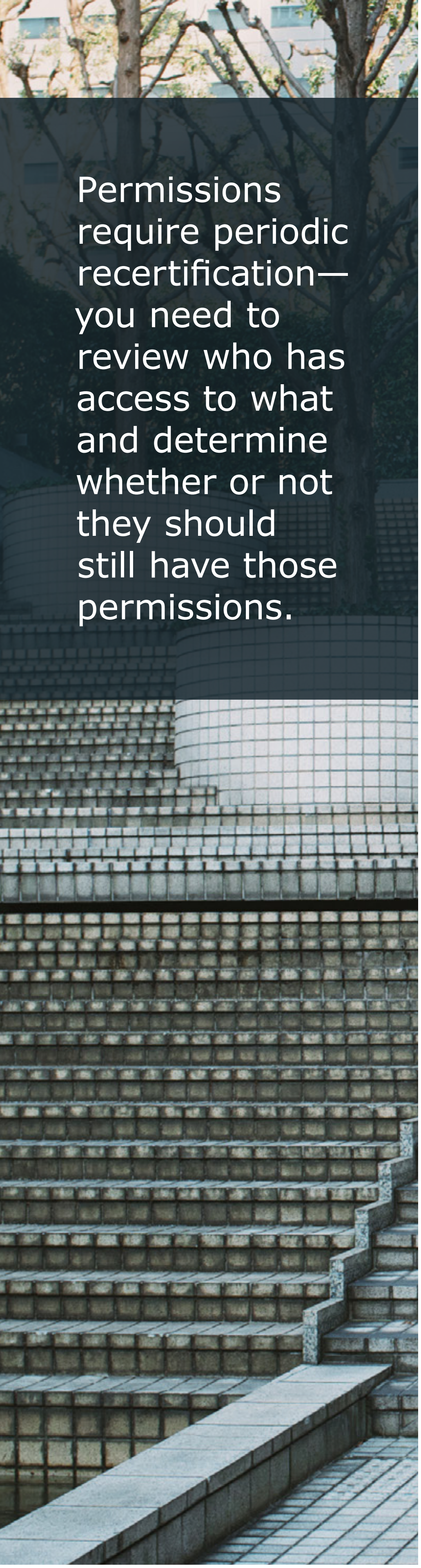
3. Provide knowledge and control to business owners

You also need to regularly answer the question, "Who has access to what?" IT coordinates the inventory of identities and permissions and provides that information to business data owners and custodians. Again, a web-based front- end is ideal for this. The idea is to let business data owners manage access to their data and to provide central reporting and control over those permissions.

4. Implement workflow

Although technology is always about embracing change, unmanaged change causes

Use your HR systems as much as possible as an authoritative source of data for your identity and access management system.



Permissions require periodic recertification—you need to review who has access to what and determine whether or not they should still have those permissions.

problems. Implementing a "request and approval" workflow provides an efficient way to manage and document change. A self-service user interface (often web-based) enables users to request permission to resources they need. Data owners and custodians can respond to these requests, helping the business ensure appropriate access, while removing IT from the decision- making role in permissions management.

You might begin by defining different kinds of permission sets, each with its own workflows. This enables different kinds of data and tasks to be treated appropriately, depending upon their sensitivity. Take the time to define who can control that list of services, who is responsible for managing workflow designs, and so on. For example, financial data might require more extensive approvals when changing permissions than company-wide information (such as details about the next company picnic), which might be changed with relatively little workflow required.

5. Automate provisioning

You need to manage new users, users who leave the organization, and users who move or are promoted or demoted within the organization. Provisioning, de-provisioning and re-provisioning are often time-consuming manual tasks, and automating them can not only reduce overhead but also reduce errors and improve consistency.

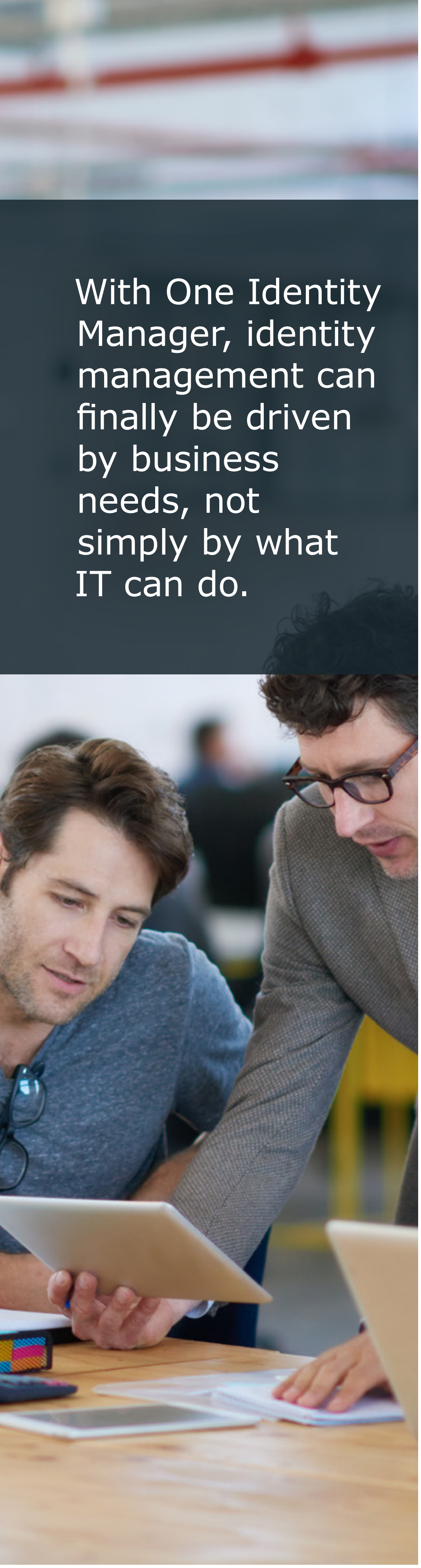
These provisioning tasks typically involve connections to numerous systems, including email, ERP and databases. Prioritize these systems so that the most important and visible ones can be automated first, and clearly define and document the flow of data between these systems and your identity management toolset. Focus first on automating the basic add/change/ delete tasks for user accounts, and then integrate additional tasks such as unlocking accounts.

6. Become compliant

Many companies are now affected by one or more industry or governmental regulations, and your identity management system can play a central, beneficial role in helping you to become and remain compliant. You'll need to focus on clearly defining and documenting the job roles that have control over your data, as well as the job roles that should have access to auditing information. Define compliance rules step by step, and assign each step to a responsible job role. Integrate rule checking in your identity management system and workflow operations to help automate remediation of incorrect actions; this will help improve consistency and security as well as compliance.

7. Check and recheck

In a well-designed identity management system, permissions are typically assigned to job roles rather than to individuals, but organizations are still likely to simply assign permissions as needed and never review them again. This practice invites security risks.


With One Identity Manager, identity management can finally be driven by business needs, not simply by what IT can do.

Permissions require periodic recertification—you need to review who has access to what and determine whether or not they should still have those permissions. Define job roles within your organization that can recertify permissions, such as system owners, managers, information security officers and so forth. Recertification can be defined in a workflow in which data owners and custodians review a current permission set and verify the accuracy (or inaccuracy) of that set. The idea is to regularly make sure that the roles and people who have permissions to resources should continue to have those permissions.

This process should also include recertification of job role membership to ensure that the users assigned a given job role are still performing that role within the organization.

8. Manage roles

Permissions are best assigned to job roles rather than to individuals. Making those roles correspond to real-life job tasks and job titles is a powerful way to manage identities and access over the long term. A certain amount of inventorying and mining will be needed to accurately identify the major roles within your organization, based at least, in part, on the resource permissions currently in force. Through user self- service IT shopping cart, users request access to the appropriate resources and services. This way, a user can

request access to "non-personal human resources information" (for example) without needing to understand the underlying technical details required to make that happen. Once a user places such a request, the owner or custodian of the affected data has the opportunity to review and either approve or deny the request—taking IT out of the permissions management loop entirely.

You'll also need to define who will manage these roles in order to ensure that roles are created,

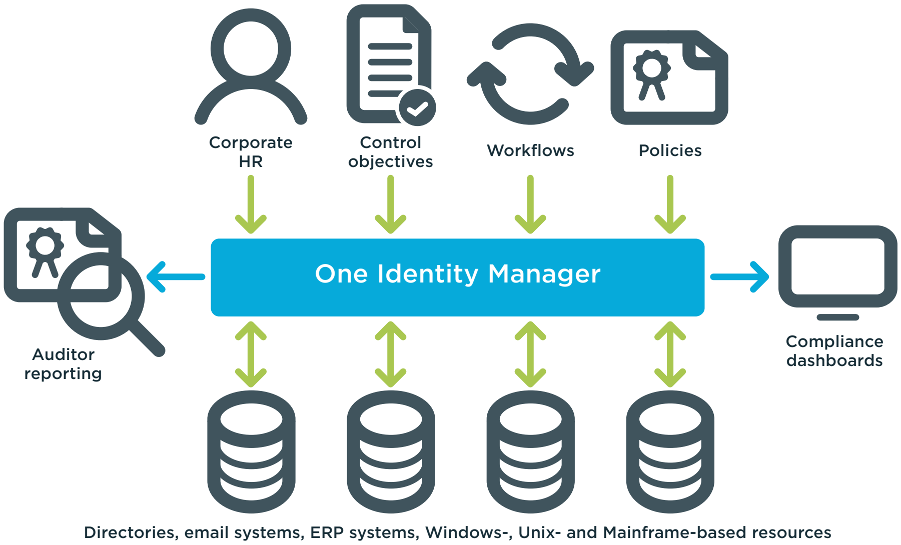


Figure 1. One Identity Manager provides comprehensive yet simplified identity and access management, which enables organizations to follow the eight best practices for IAM outlined in this brief.

modified and deactivated only by authorized individuals following the proper workflow.

Choosing the right tool

Traditional approaches

Unfortunately, it's unlikely that your business can rely on native tools to effectively implement these eight best practices. You simply have to deal with too many native toolsets, such as Microsoft Active Directory, SAP, PeopleSoft, Unix or Mac OS. You need a central place to manage the identities used by all of these systems, and you need to do so in a consistent, secure, efficient and controlled fashion. Traditional IAM frameworks are often expensive and require extensive implementation, often making them impractical.

Many companies instead opt for adhoc IAM, cobbling together home-grown and third-party tools into a disjointed workaround that basically gets the job done—but at a high cost in efficiency and security. Ultimately, identity management becomes driven by what IT is capable of, and not by what the business needs.

One Identity Manager

One Identity Manager, a part of the One Identity products from Quest, helps organizations achieve effective IAM for less money, and with markedly less effort, than previously possible. Employees enjoy full access to their applications, platforms, systems and data throughout their time with the organization, and your organization doesn't have to invest in long, expensive customizations or never-ending consulting engagements. You can even enable line-of-business employees to manage the identity lifecycle process through self-service, offloading IT overhead onto actual business data owners and custodians. One Identity Manager also provides full workflow, including separation of duties that are often lacking in IAM solutions.

With One Identity Manager, identity management can finally be driven by business needs, not simply by what IT can do.

For More Information

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

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

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (**www.quest.com**) for regional and international office information.

ONE IDENTITY™