Strategies to ensure success for your IAM project

The do's and don'ts of identity and access management

By Todd Peterson, IAM evangelist, Dell Software

DELL Software

Introduction

Identity and access management (IAM) is at the front lines of security. Yet for all its importance there are too many IAM projects that haven't lived up to expectations, took too long, cost too much to complete and even failed outright.

> Too many IAM projects haven't lived up to expectations, took too long, cost too much to complete and even failed outright.

But everything about IAM — controlling access, managing and securing privileged accounts, achieving governance — is so important that organizations keep hammering away at their IAM projects hoping that things will get better.

How can you do things differently and make sure that your IAM project doesn't become another wreck on the road to security and compliance? In this e-book, I'll describe the multi-faceted world of IAM and point out common characteristics of failed projects. Then, I'll introduce new thinking, new tactics and new approaches like Dell One Identity that can help you make sure your project succeeds.

Identity and Access Management 101

Let me start by quickly reviewing what IAM is:

Anything you do to make sure that people can get to the stuff they need to do their jobs.

That's it.

That boils down to the processes and technologies around three functions:

1. Setting up user **access** to applications, data and systems
2. Ensuring that the access given to that user is the access, or **privileges**, that user is supposed to have
3. Providing for oversight, or **governance**, to ensure that the organization and those who regulate it know what that access is and agree that it is appropriate.

IAM — the 3 pillars of functionality

Let me define the 3 pillars in more detail.

1. **Access management,** or the things you do to set up and maintain user access. This is the most commonly addressed area of IAM, including familiar concepts like single sign-on, provisioning and password management. You have to build out all other parts of IAM on top of access management. After all, if it's a struggle for you just to grant your users appropriate access, then IAM is never going to be more than a tactical, operational exercise for you. Many IAM projects fail at this basic level.

> If it's a struggle for you just to grant your users appropriate access, then IAM is never going to be more than a tactical, operational exercise for you.

2. **Privilege management,** or the things you do to control access to the "superuser" accounts that are required for every system. The potential for problems with these accounts runs high for three reasons:
   - They are anonymous.
   - They are nearly unlimited in power.
   - It is difficult to assign individual accountability to the person using the account.

   Most major breaches are the result of compromised privileged accounts, and many organizations fail audits because of poor management of privileged accounts and users.

3. **Identity governance,** or the things you do to prove that the access granted to users is appropriate and within guidelines for security and compliance. One of the major components of a governance program is attestation, or recertification, which requires line-of-business personnel to periodically attest to the access rights possessed by all users who report to them. The major barriers to successful identity governance programs are a lack of access management (see #1 above) and over-emphasis on a single area, like user access to applications, to the exclusion of other important areas, like access to unstructured data and privileged accounts.

Thus, the essence of successful IAM lies in addressing all three pillars of functionality.

Why IAM projects fail

You may be saying, "I already do all this stuff!" My reply is, "Yes, you do. But how effectively do you do it?"

Are you sure that your people can access their stuff? Are you spending too much time and money providing and managing access? Is the access you're providing on par with organizational, regulatory and user expectations?

Here are the most common types of failed IAM projects:

Death by one-off, in which multiple solutions from multiple vendors provide similar functionality, but in multiple pockets of the infrastructure. Think, for example, of all these solutions running in the same organization:

- A manual process for provisioning Active Directory with native tools
- A highly customized provisioning framework for the rest of the enterprise
- A purchased solution for authentication to federated applications
- A home-grown solution for authentication to internally-developed applications
- Another home-grown solution for single sign-on to legacy applications
- A manual process for privileged password management
- A dedicated Active Directory bridge for some UNIX privileged account management tasks
- A self-service solution for resetting user passwords

Are you spending too much time and money providing and managing access?

One size fits some, in which the organization engages a big platform vendor for an enterprise solution that, at first glance, will meet all of its IAM needs. But a few years into the project the organization finds that it is still performing too much of its IAM manually, buying too many point solutions with siloed functionality and pumping in too much effort with no end in sight.

Provisioning only. The lynchpin in any IAM program is provisioning, or the processes that provide the access for both standard and privileged users. Yet provisioning is often the most time-consuming, error-prone and disjointed IAM activity, and if the organization can't be certain that each user has precisely the correct rights across each system, then it will not achieve good governance. Most traditional IAM solutions from big platform vendors focus on provisioning, but because they are complex, custom-built and expensive, they are often the poster children for failed IAM projects.

You may be able to see yourself in at least one of those scenarios.

The consequences of a poorly executed IAM program

So what does the fallout from an IAM failure look like?

Inefficiency — Basic access management duties take too long, require too much IT involvement and are done too inconsistently. How long does it take your organization to fully provision a new user with all necessary access rights? How many separate e-mails, phone calls, spreadsheets and processes are involved? How many separate IT entities does it affect? Your users should be fully provisioned the minute they start, with a single request and fulfillment action, and IT should be involved only if something goes wrong; otherwise, you are probably at some stage of a failed IAM project.

Audit exposure — When the auditor comes calling, do you head for the hills? If it is difficult for you to gather, deliver and interpret information for an auditor, your IAM was likely a failure. And if the audit requires lots of IT staff to perform lots of manual tasks while their real job goes undone, it was certainly a failure.

> Your users should be fully provisioned the minute they start, with a single request and fulfillment action. Otherwise, you are probably at some stage of a failed IAM project.

Living on a prayer — When there is a disjointed, heavily IT-dependent, multi-siloed approach to IAM, business stakeholders must hope that everything is going well. An undeniable sign of an IAM failure is not knowing about a problem until it is too late.

Inflexibility — If you had to manage access to a new, business-enabling application with very little notice, could you? If a BYOD flood hit your company, could you handle access for all those devices? If dealing with that kind of change is difficult (or impossible) and requires more new IAM solutions, more IT involvement and more siloed approaches, your IAM project is not likely successful.

In short, a number of factors can get in the way of a successful IAM project:

- Maintaining manual processes
- Dealing with issues only as they come up and only in silos
- Relying too heavily on customization
- Choosing the wrong technology
- Inability for organization to adapt to change
- Improperly scoping the project
- Dumping everything on IT, including things that the business should be dealing with
- Keeping end users and line-of-business managers from performing access management tasks – in other words, a lack of self-service
- Letting complexity get out of control and attempting to solve the problem by adding even more complexity.

You’re not alone. Plenty of your peers struggle with IAM.

IAM projects bedevil companies in many different industries.

One Fortune 100 company believed its only option was to invest heavily in a customized IAM solution from a large vendor. The company engaged 16 Java developers to custom-build connectors for provisioning and de-provisioning users across hundreds of applications. Two years into the project, this army of developers had succeeded in building only one connector and was able to provision users to Active Directory, but could not de-provision them.

The technology company realized that it had three full-time employees tasked with simply filling the provisioning gaps left by its customized solutions.

A major bank had a set of 12 UNIX-based applications used every day by every teller. As a result of integrating these applications with the bank’s large IAM framework, each teller had to remember 12 passwords. The cost of resetting the passwords the tellers forgot was more than $1 million per month.

A large technology company spent years with major IAM vendors on two failed projects for provisioning more than 100,000 users. One day, the company realized that it had three full-time employees tasked with simply filling the provisioning gaps left by its customized solutions.

A document management company successfully implemented a framework for provisioning, but then found out how much time and money it would take to add other needed IAM functions. It was compelled to shop for other products for managing single sign-on, passwords, Active Directory, UNIX directories, privileged accounts and governance.

Three months into a 12-month IAM project, an energy company was barely able to provision and still unable to perform governance. The vendor was acquired by another vendor that recommended an entirely new, equally expensive and potentially longer project to accomplish the same things, minus governance. Meanwhile, the costs the company incurred to maintain homegrown applications were becoming excessive.

Do you see your company in any of those five examples?

The recipe for IAM success

But … there is hope.

A growing number of organizations are finding that, with the right approach, IAM can go from a necessary evil to a business-enabling asset. For these organizations, the utopia of users having what they need to do their job (access); every user having exactly the right access (provisioning); all the right people making it happen and knowing what goes on (governance); and a unification of all of those is much closer to reality than they thought possible.

> When line-of-business managers decide who should have access to what, and when they can provision on their own, everything gets easier.

Here are a few common characteristics — a basic recipe for IAM success — that we can draw from successful projects:

- **Unify, unify, unify.** The more identities people have, the more places they must be provisioned, the more passwords they can forget, and the more holes an audit can find. Seek to arrive at a single source of the truth and then implement it enterprise-wide. And don't forget that two or three passwords are still much better than ten or twelve of them.
- **Minimize customization as much as possible.** The more you can use configurable IAM solutions, the sooner you will realize value, the easier it will be to react to change and the less money you will spend on an army of developers and consultants.
- **Get provisioning right.** Make sure that you provision, re-provision and de-provision users in an entirely unified and consistent manner. Unifying and minimizing customization are a big help in getting provisioning right.
- **Put the business in charge.** When line-of-business managers decide who should have access to what, and when they can provision on their own, everything gets easier. IT doesn't need to be involved, audits are less painful and the organization is more secure.
- **Automate and enable.** Manual processes indicate an unsuccessful IAM project as much as customization does, so as you follow this recipe, look for places where automation can save time and money. Automation also decreases the likelihood of error and can enable the line-of-business staff to do many things they rely on IT to do.
- **Always look forward.** If you think of your IAM project as a static situation at a specific time, you'll have trouble adapting to the constantly evolving world of users, access needs, compliance demands and security threats. Approach your project with a "what if … ?" mindset. While you can't predict everything, keep your eye on whether your IAM solutions will fit into your environment, whether they are cloud-ready, how they support trends like BYOD and how they conform to industry standards.

Happy endings

To return to the five projects I described earlier, four are well on the path to IAM success.

The password-challenged bank consolidated all UNIX identities and logins to take advantage of the existing, ubiquitous Active Directory logon. That virtually eliminated the $1 million-per-month burden of resetting its tellers' passwords.

The technology company implemented a configurable provisioning and governance solution. It achieved all of its objectives in a few months, instead of the few years the failed project had taken. The senior manager for identity and directory services at the company says, "Now we have a global, intelligence-driven IAM platform for access governance that ties our people's identities, permissions and roles to business rules." (Read the entire story here.)

The document management company continued to build IAM functions on top of its framework for provisioning, always emphasizing interoperability, adherence to standards and reduced complexity. Eventually, the futility of maintaining the custom solution became obvious, so the company implemented a future-proof provisioning and governance solution.

The energy company implemented the same provisioning and governance solution as the technology and document management companies. In 14 weeks the company achieved what it had failed to do in three years with the previous solution. The director of information security at the company reports, "The time savings has been remarkable. We can now auto-provision 50 percent of our application tasks." (Read the entire story here.)

In 14 weeks the company achieved what it had failed to do in three years with the previous solution.

Each of these projects followed the recipe for IAM success and used the Dell One Identity family of products.

About Dell One Identity

Dell One Identity is a multi-award-winning family of solutions built on the three pillars of IAM functionality:

- **Access management** to help organizations ensure that all users can get to the resources they need to do their jobs from any location and any device in a convenient, secure and compliant manner. Use cases for Dell One Identity in access management include Web access management; single sign-on and federation; directory and identity consolidation, migration and management; strong and adaptive authentication; and password management.
- **Privilege management** to empower organizations to manage privileged accounts centrally with individual accountability through granular control and monitoring of administrator access. Some of the important capabilities available from Dell One Identity for privileged management include enterprise privilege safe, least privileged access; session management and keystroke logging; Active Directory bridge; and separation of duties enforcement.
- **Identity governance** to help organizations achieve complete, business-driven governance for identities, data and privileged access by marrying visibility and control with administration. Use cases of Dell One Identity for governance include automated enterprise provisioning; access, data and privileged account governance; business-enabled access request and fulfillment, attestation and recertification; role engineering; identity unification and process orchestration; and context-aware security.

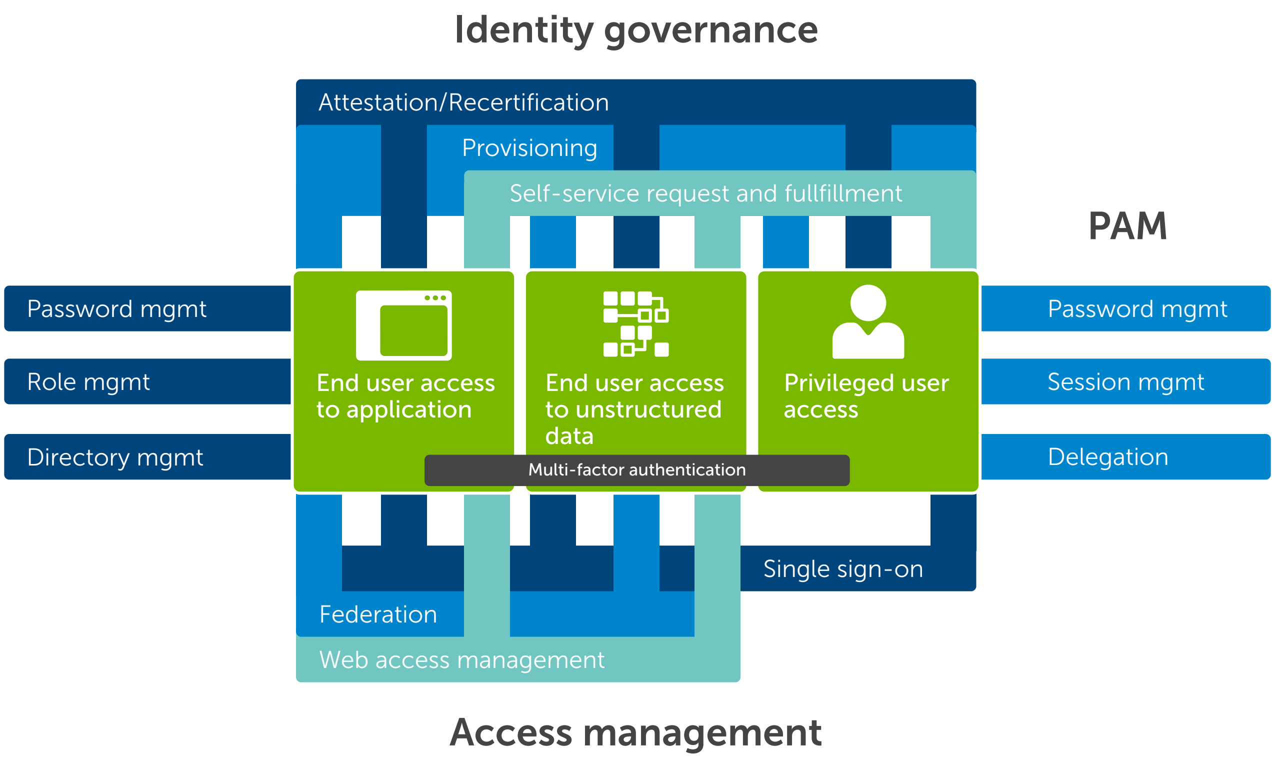

Figure 1: Dell One Identity provides access management, identity governance and privileged management for the widest range of user types and access scenarios

Many vendors offer solutions similar to pieces of the Dell One Identity family, but none offers the breadth across all areas of IAM or the success-enabling features explained in this e-book. Consider the unique, powerful and business agility-enabling benefits of Dell One Identity:

1. **Designed for governance** – All Dell One Identity solutions provide governance as an integral part of the overall solution, not as an afterthought or a poorly integrated add-on.
2. **Business-driven** – From access request and fulfilment to unified policy and enforcement, Dell One Identity solutions place the power in the hands of those with the most at stake — the line of business.
3. **Future-proof** – Unlike other IAM products, Dell One Identity solutions do not require extensive customization. Their configurable approach means that the constant flow of change is easily, quickly and completely addressed in a fraction of the time and at a fraction of the cost of traditional IAM frameworks.
4. **Modular and integrate**d – Dell One Identity solutions do not require an underlying technology framework, often the cause of failed IAM projects. With Dell One Identity you can start anywhere and build with a wide range of solutions that easily plug into existing technologies and one another.
5. **Ready to deliver value** – This all adds up to an IAM approach front-loaded for success. With Dell One Identity you deploy in weeks not years, you streamline and automate the tasks that previously were so difficult, you relieve the burden on IT and ultimately you save money while enabling business agility.

To learn more

Find out more about the Dell One Identity family of IAM solutions at software.dell.com/solutions/identity-and-access-management/

For an in-depth look at IAM, read the e-book Identity and Access Management for the Real World: The Fundamentals. And stay tuned for more e-books in this series. I'll cover the entire range of IAM projects:

- Identity governance
- Access management
- Privileged management

The information in this document is provided in connection with Dell 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 Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell 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. Dell does not make any commitment to update the information contained in this document.

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.Dell.com
Refer to our Web site for regional and international office information.