Strategies to ensure success for your governance project

Governance – The elusive last mile of identity and access management (IAM)

By Todd Peterson, IAM evangelist, Dell Software

Introduction

When IT professionals talk about identity and access management (IAM), governance now dominates the conversation.

In years past when we talked about IAM, the hot topics were provisioning, single sign-on and role-based access control. But we must have gotten bored with those stale topics and needed something new to focus on.

It makes sense. If you think of IAM as a maturity model, similar to Maslow's Hierarchy of Human Needs, the IAM of days gone by would be at the base of the pyramid and the governance of today would be at the apex, as shown in Figure 1.

> If you think of IAM as a maturity model, the governance of today would be at the apex.

Governance may be cooler, newer and more "self-actualized" than the IAM staples of access management and provisioning, but that doesn't mean that these components are any less important to a successful IAM project. However, governance is the goal, and many organizations are finding it hard to reach.

Why is that?

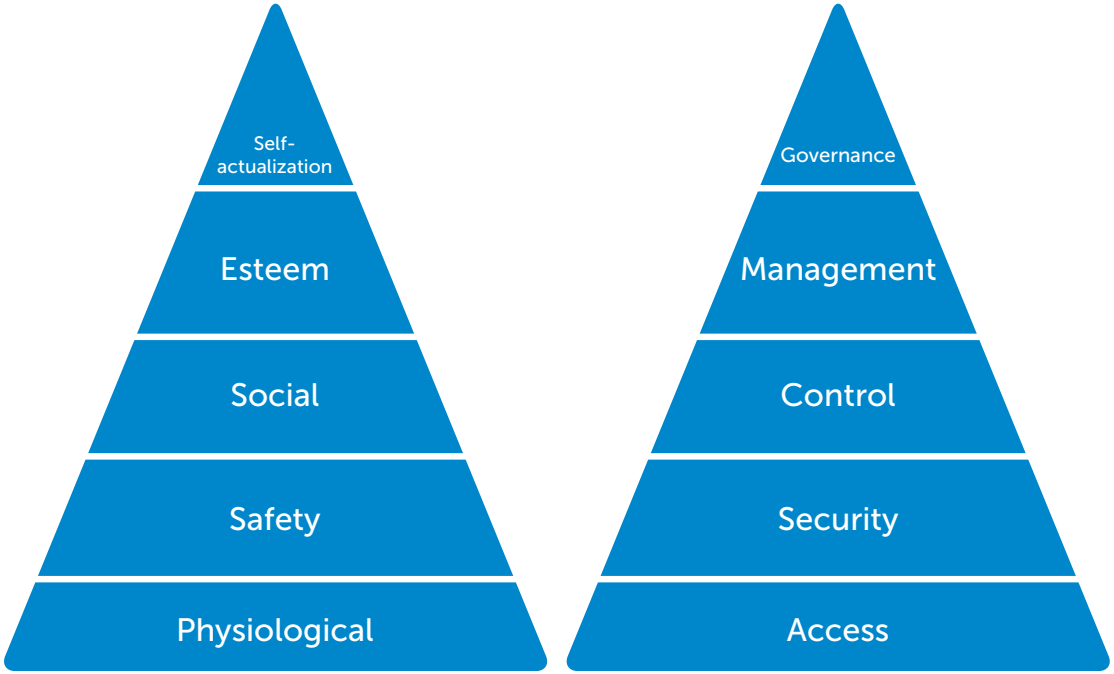

Figure 1: Maslow's hierarchy and the hierarchy of IAM needs.

What is Identity and Access Governance (IAG)?

Gartner defines the combination of identity governance and administration as follows:

"Identity governance and administration (IGA) solutions manage identity and access life cycles across multiple systems. Core functionality includes automated provisioning of accounts among heterogeneous systems, fulfillment of access requests (including self-service), password management, governance over user access to target systems via workflows and automated policies, and access certification processes. Additional capabilities often included in IGA systems are risk scoring of a user's combined entitlements, segregation of duties (SOD) enforcement, role management, role mining, audit case incident management, and analytics (historical change, performance, recommendations for entitlements or certifications, and so on).[1]"

In other words, while identity administration pertains to granting and maintaining access, governance is the process of ensuring that access is correct and auditable, and that it follows the rules, be they internal policies, best-practices frameworks or regulatory requirements.

Governance is the process of ensuring that access is correct and auditable, and that it follows the rules.

Think of governance as ensuring that:

- the right people
- have the right access
- to the right stuff
- at the right time
- in the right way

and that all the right people know about it and agree that it is right.

That's a lot of "rights" — which may be why IAG projects often go so wrong.

[1] Felix Gaehtgens, Brian Iverson, Steve Krapes, "Magic Quadrant for Identity Governance and Administration," Gartner Inc., January 12, 2015, https://www.gartner.com/doc/2960417/magic-quadrant-identity-governance-administration.

Why IAG is important

Organizations wouldn't focus on governance if it weren't important, But many question why they need an IAG program when identity administration is difficult enough.

Here are four main reasons for IAG, based on years of our interaction with real-world organizations like yours. This is a combination of reasons provided by potential customers and internal justification by security teams to get executive buy-off for an IAG expenditure.

Reason #1: Risk is everywhere

Everyone has a different mix of applications, a different set of user requirements and a different set of "crown jewels" that must be protected, but all require that protection. IAG ensures that the proper protections and controls are in place to remove as much risk as possible.

IAG ensures that the proper protections and controls are in place to remove as much risk as possible.

A common question is, "Aren't we already protecting everything with passwords, role-based access control and all the rest?" The answer is, "Yes you are, but do you even know who can access what? How can you prove it?" Anyone who has attempted an enterprise-wide access recertification exercise knows how long it takes and how the information it yields can be inaccurate or incomplete.

If done properly, IAG places a unified umbrella of governance over all that difficult-to-quantify access, resulting in significant gains in efficiency, major improvements in security and an enhanced ability to satisfy compliance and audit demands.

Reason #2: Too many siloes

Siloed identity stores and their corresponding collections of identities, workflows, authorizations and policies hamper security and disrupt business operations. By approaching IAG on a point-by point basis it becomes nearly impossible to quantify and manage risk for four reasons:

1. The very thing the organization is trying to govern — individual user access rights — stretches across disparate, unconnected systems with no auditable view of access rights and no automated, policy-based way to modify those rights.
2. There is no way for systems to verify user identities consistently through a unified identity store.
3. Conflicting identity attributes in siloed, unconnected systems result in disruption to business operations.
4. Different teams in IT use different tools and processes to perform roughly the same governance task in their domain but no other.

Reason #3: Blind or no attestation

A critical activity that governance demands is the periodic attestation (sometimes called recertification) by line-of-business managers that employees, contractors and vendors actually need the access they have been granted to applications, systems and data.

Business agility plummets when users have been under-provisioned and cannot access the network assets they need. At the other extreme, risk skyrockets when users have been over-provisioned with rights beyond what they need. (This often happens as a result of ad hoc intervention to correct under-provisioning errors.) When separate IT teams try to impose governance on this provisioning across silos, the result is a confusing jumble of spreadsheets that line-of-business managers are lucky to have the time to study, let alone understand.

Those managers must resign themselves to saying, “I trust that everything is correct. After all, we haven’t had an incident.” This is blind attestation — a big red flag for auditors.

Those managers must resign themselves to saying, “I trust that everything is correct. After all, we haven’t had an incident.” This is blind attestation — a big red flag for auditors. Either you get out in front of the problem with an IAG program that you drive, or you let the auditors discover your blind attestation and promise them you’ll solve the problem shortly.

Reason #4: Provisioning is a mess

IAG boils down to ensuring that access to resources is done right in your organization. The lynchpin that makes or breaks any IAG program is provisioning.

If your organization provisions accurately, correctly and completely, then all access rights will be correct and governance will be easy. Conversely, if provisioning is a laborious process of phone calls, e-mails, spreadsheets, forms and assumptions that one user’s rights are correct and her peer needs the same rights, it becomes difficult to prove that access to stuff is done right in your organization.

Implementing an IAG program on a broken provisioning foundation will result in frustration, failed audits and increased risk. But governance can be a driver to correct the underlying flaws in identity administration. Welcome side-effects would be increased security, gains in efficiency and IAM as an enabler of business agility, not a barrier.

Why do IAG projects fail? A final word from Gartner on why these programs are critical:

“Through 2016, enterprises without formal IAM programs will spend 40% more and experience twice as many IAM project failures than enterprises with such programs.”[2]

[2] Brian Iverson, Steve Krapes, “Horror Stories: Why IAM Programs Fail,” Gartner IAM Summit 2014, December 2, 2014, http://www.gartner.com/technology/summits/na/identity-access/agenda/tracks/track-1.jsp

Making your IAG program successful

As you face the need to implement governance in your IAM program, several strategies can improve your chances of success. The following recommendations map closely to some of the previously-cited reasons for needing IAG.

Mature methodically

Let's return to the comparison of IAM to Maslow's Hierarchy of Human Needs. Just as self-actualization cannot be achieved when foundational pieces of the hierarchy – such as physiological and social needs – remain unfulfilled, a jump to governance without management and control is destined for failure.

If you are being pushed to address governance, wisdom suggests focusing on the foundation first. Implementing management and control across the board will make governance a natural byproduct. However, if you attempt governance without addressing those foundational aspects, your effort will be full of holes and inconsistencies, and fail to deliver the objectives that justified the investment in the first place.

If you attempt governance without addressing foundational aspects, your effort will be full of holes and inconsistencies.

Unify and streamline

Silos are the biggest contributors to a failed IAM or IAG project. To assess how siloed your approach is, simply evaluate the process of provisioning a new employee. The more processes and IT staff that are involved, and the longer it takes to get the new employee fully provisioned, the more siloed you are.

As noted above, silos make attestation/recertification nearly impossible. However, governance immediately becomes easier in these circumstances:

- A single provisioning action can set up access for a new user on all systems.
- That action can base access on a unified policy that includes all the appropriate rights.
- The processes occur automatically upon request from the line of business.

In other words, get provisioning right first.

Line-of-business managers can verify that they completely affirm the attestation, which is based on sound principles in a language they understand.

Put the business in charge

In blind attestation, the line of business relies on IT (usually a lot of different people in IT) for the information regarding access and then the line of business performs the attestation . Unfortunately, IT usually provides information that is unintelligible to the line-of-business manager. Rather than ask for clarification or "translation" of IT-speak, the manager simply assumes it is correct and makes a blind attestation.

Suppose, on the other hand, that access rights are based on a unified definition of who people are, and which roles should access which resources. Suppose that the line of business has a hand in creating the definition, and executes the provisioning action through the correct tool. In that scenario, the line-of-business managers are verifying that they completely affirm the attestation, which is based on sound principles in a language they understand.

Govern everything

The requirement of IAG is to provide insight into and verification for access. That is a universal requirement, not limited to specific types of access, users or systems. Unfortunately, it is tempting to address governance with the same siloed approach that causes so many problems with identity administration, putting out one fire at a time with whichever tool seems to be the best.

Governance applies to three main types of access:

1. User access to applications
2. User access to data (typically unstructured data)
3. Privileged user access to administrative accounts and "superuser" credentials

Best practices point to an IAG solution that will cover all three types of access: end user access to applications, end user access to data, and privileged user access to administrative accounts

If each type of access is addressed only as it rises to the top of the auditor's list and with separate tools, expenses spiral out of control and the actual work of governance triples. So, best practices point to an IAG solution that will cover all three types of access. Eventually, the auditor will examine all of them.

To summarize, the four components of a successful IAG program are:

1. Start with the operational activities that control access.
2. Get provisioning right.
3. Move as much into the hands of the business as possible.
4. Use a unified approach that covers users, data and privileged accounts.

Dell One Identity for successful IAG

The Dell One Identity family of IAM solutions includes a business-driven, future-proof, modular and integrated offering for IAG that delivers each of the ingredients for success.

Dell One Identity Manager marries provisioning to governance to put the right people in charge and make readily available the information necessary to achieve governance. While most governance solutions either do not offer provisioning or do so only as an afterthought, Dell One Identity Manager has been engineered with provisioning from the ground up.

Dell One Identity Manager solves blind attestation with rights defined at the business level and tracked throughout their lifecycle.

That means that an attestation activity can be as simple as line-of-business managers calling up a dashboard, reviewing the rights over which they have stewardship and verifying their accuracy. They do not need to pull an IT administrator away from important work to provide information that they may not understand anyway.

Dell One Identity Manager solves blind attestation with rights defined by the business and tracked throughout their lifecycle. It puts you in the driver's seat in case of an audit.

The single governance foundation in Dell One Identity Manager can cover user access to applications, user access to unstructured data and privileged access. It uses a single set of interfaces, policies, provisioning workflows, roles, identities and attestation activities. For organizations lacking the personnel or expertise to implement governance in-house, Dell One Identity Manager is available as a service.

Dell One Identity Manager was named overall leader by KuppingerCole in its comprehensive review of IAG products.[3]

To learn more

To learn how you can finally get a handle on identity and access governance, visit software.dell.com/solutions/identity-governance.

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 that will cover the entire range of IAM projects:

- identity governance
- access management
- privileged management projects

[3] Martin Kuppinger, "KuppingerCole Leadership Compass, Access Governance," KuppingerCole, October 2014, https://software.dell.com/whitepaper/kuppingercole-leadership-compass-access-governance-2014872605#.

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.

Ebook-StrategiesForYourGovernanceIAM-Part2-US-GM-25872