Identity and Access Management for the Real World: Identity Governance

By Todd Peterson
IAM evangelist, Dell Software
Introduction

In an ideal world, we’d have the budget and time we need to get things done. And tomorrow would be predictable. But that’s simply not the case, especially in the IT universe.

As you well know, the world of identity and access management (IAM) is one of constant change, shrinking deadlines, minuscule budgets, overtaxed staff and unmerciful regulations. Unfortunately, this historical approach to IAM involves piecing together “half solutions” in hope that tomorrow’s solutions will address real world needs.

This short e-book evaluates what IAM for the real world would, should and can look like. It delves into the most pressing IAM issues faced by virtually every organization and offers actionable, affordable and sustainable approaches to the challenges you face. With today’s heightened IT security and complexity, achieving identity governance is one area of IAM that presents unique obstacles. Here we’ll explore the root of the challenge when it comes to identity governance, and how you can move your organization closer to a unified model that encompasses application, data and privileged access. At Dell, we help you achieve your IAM objectives for your real world in a way that enables you and your business to achieve your goals.

I hope you find value in “Identity and Access Management for the Real World: Identity Governance.”
Conventions

Throughout this e-book, we’ve used a number of conventions to help highlight important points, provide supporting evidence, or advise you of our obvious bias. Look for the following conventions:

**Real-world example** – Stories of real organizations, facing real challenges, and really solving their problems (often the names have been changed to protect the innocent)

**Facts & figures** – Research-based information that supports principles discussed throughout the e-book

**Techie alert** – Definitions and terms used in the identity and access management industry that may not be familiar to you (Then again they might.)

**Useful tip** – Information that will help you easily achieve things discussed throughout the e-book

**Blatant sales pitch** – Where we get to why we actually wrote this e-book. It may be a little biased, but we suspect that the reason you’re reading this e-book is to find solutions to your challenges. This is where we give them to you.
"You go straight... down the hall, turn right... go about 30 feet, jog to the left... straight ahead... turn right for the next two corners... first door says ‘Authorized Personnel’... You’re musicians, aren’t you? Rock and roll... Hello Cleveland! Hello Cleveland!"

*Backstage maintenance guy, Derek Smalls, and Nigel Tuffnel*

“This is Spinal Tap” – 1984
Identity Governance – Governance leads to agility

How often do our efforts at governance seem like the futile attempts of the boys in the band to find the stage in the 1984 comedy, This is Spinal Tap? How often do those we rely on for governance seem to be speaking a different language? And how often do we, in spite of our best intentions and efforts, find ourselves wandering through the maze of our organization, hoping to stumble across the stage door that leads to our dream gig?

For our discussion, governance is defined as business-enabling activities that move technology beyond simple efficiency tools into the realm of confidently and correctly providing access and performing administrative activities. This also means all this is done with the full knowledge and endorsement of the organization, while satisfying any internal or external regulations. Providing all these requirements are met, governance acts as the framework for how those activities should be done.

Put simply, governance is ensuring that:

- The right people...
- Have the right access...
- To the right resources...
- At the right time...
- In the right way...
- With all the other right people knowing what’s going on and saying it’s okay.

In a perfect world, getting it right would be easy. The risks of inappropriate access or activity would be minimal because all of it would be controlled by the right people with complete visibility. Your organization could easily satisfy compliance requirements. If an auditor asks for information, or you need a periodic entitlement recertification, you could generate an accurate and user-friendly report with just a few mouse clicks. But, unfortunately, we don’t work in the perfect world. We work in the real world.

In the real world, governance is a major challenge. In fact, governance can’t even be considered until access, security, control and management have been achieved. If simply provisioning access is difficult, leveraging that access to enable business agility – the goal of governance – is impossible. If all your time is spent remedying a forgotten user password, for example, how are you going to ensure that the correct controls are in place so that the user had the appropriate access in the first place? And that’s just a couple of components of being compliant. The real challenge is proving compliance. It’s a complex situation.
Several key “governance” factors are involved in a typical audit. They may take different forms, but it all boils down to:

- **Provisioning** – making the process of thoroughly and correctly granting access across the entire environment as efficient as possible. This includes the more important security-related action of “de-provisioning.” While provisioning itself is an access management activity, without provisioning done right, governance is impossible.
- **Workflow** – showing the steps from access needed to request to fulfillment, ensuring compliant processes are followed throughout
- **Attestation** – fulfilling the periodic requirement to review all access entitlements (or rights) and certify their appropriateness
- **Policy** – documenting and enforcing the underlying rules that govern user access to applications and data, as well as showing that those rules comply with established regulations
- **Approvals** – ensuring all the right people approve access requests before it is fulfilled

While access management is primarily concerned with simply getting things done, governance addresses getting those things done the right way.

"96 percent of breaches were avoidable through simple or intermediate controls."

*Source – 2011 Data Breach Investigations Report, Verizon RISK Team with cooperation from the US Secret Service and the Dutch High Tech Crime Unit*

**The elephant in the room**

There’s an old story about a bunch of blindfolded people being let into a room with an elephant and asked to identify it based on only what they can feel with their hands. One felt the elephant’s tail and declared, “it’s a rope.” Another, feeling the elephant’s side stated, “It’s a wall!” The trunk was identified as a snake, the leg as a tree, the tusk as a spear, and the ear as a fan. We’ll pretend that none could smell or hear... but that’s beside the point. Each person’s perception of the elephant was limited to what they were able to experience directly.

Governance is similar.
It seems that the default approach to governance is limited to what an organization is experiencing at the time, or what they are able to most easily comprehend, measure and control. For many, governance may be confined to the narrow scope of satisfying the auditor’s finding of the day. For others, governance may be influenced by a specific security breach or incident. And to still others, governance may be focused on the organization’s “crown jewels,” those applications or data sets that are the most important to achieving business agility. All are absolutely appropriate and all are equally important. However, just like the elephant in the room of the blindfolded, a narrow focus will leave out critical pieces of the bigger picture.

Therefore, governance must be concerned with the whole of IT, not just the easy parts. Governance for the real world should be focused on:

- User access to all applications
- User access to all types of data
- Administrator access to all systems

**The root of the problem**

The challenges associated with governance are all too common in today’s highly complex and security-conscious landscape. Basically governance can be illustrated by a “closed loop” model.

"48 percent of respondents rated the odds of experiencing a compliance risk within the next 18 months as “high” or “very high.”

*Source – State of Compliance 2011, PWC*
As discussed earlier, each system requires access; therefore each system can be subject to governance. Access is the result of provisioning that is controlled by policy and streamlined through the use of roles or other attributes. Compliance demands attestation to the appropriateness of the access, which in turn feeds into continued maintenance of the identity lifecycle for continued access. The operable word here is “each” system.

The four fundamentals of IAM are authentication, authorization, administration and audit. Just as executing these four “A’s” across a diverse large mix of systems is the source of inefficiency, and ultimately security vulnerabilities, this same diversity (or complexity) makes approaching governance on an ad-hoc basis inadvisable. What do you start with, and what do you leave out? There are simply too many ingredients required to make the soup, and too many cooks in the kitchen.

The “real world” of governance for the vast majority of organizations looks like this:
- Many and varied systems (applications, data sources, capabilities, etc.) that users must access to do their jobs
- Too many different ways that access is granted
- Many different IT teams with too narrow an area of expertise
- Too little knowledge from the business of how these things work
- Too little knowledge from IT as to why they need to work in a certain way, and what the implications are if they don’t
- Too much reliance on “this is the way we’ve always done it”
- Too much blind verification ... “If Joe has the same access as Sally, it must be right...right?”
- Too much security policy developed by those that implement it (IT) rather than those on the hook if it goes wrong (the business)
- Too little visibility by the business into what access people have and how they got it

A real-world approach to application access governance includes prerequisites to governance like good provisioning, strong policy, adequate visibility, and a complete understanding of who can access what. All this would be tightly coupled with the ability for the right people to easily have access to the information they need.
need to do precisely that – govern. Only the Dell One Identity family of IAM solutions and Dell One Identity Manager provides these governance-enabling capabilities without the heavy overhead of a cumbersome and rigid framework, or the myopic inadequacy of a focus only on one area, one type of user, or one aspect of governance.

**Too many closed loops**

Many organizations take a stance that governance begins and ends with user access to applications. It’s understandable since applications are highly visible. Applications are most easily understood and have been targets for governance initiatives and vendor solutions for many years. And applications absolutely must be governed. But how many applications do you have and how many “closed loops” do you end up with? How many manual processes exist that put the IT team and line-of-business personnel on different pages? How difficult is it to provide even the most basic governance information?

![Figure 2: Traditional approaches to governance implement separate closed loops for each system or scenario that must be governed.](image)

In the real world, unifying governance for all applications can move you miles closer to agility. Ideally, you want them to be tied to an equally unified enterprise provisioning approach with a single source of the truth for policy, workflow, roles and approvals.

![Figure 3: A unified approach to governance provides a single closed loop that encompasses all access needs.](image)
But applications are only part of the story. A very large percentage of data at any organization can be classified as unstructured.

Unstructured data exists outside of the strictly organized confines of a database. Unstructured data can be spreadsheets, PDFs, videos, audio files, PowerPoint presentations or Word documents.

These can contain benign information that’s not governance demanding, but very often they contain critical data regulated by compliance. For example, spreadsheets that contain personally identifiable information such as Social Security Numbers, birthdates and addresses must be governed. Proprietary information, such as trade-secrets, plans and financial performance, often exists in PDFs and PowerPoint presentations. Unfortunately unstructured data exists in myriad places – many outside of the control of IT. File shares, NAS devices, and SharePoint sites may contain sensitive unstructured data. In many cases, the best an organization can do to govern these resources is to roughly control access to the server or file share itself – a lowest common denominator approach that either is too restrictive for efficiency, or too lenient for compliance.

So governance of access to unstructured data often follows the same path as application access governance: disjointed, nonexistent, manual or inconsistent. Bottom line, doing the best you can with what you have is not good enough. Our closed loop governance model reflects the challenges of provisioning, providing appropriate access and attestation. These challenges are magnified as the diversity of locations for unstructured data expand and more of those locations slip out of the control of IT – the ever-popular SharePoint gone wild! In some areas closed loops exist. In others they don’t.

Figure 4: It is difficult to implement a closed loop governance model on disparate sets and locations of unstructured data.
The number of circles representing governance of unstructured data could be much larger than those representing application access. And the potential for rogue storage locations, non-governed access permissions and sensitive data being innocently put at risk is extremely high.

In the real world, it makes no sense to address governance of unstructured data independently of application access. The users are the same, the roles that should control access should be identical, and the line-of-business personnel that are on the hook to attest to access don’t change when the app or data being accessed is different or more difficult to govern.

Privileged accounts—such as the Unix root account, an application administrator account, or the superuser account required to administer any system—are a governance nightmare. Their high level of access rights, their anonymous nature and the lack of visibility makes them high risk.

If governance of unstructured data is difficult, then governance of privileged access is nearly impossible when approached in the disjointed manner so often applied to shared superuser access. Application access has matured to the point that, if you want governance, you can get it. Data governance is in a similar state, though less visible. However, the vast majority of privileged account activities are mired at the access and security levels of the hierarchy, barely dipping their toes in control or management. Governance for privileged access struggles to achieve a closed-loop model.

![Figure 5: Governance for privileged access typically struggles to achieve a closed-loop model.](image-url)
Governance for privileged access is often the realm of “we have controls in place, but we can’t prove that they are working.” Many organizations are able to control the issuing and use of superuser credentials, and some are even able to watch what is done with those rights. Yet true governance activities of provisioning, attestation, and reporting are done manually in silos by the very people they are meant to govern at best. At worst, they are ignored altogether.

But administrators are people too. They have roles. They have identities in systems. They have polices that are meant to control what they do. And they have supervisors that are required to attest to their access rights. Auditors don’t give you a pass just because those accounts are more difficult to govern, or you don’t have the tools to make what you have to do any easier.

A real world approach to privileged account governance unifies those things that control access, such as roles, identities and policies. It accomplishes this with tools that enable the line-of-business to understand, control and attest to appropriate administrator access across the entire range of systems.

A unified, real-world approach to identity governance would be able to govern user access to applications, user access to unstructured data and administrator access to systems. It would look like this:

![Diagram showing unified governance approach](Diagram.png)

*Figure 6: A real-world approach to governance would encompass application access, data access, and privileged access in a unified manner.*
A few important action points can be learned from viewing governance in a holistic way:

- Move as much of the control, decision making and visibility required for governance away from IT and onto the business to solve many problems.
- Reduce the number and disparity of points of audit to increase accuracy and accelerate compliance.
- Avoid blind verification.
- Involve the business in the development and execution of policy – IT knows how to do things, but isn’t paid to know why they are done.
- Integrate provisioning, access request, recertification/attestation and compliance reporting tightly as possible.
- Remember the entire range of access when dealing with governance – it’s about identities and accounts, applications and data for both general users and privileged users.

Identity governance for the real world takes into account the complexity of organizations, the merciless nature of compliance, the heavy workload of both IT and line-of-business personnel, and the understanding that governance is an ongoing journey and not a final destination. A real-world solution for identity governance will empower the business to own governance. This capability is sorely missing in most legacy IAM framework solutions.

An international oil and gas exploration company had big challenges when it came to access governance. The company’s requirement to share information with partners was proving difficult to achieve without placing sensitive information at risk. Efforts to restrict access through traditional IAM framework technology were a managerial nightmare, due to the constantly evolving population of internal and third parties that needed access. However, opening access up was not an option due to the proprietary nature of the data. Adding to this challenge was the fact that much of the required information sharing was taking place in a rogue fashion with no corporate oversight and a high amount of risk. When it came time to satisfy the strict regulatory requirements of the energy industry, simply providing accurate data on information exchange and access rights was near impossible.

The company solved its problems by standardizing its access governance processes on a single foundation of uniform processes, unified policy, complete visibility and a high-amount of “self-service.” Internal employees and third parties could request access as they needed it and be automatically granted appropriate access when policy requirements were satisfied.

This real-world approach to access governance, gave this company a single source of the truth for access request, fulfillment (provisioning), recertification and
attestation, and compliance for application and unstructured data access. In addition, IT was relieved of a majority of the tedious and error-prone processes that were once so fundamental to access management.

Dell One Identity has been used by thousands of companies to address their IAM needs, including a quickly growing roster of organizations using One Identity for business-centered access governance and privileged account governance. One Identity unites access management, privileged account management and identity governance through a single, business-centric, future-proof foundation. It ensures that governance is done right – affordably and securely. This proven solution places control in the hands of the business with the visibility needed to ensure security and compliance balanced with trouble-free access to applications and data.

Among the identity governance capabilities available through Dell One Identity, some of the most prominent include:

- Enterprise provisioning
- Access request and certification
- Governance of unstructured data
- Role engineering
- Privileged account governance

For more information on the Dell One Identity approach to identity governance, to assess your current governance position or to try some of these capabilities yourself, visit us at software.dell.com/solutions/identity-and-access-management/.
Identity and Access Management for the Real World

Copyright © 2014 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. (“Dell”).

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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
Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.Dell.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.

iam.askanexpert@software.dell.com