AVATIER™

Provisioning | SSO | Governance | Password

TOP 10 IDENTITY MANAGEMENT BEST PRACTICES

The proven working guide for successful implementations.

2016 EDITION

TOP 10

Steps to Success

Successful identity management requires robust technology as well as coordination with IT and business processes as they pertain to the management of user information, access management rights and company-wide user provisioning and access management policies.

Successful Identity Management Implementation

Identity and access management (IAM) success comes only with careful planning, strategic decision-making and innovative technology tools. While Avatier's identity management software, delivers on the last of these elements, we're also committed to helping you throughout the entire lifecycle of your project, which offers the guidance you need to prepare for a successful IAM deployment.

Executing on your IAM strategy requires some careful consideration, as many challenges can emerge along the way to derail a project of this magnitude and importance. With that in mind, this guide is designed to help you sidestep these challenges by providing some practical, pre-deployment advice. In the following pages, you'll find the top 10 best practices that cover everything from preparing your directories, to working effectively with your in-house team, to making smart customization investments, and more. Use it to determine how to build a sustainable IAM strategy that will protect your company and assets from risk now and well into the future.

We hope you'll find this guide useful in preparing for your IAM project. When you're ready to move ahead, give us a call. We'll have the right solutions ready to meet your goals and exceed expectations.

TOP 10 Steps to Success

Step 1: Directory cleanup.

Don't jump into an IAM project with messy directories. First, free your system from clutter. Clean up your information security risks. Start by identifying accounts that are out of compliance with existing corporate policies and those no longer used. You do this by running reports to find accounts with missing attributes such as manager, department, company, office location and other key elements. Aside from helping clean your directories, there's an added benefit to identifying these accounts: The Information security of your directory environment dramatically improves.

As part of your cleanup efforts, connect with HR to validate the accuracy of HR data, which can translate to a higher role-based access control success rate. Clean up existing user access: Determine role strategy at the organizational, application and simple "birthright" role levels. All this will help streamline future user provisioning and access management after your new IAM solution is deployed.

☐ Approved by _____

☐ Date completed _____

Step 2: Create an anchor account.

Once you're ready to select an IAM solution, consider one that utilizes your existing LDAP directory as the authoritative source of user data rather than requiring the creation of another LDAP directory, virtual directories, synchronization engines or databases. This decision simplifies your project and jumpstarts your initiative since you will already have your identities established in the core directory. Simplification also translates to a solution that is sustainable and easier to support long-term.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

When selecting an IAM solution, look for the specific attributes of each system or service to determine whether it provides the functionality you need to accomplish your goals. Once your choices are narrowed, the ability to execute a proof-of-concept, as opposed to a prolonged RFP, is invaluable.

Step 3: Standardize on user account naming conventions.

Typical real-world environments are heterogeneous in nature and legacy systems combined with newer technology often reveal a different naming convention among user accounts on your systems. By standardizing on naming conventions across all platforms and documenting them ahead of time, you avoid unnecessary complications when it comes time to deploy your new IAM solution. In many legacy systems, it is easy to rename accounts to match a new naming convention. Take advantage of this to normalize your environment.

☐ Approved by _____

☐ Date completed _____

Step 4: Align password policies across each system.

Different systems will likely have different password complexity policies. Make sure these rules are documented so that configuration will be expedited when the new IAM solution is deployed. Once you understand the password policy settings, identify a policy that works across all your system types. When users only have to remember one complexity policy and password, the user experience and security improve.

☐ Approved by _____

☐ Date completed _____

Step 5: Build a user account mapping strategy.

Systems tend to contain their own naming conventions for user IDs, and your IAM solution must be able to map all accounts that belong to a user together in some fashion. Therefore, a plan for incorporating the existing user base into your account mapping strategy is recommended. To facilitate the creation of a strategy, examine user accounts across platforms. Once the account IDs are correlated, the ability to quickly and effectively remove all network access on user termination, as well as cross-platform self-service password reset and account unlock, become possible. Examine ways to export the user directories from all systems, and the different methods to correlate those IDs.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

Step 6: Establish "ownership" for systems.

In each organization, a single individual should have the ultimate authority to grant access to specific company resources. By determining and establishing owners for all systems, subsystem containers and the individual privileges within those systems beforehand, a streamlined workflow approval path will be created when an entitlement is requested in the new IAM system. Make sure these owners understand their responsibilities so they can assist with keeping systems secure.

☐ Approved by _____

☐ Date completed _____

Step 7: Decide how to communicate with users for all IAM needs.

Whether a password change or workflow approval, every IAM action and task performed throughout the system must be communicated. Decide how to word these communications, and then document the agreed-upon nomenclature to streamline the IAM system configuration and accelerate use case testing for user acceptance. Also, consider which system events or actions will interact with your existing help desk ticketing system, and document those requirements as well. The appropriate quantity of messaging is also important, since too many notices can often be treated as SPAM and will be ignored.

☐ Approved by _____

☐ Date completed _____

Step 8: Engage with fellow colleagues — Your user base.

Querying the actual users to find out their needs and pain points is an important step in determining the type of functionality you'll be looking for in an IAM solution. First, identify the top 10 percent of requesters through your existing IAM solution or help desk, and meet with them to gather their comments and suggestions. Learn about document broken identity processes, which could include HR onboarding or off boarding, physical security, asset management, help desk issues, and IT security. Meet also with your IT audit control and access governance teams to get their sign-off on a solution early and in writing.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

Step 9: Make smart spending decisions.

It's easy to get caught up in all the bells and whistles a new IAM solution offers. But keep your head. Think about your top concerns and spend accordingly. We recommend spending on customizations that reduce operational pain and on innovative ideas that address a business need. Also, consider investing in a solution that offers access to efficient, knowledgeable resources that know the solution, the industry and your pain points, inside and out.

As for what not to spend on, avoid low-value high dollar customizations. Reject any customizations that address a specific business process that could change (such as new management, reorgs, acquisitions and mergers, etc.). And forget trying to solve the last 5 percent of your security needs. You'll end up spending more than it's worth. Keep in mind that simple business process changes should be investigated along with customizations, since change management often improves security without financial impact.

☐ Approved by _____

☐ Date completed _____

Step 10: Select your front runners.

Once you've checked your organization's needs against what's out there, bring in the vendors for proofs of concept. Their responses on paper won't mean much until they can prove it in your environment. So connect the competing solutions to your systems to separate the wheat from the chaff.

☐ Approved by _____

☐ Date completed _____

IDENTITY MANAGEMENT DEPLOYMENT

TOP 10 Steps to Success

IAM Success

By investing in the right identity management solution, you can realize quick ROI, while strengthening your organization for the long haul. But remember that whichever solution you choose, it must be able to balance core identity management and access management requirements with a user-friendly interface to ensure its use across your organization.

IAM success— that is, reduced risk, improved service levels and lower operational costs, is absolutely attainable, but you must lay solid groundwork first. As part of this, you must have a complete understanding of your organization's business goals. Following these simple preparatory steps is equally critical, and ultimately ensures a smooth, relatively streamlined journey to IAM implementation success.

Innovative Identity Management and Access Management Delivered

Avatier is a leading provider of enterprise identity management solutions. Avatier Identity and Access Management Software Suite (AIMS) enables business line managers to take control of the identity management life cycle through a patented IT storefront for service catalog user provisioning, a universal mobile client for access certifications, and self-service password management. Avatier solutions maximize operational efficiency through IT automation and self-service operations.

Provisioning | SSO | Governance | Password

TOP 10 Steps to Success

Notes