AVATIER™

Vulnerability | Planning | Identity | IT Risk

TOP 10 IDENTITY MANAGER LEGACY MIGRATION

BEST PRACTICES

The proven working guide for successful migrations.

2025 EDITION

TOP 10

Steps to Success

Migrating off a legacy identity manager solution to a next generation IAM HD product provides measurable benefits that help further automate IT and place accountability in the hands of the business. Luckily, identity manager migrations are now greatly simplified because the latest technologies deploy faster and adapt to changing business processes with configuration ease.

Identity Manager Legacy Migration

Migrating off of older Identity Manager technologies can be a daunting task, and many organizations are concerned about undertaking such an effort when their original project or projects involved so much complexity. However, the good news is that the majority of effort applied to the original legacy solution implementation can be leveraged to deploy a next-generation identity and access management solution that provides greater business value. Luckily, next generation identity manager solutions deploy much faster than older "platform-based" environments.

This best practice guide helps organizations migrate smoothly off of outdated legacy identity managers to a holistic definition of Identity and Access Management or IAM HD, which provides additional business and security benefits through faster time-to-value at lower support costs. For migration projects, revisit current issues and audit concerns since these can be successfully remedied with the latest technology. By using this workbook, you will realize the full benefits of a next generation identity manager.

TOP 10 Steps to Success

Step 1: Identity manager account mapping.

Systems tend to have disparate naming conventions for user IDs, and your identity manager 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 and leverage your existing IAM solution as a reference if accounts have already been mapped. 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 _____

Step 2: Identity manager directory cleanup.

Don't jump into an identity manager project with problematic directories. Even though you already have a legacy identity and access management solution in place, you should validate that your directories are free from clutter. Start by identifying accounts that are out of compliance with existing corporate policies or are no longer used. You can 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 will be dramatically improved.

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 when your new IAM solution is deployed.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

When selecting a new identity manager, look at the specific attributes of each to determine whether they can provide 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: Identity manager account naming conventions.

Real-world environments are heterogeneous in nature. Legacy systems combined with newer technology often reveal various naming convention among user accounts. Standardize naming conventions across all platforms and document ahead of time so you can avoid unnecessary complications when it comes time to deploy your new identity manager. 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: Review top access requests and broken processes.

Query users to find out their needs and pain points. This is an important step in determining the type of functionality you'll be looking for in an identity manager. First, identify the top 10 percent of requesters through your existing identity manager or help desk, and meet with them to gather their comments and suggestions. Learn about 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 audit control and access governance teams to get their sign-off early and in writing.

☐ Approved by _____

☐ Date completed _____

Step 5: Communicate with users for all identity manager needs.

Whether a password change or workflow approval, every IAM action or task performed throughout the system must be communicated. Review existing communications assigned in your legacy solution, and then fix problem areas. Identify nomenclature to expedite the identity manager system configuration. This accelerates use case testing and efficiency 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 6: Revisit identity manager roles and role mining.

Regardless of whether you have implemented full role-based access control or you simply need to grant birthright access to new hires, take the time to revisit your organizations roles and access requirements. Most likely, roles and access requirements have changed over time which could result in excessive access being granted. Therefore, the roles should be validated and remedied prior to moving them over to a new solution. Also, you should take this opportunity to potentially expand your RBAC approach since you are implementing newer technology. There are services and tools that can make role mining much easier nowadays.

☐ Approved by _____

☐ Date completed _____

Step 7: Transfer identity manager access privileges.

One of the most challenging aspects of deploying an access management solution is determining the individual rights/privileges required for each access type and configuring them in the identity manager. Since an existing solution is already in place and consists of all of these access rights, it will be very easy to re-create the privileges in a next-generation identity manager. As a result, investigate applications that potentially were not in scope during the original implementation and add them to the new solution. The more you automate the better.

☐ Approved by _____

☐ Date completed _____

Step 8: Add IAM HD assignments to your identity manager.

IAM Holistic Definition is a concept that should be investigated in any new identity manager. IAM HD takes into account all aspects of an identity's assignments, not just access requests. The access management interface should allow for selection of access, assets, services and virtually anything your users' needs. Since an identity manager handles all workflow approvals, your request processes for all assignments become more secure, streamlined and with built-in audit controls.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

Step 9: Expand identity manager connector scope.

Newer identity managers offer an easy-to-use connector framework that enables greater enterprise automation. While your legacy identity management solution may have only addressed active directory and a couple other key applications, take the time to extend capabilities by adding more automated connectors to your key systems. The amount of time it takes to configure a next-generation identity manger is minimal, so the benefits of automating access requests to a greater number of systems is well worth the effort. Keep in mind that every application that is automated in the solution reduces the number of manual service tickets opened to an IT administration team.

☐ Approved by _____

☐ Date completed _____

Step 10: Address existing identity manager audit concerns.

Most likely, new and unresolved audit concerns exist because of the inflexibility of legacy identity managers. Review current audit findings and work with your audit teams to discover what can be solved as part of a migration project. It is probable that a new identity manager addresses some or all of these concerns out-of-the-box. Nevertheless, you must understand the concerns in order to configure a solution to meet your needs. Keep audit teams involved to gain support throughout the project.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

IDENTITY MANAGER DEPLOYMENT

Identity Manager Success

By migrating to a next generation identity manager, you realize quick ROI. You also strengthen your organization for the long haul. Remember that whichever identity manager 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.

Identity Manager success — that is, reduced risk, improved service levels and lower operational costs — is absolutely attainable, and the fact that you have already invested time to understand your needs during legacy identity management projects will make the move to IAM HD easy. Follow these migration steps. It is critical and ultimately ensures a smooth streamlined journey away from your legacy identity manager.

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.

Vulnerability | Planning | Identity | IT Risk

TOP 10 Steps to Success

Notes

AVATIER™

800-609-8610 North America
+44 (0) 207 877 1807 EMEA
+61 (0) 2 9959 1047 APAC
www.avatier.com