Provision IAM

10 Things to Consider When Implementing an Identity Management Solution

How to best prepare to add an IAM solution at your bank or credit union.

Community banks and credit unions manage hundreds of systems. Due to personnel turnover, hiring, and role changes, permissions on every system generally need to be updated frequently through a manual process. The use of an IAM system to automate common tasks to improve employee productivity, ensure security, and reduce the time required for audit preparation is a game-changer. If you're here, you already know that. Through conversations with past clients and our own experience, we've put together this list...

□ 1. Gather the Right People and Gain Alignment

Before you start talking about the real implications of IAM, pause to be sure all involved departments have a seat at the table. Think granularly about how permissions will be set up, and who should have input. Some obvious suggestions are Human Resources, IT, and Compliance. Create common goals, objectives, milestones, and a realistic timeline. Ensuring that executives and department leadership are aligned in the importance of IAM will be critical to your success.

□ 2. Reach Agreement of Roles and Permissions Throughout the Organization

Before you start making decisions on how to manage the identity solution, it's important to understand (across all departments) what the bare minimum permissions should be, as it relates to different roles throughout the organization.

□ 3. Evaluate On-premise, Cloud, or Hybrid Deployment Options

IAM Solutions come in many forms. One of your earliest decisions will be choosing between on-premise, cloud, or hybrid deployment. Reliability, security, flexibility, ease of use, agility, and cost should all be considered in relation to your institution's unique challenges.

□ 4. Review Your Current Authentication Procedures

It's important to ensure that you trust in the identity policy that's being created, having an established policy that includes

MFA (multi-factor authentication) and/or SSO (single sign-on.)

□ 5. Establish a Firm Workflow That Addresses Authorization of Important Changes

Decide at what point in the employee lifecycle stakeholder acknowledgment is needed. Will permissions need to change? For example, if an employee role needs changes temporarily, what workflow will be triggered? Also consider automated account provisioning needs. When should there be a pre-provisioned Active Directory account prior to hire? What other automated provisioning needs to be planned?

□ 6. Prioritize Systems That Are Critical to Your Business and Dig Deeper

Identity and prioritize systems that contribute materially to your identity risk, such as your core provider, HR system, loan origination system, and more. For example, if your HR department uses ADP, your ADP representative will need to assist in gaining API access. Identifying these scenarios, and creating an early connection with core providers, such as FIS, will once again save you time and prevent project hold-ups. Additionally, you should take a close look at your systems and decide who should be authorizing access to each one, and who the authoritative source for assigning that responsibility is. Is it a committee, the executive team, IT leader?

□ 7. Hone Your Understanding of the Compliance and Regulatory Environment

It's important to know what is expected of your institution from auditors, so that the IAM system can be managed in a way that efficiently addresses those needs. Both internal and external audit teams are likely to request reporting that proves compliance with numerous regulations and best practices, among other things. Be sure your implementation team is in-the-know about regulations such as the GDPR and CCPA. For example, the FDIC/NCUA typically require that people who monitor systems access and request changes are different from the people who approve those changes.

□ 8. Define a Certification Policy Designed to Audit Your User Access

Automated systems are great when it comes to managing access certifications, but there should be a policy in place that outlines a recurring review of those permissions. Reviewing your roles periodically is important to ensure that your employees only have access to what they need to do their job. Access needs can change, and department heads, an assigned committee, or other identified stakeholder should plan to review and recertify access within their institution at least annually, if not more often. Having a policy that ensures everyone is in agreement about how, and how often, this review will take place is important.

□ 9. Define IAM Success

Set some expectations for what this implementation means at your institution. What is the end goal, and how will you know the investment was worth it? Is it a time savings from your staff, or perhaps the ability to have flexibility in future years as the regulatory landscape changes? Maybe it's the reduction of future risk and reallocation of company resources to more important projects. Whichever benefit first piqued your interest in an identity management solution, keep in mind all of the additional benefits that will come along with the completion of this project.

□ 10. Talk to an Expert

Before you go all in, engage with someone who has a variety of experience in implementation. Consult with peers in the financial information security community, such as FS-ISAC, to uncover helpful hints; talk to a representative from your core provider; and interview the sales professionals representing the systems.

Contact Bobbie Cooper:
bcooper@provisioniam.com • **O:** 888-545-5008, x145 • **M:** 814-397-8732

Our Mission: To empower community banks and credit unions with the same cybersecurity and management tools as large enterprise financial institutions to deliver increased security, value, and efficiency.

Learn more or schedule a demo today at provisioniam.com.