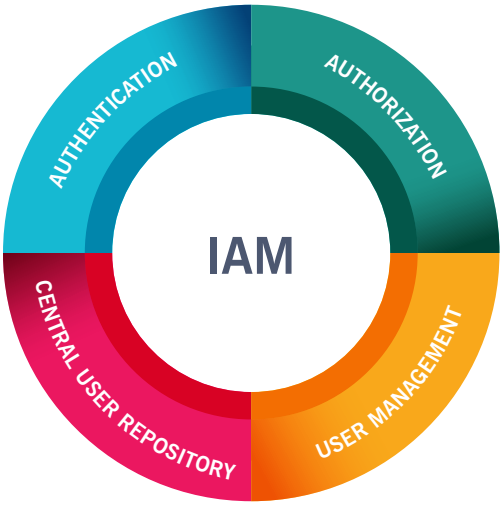
SYSFORE TECHNOLOGIES

BEST PRACTICES OF IDENTITY ACCESS MANAGEMENT (IAM)

Introduction

Identity and access management (IAM) isn't something you do once and then forget about. It's an ongoing process, a critical part of your infrastructure that demands continuous management. Even if you have a fully implemented directory, it's never too late to take advantage of best practices to help continuously manage this crucial part of your environment.

A key insight about identity and access management is that IT should not be heavily involved in identity management. Just because IT has the tools needed to manage identity, it should not be placed in the role of "gatekeeper". But with the right identity management tools in place, IT maintains the tools and infrastructure, and the business controls the actual identities.



Here are eight key practices, that Sysfore has gathered from years of Cloud experience and informed by this key insight, that will help you improve your identity management system to ensure better security, efficiency and compliance.

Best practices for IAM

Define your workforce

Your organization's workforce is managed by your human resources department. They also have to manage information about people who are not employees, such as contractors and consultants. Most of these people require access to company resources.

The first best practice is to use your HR systems as much as possible as an authoritative source of data for your identity and access management system. This will help you avoid repetitive work, errors, inconsistencies and other problems as the IAM system grows. You can provide a user friendly managed front-end, such as a web based interface that can be used to verify the quality of the imported data, revise data as needed and so on.

Define identities

The next best practice is to implement a single, integrated system that provides end-to-end management of employee identities and that retires orphaned or unneeded identities at the appropriate time. Typically, you'll identify the following:

- A primary directory service (often Active Directory)
- A messaging system (such as Exchange Server or Lotus Notes)
- A primary Enterprise Resource Planning (ERP) system (such as SAP)

Once identified, these crucial systems are integrated into the overall identity management architecture. They provide identity integration across the most-visible and most-used resources that users interact with on a daily basis. More systems can be integrated later.

In reality, each disparate system will continue to have its own user accounts. Your integrated system simply maps identities to these accounts, and you'll often use a web-based front-end to manage that mapping process. There will be invariably a few identities that can't be automatically mapped, and the front-end will allow those to be handled on an exception basis.

Provide knowledge and control to business owners

A proper identity access management regularly answers the question, "Who has access to what?" It enables the business data owners and custodians, to manage access to their data and to provide central reporting and control over those permissions. Again, a web-based frontend is ideal for this.

Implement workflow

Implementing a "request and approval" workflow provides an efficient way to manage and document change. A self-service user interface (often web-based) enables users to request permission to resources they need. Data owners and custodians can respond to these requests, helping the business ensure appropriate access, while removing IT from the decision making role in permissions management.

You need to be careful about defining different kinds of permission sets, each with its own workflows. This defines who can control that list of services, who is responsible for managing workflow designs, and so on.

Automate provisioning

You need to manage new users, users who leave the organization, and users who move or are promoted or demoted within the organization. Provisioning, de-provisioning and re-provisioning are often time-consuming manual tasks, and automating them can not only reduce overhead but also reduce errors and improve consistency.

These provisioning tasks typically involve connections to numerous systems, including email, ERP and databases. Prioritize these systems so that the most important and visible ones can be automated first, and clearly define and document the flow of data between these systems and your identity management toolset. You can focus first on automating the basic add/change/delete tasks for user accounts, and then integrate additional tasks such as unlocking accounts.

Become compliant

More than one industry or governmental regulations govern the way companies are run today. You can have an identity management system that clearly focuses on defining and documenting the job roles that have control over your data, as well as the job roles that should have access to auditing information.

You should define detailed compliance rules step by step, and assign each step to a responsible job role. Integrate rule checking in your identity management system and workflow operations to help automate remediation of incorrect actions; this will help improve consistency and security as well as compliance.

Check and recheck

Ideally, permissions should be assigned to job roles. But in reality, permissions are assigned to individuals as needed and never reviewed again. This poses security risks.

Permissions should be periodically recertified. You need to review who has access to what and determine whether or not they should still have those permissions. Start by defining job roles within your organization that can recertify permissions, such as system owners, managers, information security officers and so forth.

Recertification can be defined in a workflow in which data owners and custodians review a current permission set and verify the accuracy (or inaccuracy) of that set. This process assures that the roles and people who have permissions to resources should continue to have those permissions.

Manage roles

Permissions are best assigned to job roles rather than to individuals. You can mange identities when you associate those roles to real-life job tasks and job titles. Conduct prior research on accurately identifying the major roles within your organization, based on the resource permissions currently in force.

Whenever a user requests access to the appropriate resources and services, the data owner or custodian, can review and either approve or deny the request—taking IT out of the permissions management loop entirely.

You'll also need to define who will manage these roles in order to ensure that roles are created, modified and deactivated only by authorized individuals following the proper workflow.

Choosing the right tools

Today's IAM frameworks is a amalgam of traditional frameworks and third-party tools that gets the job done, but at a high cost in efficiency and security risk.

You need a central place to manage the identities used by all of the native system such as Microsoft Active Directory, SAP, PeopleSoft, Unix or Mac OS. Ultimately, identity management becomes driven by what IT is capable of, and not by what the business needs.

About Sysfore:

Sysfore is a systems integrator (SI) specialized in building computing systems for enterprise clients using the best of cloud, mobile, and responsive web technologies. We serve a global client base, offering consulting, technology and managed services.
We are a team of about 100 people, passionate about using the best technology and tools to achieve results for our customers. We call Bangalore, India as Home. We have worked with customers from across the globe, successfully delivering quality work products and making a positive contribution to their businesses. Since the beginning, we've always been committed to a customer's success and go that extra mile towards achieving delight.

Sysfore is a recognized Microsoft Gold Partner and Amazon Web Services Consulting Partner delivering results for customers, through comprehensive consulting, deployment and cloud managed solutions.
We take pride in having over 70 global clients, done over a 100+ cloud consulting engagements, 80+ cloud migrations, 50+ POCs and deployed over 50 Storage and DR Solutions across multiple industries.

For more details or information, connect with us:
Email: info@sysfore.com
Call us : +91-80- 4110-5555
Website: www.sysfore.com