protiviti®
Face the Future with Confidence

How to implement an effective identity management strategy

Introduction

Identity management doesn't happen overnight; there's no "Easy" button to press, or magic snap-of-the-fingers instant fix. In fact, identity management has transformed into something far more complex than password authentication and simple security measures. It's important to understand that jumping into a new technology instantaneously isn't necessarily the right first step to ensuring a successful program.

Getting the keys to the kingdom has become harder than ever before. To do it the right way, you need an appropriate foundation in place for decision-making. This includes prioritizing projects that will roll-up into an identity management, or IAM, program.

So we get it: identity management takes work and pre-planning — but how do you know what constitutes a strategy that will be truly effective and ironclad?

The surface answer is that you need expertise to help it flourish before, during and after deployment. From governance to policy frameworks and infrastructure, in this guide we are going to show you the steps for implementing an effective identity management strategy. This includes how to get there, and stay there, with advisory tailored to fit your company's pain points and needs.

Why Identity Management?

The question may come of no surprise to you: identity management, or IAM, has been around for years. Despite its long-running history, IT departments have yet to fully implement this as a step in securing enterprises.

It's not that IT professionals don't want to. The reasons may span from not having the resources to even feeling like it's not necessary (hence the dawn and inevitable continuation of shadow IT).

However, implementing identity management is necessary, and chances are that your IT department isn't equipped to handle the needs and expertise that comes with identity security and protection.

As a result, you must go back to the quintessential IAM definition when asking "Why identity management?" One IAM definition: *This was referenced from Gartner: Enabling the right individuals to access the right resources at the right times for the right reasons.*

The Key to Success

The key to success in an identity management strategy is following simplicity and taking precautionary initiatives before implementation. Every project varies depending on your needs as an enterprise, as well as your current and predicted pain points. You should always make decisions with usability and scalability in mind.

Remember not to dive right into deployment! If an IAM firm is pressuring you to deploy new technology right away without an audit (which comprises of addressing your needs and procedures) there's a problem!

There are a number of other steps that come before technology. Some examples are:

- Documented policies embedded within the culture
- Procedures that are well documented and right procedures to automate
- HR user data hierarchy
- Inventory of applications with associated risk ratings (impact x likelihood)
- Application owners identified
- Process owners identified

Take the time to diagnose your business and where it may be faulty or have kinks. The key to success lies in finding those things first. After all, you can't treat a disease without knowing what the cause and symptoms. The same principles apply to deploying IAM.

It's from there that you can formulate the proper approach for your identity management strategy.

Making Identity Management Effective

So you've compiled your company's pain points and conducted an audit of your processes, data and procedures. You know where things are lacking, and what needs fixing and protecting. This is where you can begin implementing your identity management program, which has been scheduled and compiled into a roadmap around the aforementioned points.

The road to deployment may be long, but the benefits also span for the long-term. It may not be an "Easy" button, but IAM is undeniably a comprehensive solution for your business's security needs.

With IAM, you are having to manage the identities of:

- People
- Accounts
- Organizations
- Groups
- Privileges
- And more…

In this regard, you must be able to align policy and technology, so automation is in place as much as possible. Using a "Plan, Build, and Run" methodology, this provides full coverage for your enterprise.

Plan, Build, and Run for an Effective Strategy

Taking a "process first, business second," approach, we here at Protiviti implement the right technologies for your business with this methodology. You get everything you need, and everything you don't in order to appropriately scale for your employees and customers. As an advisory and consulting firm, we find this framework to be versatile and work well with most clients.

Also, as a best practice for plan, build, and run for an effective identity management strategy, don't forget to establish a comprehensive IAM Governance track. Consider leveraging an IT Governance framework such as COBIT5 or ITILv3 as they ensure complete coverage over your plan, build, and run activities.

Personalize those frameworks to your IAM program by defining roles and assigning them to people in your organization. This will yield a clear understanding of who is responsible and accountable for what's in your IAM program.

Advisory to Fit Your Needs

If a pipe under your sink broke, would you try to fix it yourself? How about a raw electrical wire in your house? It's best not to take that risk — for IAM, it's always ideal to call upon an expert to help evaluate your situation and select the right technologies.

If not, you may risk putting a Band-aid over the problem and not actually fixing it. This can include utilizing the cloud without regulating or restricting access.

This will maximize your company's effectiveness once an identity management strategy is implemented.

There are many advisory firms that are the plumbers and electricians of IAM. They are invaluable to maintaining and driving your IAM initiatives.

Conclusion

Instead of worrying about the price of a safe and secure enterprise, try to think of the cost of not having it safe. It is far worse to experience a provisioning problem or security issue that exposes your company's data and personal information, especially for your customers.

Your reputability as a company is directly correlated with the security and trust customers hold in you. Having an identity management strategy will do just that for you and more.

To learn more, we invite you to contact the Protiviti team for a free consultation. Thank you for reading this guide; we hope it has been helpful in your search for what makes an effective identity management strategy!