



eBOOK

Starting off on the Right Foot:

Best Practices for Creating an Identity Management Strategy



Today's business world moves more quickly, entails more types of applications, involves more categorizations of users, and is exponentially more complex for IT to enable than ever before. What once used to be straightforward has become a giant, inter-connected ecosystem teeming with thousands of applications, people and devices, all creating a web of access points and connections. It's no surprise that an enterprise operating in this reality now has millions – if not a billion – points of access that they must control and manage, securely and efficiently.

It's no surprise that many security professionals find themselves looking for a next-generation identity management solution that can address today's challenges and scale to meet future ones. Once you start peeling back the layers and see the breadth of the project set before you, it can be overwhelming. But with the right plan in place, and the right mindset, you can not only succeed, but flourish, helping your organization become more efficient, more secure, save costs, and ease frustration from ineffective practices and policies.


Begin with the End in Mind

The catalyst for this search is usually caused by a pain point in your organization. Perhaps the helpdesk is overburdened with access requests and password resets. Maybe a recent compliance audit was failed, or excess user permissions were discovered. Or, recent adoptions of cloud-based applications have decreased security visibility but increased the complexity of the IT ecosystem. Worse, perhaps you realized that it's only a matter of time before a major data breach impacts your organization.

As with most large undertakings, the first step of this process is to simply imagine where you want to end up. This could take the form of many types of goals that you want your organization to achieve, but they generally encompass saving time and money.

Common goals of Identity Management:

- Automated onboarding and offboarding
- Handling temporary access of contractors
- Self-service access requests and password management
- Demonstration of compliance for IT audits
- Routine review and certification of appropriate user access



**You can't know
how to get there
if you don't
know where
you're going.**

While it would seem simpler to solve only the issue that is causing you the most trouble, you must also think about how it impacts your IT security at large. Each piece of your security program must connect to one another, use the same information and have full visibility of the available data if it is to help the IT department make the right decisions and answer the all-important question: “Who has access to what?”

The identities in your organization – the employees, contractors, suppliers, vendors, partners, and even customers – are who access your data. Securing those identities is everything, and governing them must be at the center of your IT security strategy. It should not be a question of just solving automated onboarding or implementing single sign-on. The real question is how you secure the sensitive data, enforce the policies and procedures that govern access to your organization’s data and applications, and do it all while making the processes involved more efficient and less costly.

Gain Support from Everywhere You Can

By beginning with what you want to accomplish, you can then create a plan that involves the right people and is structured the right way to achieve success and realize value. This is not a one-person or even a one-team job. You must have buy-in and support from all areas of the organization in order for the program to continue moving forward and gain traction within the business. Find representatives in each of the departments and understand their wants and needs from an identity management program. Then, you can build the program to satisfy those needs and prove value to the organization at large.

While it may seem that the initial approval milestone is the most difficult to overcome, the road along the way can be where it ends up falling apart. Joining together teams that may not usually communicate, involving people with the wrong set of skills or simply neglecting to set clear guidelines for how the program will run can result in failure. If a piece of the puzzle ends up not fitting, it can sometimes be easier to give up altogether rather than find the right piece. By preparing for the potential problem areas, you can know what the signs of trouble look like and take steps to avoid them.

Common reasons an identity management program fails:

- No executive support
- Lack of funding
- Not involving the business users
- Insufficient communication of project value
- Poor understanding of program depth

Focusing only on what happens when something goes wrong, however, is not enough either. In order for the program to feel like a success, you must also employ champions and cheerleaders within the organization, showcase the potential and realized value and then demonstrate that the end you set in mind is being worked towards and eventually achieved.

During the initial implementation, creating smaller projects that are part of a larger program will help to keep timelines short and focused, while also giving periodic achievements to celebrate. This kind of “short sprint” project cycle will aid work in the future when additional modules need to be integrated, or the identity management program expands to include more aspects of the IT systems. It is also important to remember that identity management is a program that will continue to evolve and grow with your organization after initial implementation is complete.

Utilize the Resources Available to You

Technology alone – the software solution you procure and deploy – can help to automate and speed up processes, depending on your particular problem set, but it will not solve every issue your organization currently faces. Only by implementing rules and policies learned from delving into your organization’s current and ideal processes can the software achieve the desired end result. Learning the best practices in regards to building (or re-building) your identity management program will determine how effective the policies and procedures will be after implementation is completed.

While another organization may not have the particular set of issues concerning provisioning, compliance, etc. that yours does, many have solved their problem set before. Seek out case studies and testimonials from customers of your potential software vendor. Read the available white papers, solution briefs and other documentation that offers best practices and lessons learned. And finally, solicit the advice and assistance from your contacts both within your organization and at the software vendor.

Implementing an identity management program in your organization may be a long journey, but any potential qualms from starting the endeavor are far outweighed by the efficiencies and cost savings (which can be in the millions of dollars) from the result of a well-planned and successful implementation.

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint’s open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint’s customers are among the world’s largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.