FIVE STEPS FOR A SUCCESSFUL IDM DEPLOYMENT
Five steps for a successful IDM deployment

Identity and Data Management (IDM) is a complex and ever-shifting aspect of every organization’s IT structure. With each new hire and business decision made, access requirements can change; identity and credential mapping, therefore, changes as well. Identity touches on a broad range of business functions – from the security team to HR, finance and beyond – and can have a far-reaching business and financial impact.

It’s no surprise, then, that IDM is essential yet challenging, involving policy design, role-mapping, identity and data controls, planning, implementation and operations. And that’s before you throw technology into the mix. Most companies already have an existing IDM program in place, albeit with varying degrees of success. Unfortunately, a combination of siloed processes and organizations, a lack of alignment among business, technology and security teams, a lack of visibility into data, or incomplete data means IDM often doesn’t work as efficiently as it should. With a patchwork or ad-hoc approach, companies are left open to security threats and business and financial risks, both from within and outside of the organization.

For future-thinking organizations, a better solution is needed. Have you already championed a new IDM deployment for your company? Let’s look at how can you make sure you get it right the first time and reap the maximum benefits of IDM.
Making the most of your IDM program

To start with, you need to be extremely clear on what your IDM strategy is, including a clear understanding of exactly what you’re hoping to achieve. Ideally, strategy, scope, goals and timelines will be covered during the cost-benefit meetings and addressed in business-case write-ups. A strategic and holistic approach to IDM includes identity governance, access management and data governance and protection.

Because of its complex nature, deploying an IDM program can be difficult. A successful deployment is often even harder to achieve. Whether it’s a lack of skilled individuals, bringing the project in on budget, or delivering on the expected business outcomes, challenges will arise. When things don’t work as they should, significant disruption to business performance and staff productivity can ensue, not to mention the financial impact to the organization due to additional time and money spent. Think of these challenges as an opportunity to correctly launch your IDM program from the very beginning.

To help ensure your success, we’ve put together our top five steps to deploying your IDM program.
Step 1

Executive sponsorship

Like any complicated, long-term project, it’s crucial not just to secure high-level sign-off but to also make sure your executive sponsor is actively engaged. A lack of management interest is a common cause of project failure. In this instance, an executive sponsor can be the thread who draws the project together. Because identity is an issue that crosses a number of important business functions, broad alignment is vital to the success of your deployment.

An engaged CIO or other senior figure can provide this alignment, helping to keep the project on track, within scope and in line with expectations. An engaged executive sponsor is also invaluable to the process because he or she has a vested interest in the security of the organization and how IDM efforts could affect business outcomes. To ensure executive- and board-level support, align and integrate your IDM program with other business objectives, particularly ones tied to enterprise governance and security initiatives.

Try to preempt the sort of issues that could cause an executive sponsor to become disengaged. Maybe the project is dragging on too long. Or, the issue might have a more complicated root cause – like limited awareness of the key business drivers or lack of understanding on why the current business landscape necessitates an IDM program. By identifying and preparing for these problems ahead of time, you can help to ensure your IDM program progresses smoothly with the support it needs.

Finally, think about how you’re going to engage with and communicate to your wider staff about the project. They’ll be the ones using it, after all. Working with them in mind from the beginning will help in the long-term.
Embrace simplicity

In both our personal and working lives, we’ve become accustomed to the notion that greater customization means better functionality. When it comes to IDM, however, Optiv has found the level of customization that is truly needed tends to be fairly small. Obviously, every organization is unique, with its own ambitions and challenges. Whether you’re an international finance company or a local recruitment office, often the same set of concerns need to be addressed. As a result, the key functionalities tend to remain the same, regardless of what your IDM ambitions are.

What does this mean for you and your organization? You should keep things simple and leverage as much out-of-the-box functionality as you can. A good rule of thumb is to follow the Pareto principle: 80 percent of the functionality in the deployment should be standard functionality of the solution, and 20 percent should be customized functionality. For example, businesses are often wary of IDM projects because they can be such a time-consuming undertaking. Embracing simplicity can help you to minimize the time and effort needed to deploy – especially if you don’t have a large, internal team of security experts in place to manage the project.

Out-of-the-box functionality can also simplify future execution and maintenance of your IDM. Highly customized systems are usually difficult to update and upgrade. To maintain a highly customized system, you’ll need specialized staff, and a skills shortage is already a pain point for IDM. Excessive customization will also make the cost higher. While we’re used to the idea that spending more means higher quality products or services, this doesn’t necessarily apply when it comes to customization. You should certainly invest adequately in an IDM deployment, but overspending on customization could be a case of diminishing returns.

The Pareto principle: 80 percent of the functionality in the deployment should be standard functionality of the solution.
Pace yourself

When you’ve spent months busily making a case for investing in IDM, it’s tempting to end up seeing it as a panacea for every one of your company’s problems. While the benefits are certainly significant, when the time actually comes to deploy, it’s important to set expectations. Bear in mind the process can be iterative. That’s good news – you don’t necessarily need to address every single audit finding and inefficiency straightaway.

If you tried to address every little issue at the beginning, your IDM would never get off the ground. The average IDM project can last up to 26 weeks. While you can significantly improve performance in this timeframe, it isn’t realistic to fix an endless list of problems. Likewise, don’t keep continually adding requirements after the project begins. IT leaders responsible for IDM deployment should develop a strategic roadmap, outlining each step that needs to be taken along the way. Set the scope and stick to it. By pacing yourself and delivering incremental business outcomes, stakeholders will see value more quickly, and security and IT staff will have time to become proficient and knowledgeable enough to properly build out the IDM program.

You can also use this process to identify gaps in the next stage. An IDM program will involve operations management and upgrades over time; solving your problems all at one time is not necessary. Define short- and long-term goals and iterative milestones. Your executive sponsor can be of great use here, particularly in terms of blocking scope creep from other enthusiastic stakeholders.
Step 4

Don’t compromise

Cutting corners is an understandable human impulse. We’ve all done it at some point or another – especially when we’re time pressured. To ensure the success of your IDM deployment, try to avoid falling into this trap. Even if the process is moving slowly, or you’ve missed an important milestone, compromising the quality of your project can have significant financial and security ramifications.

Typically, disparate and siloed systems or manual processes are the cause of delays in the process. The lack of integration, alignment and automation often goes back to the fact that IDM spans several departments. Because of the manual process of provisioning and deprovisioning employees when they join the company, change roles, or leave the company, it’s not uncommon to discover some information comes from an HR system, while other information is generated by finance processes. In pursuit of a quick resolution, it’s sometimes possible to fudge the system or take certain systems out of IDM scope.

Remember that in a properly organized IDM, there are countless dependencies at play. If you spot an opportunity to go the easy route by automating an incorrect process or succumbing to incomplete data, resist. Don’t perpetuate bad processes or policies in hopes of speeding up implementation. Instead, work with your executive sponsor to reset expectations, assess the risks and develop alternative solutions.

Remember that in a properly organized IDM, there are countless dependencies at play. If you spot an opportunity to go the easy route by automating an incorrect process or succumbing to incomplete data, resist.
Step 5

Build for the long-term

Once you have sign-off to invest the time and resources in an IDM program, it’s important to get it right for the life of the solution. With the right guidance, setting up IDM isn’t prohibitively complicated – but managing it on an ongoing basis can be. Before you’ve even begun your implementation, you should be thinking about who’s going to manage IDM down the line. Ideally, businesses should plan for the future with a people strategy that ensures the relevant training, hiring and onboarding has already started once the business case and budget are approved.

Thinking about and planning for organizational change is to your long-term benefit as well. Negative financial consequences could be spread far and wide if you’re unprepared. From mergers and acquisitions to new hires and redundancies, most businesses undergo periods of flux, and your IDM systems need to evolve in parallel. Fundamental business modifications, such as moving into a new geographic area or shifting services online, can also have an impact. Any such transformation can place new demands on your identity and data program. If you’re anticipating any sort of growth or development, you need to build your IDM with the prospect of change in mind.

Your IDM program should be thought of as an ongoing identity and data capability that remains in lockstep with your business and grows with your people.

Your IDM program should be thought of as an ongoing identity and data capability that remains in lockstep with your business and grows with your people.
Get ready for IDM success

During your IDM program, revisit the steps we’ve outlined to ensure you’re progressing with the right objectives in mind. You don’t want to be one of the many organizations suffering from a lack of control over privileged access and critical assets, inadequate visibility into data locations or a lack of IDM expertise. Spend the time and effort to invest in a new program and the staff training to properly deploy it. Doing so will create a solid identity and data foundation that aligns with your business growth goals and improves your security posture.

Find out how one of our retail customers successfully deployed our IDM program and reaped the rewards.

Read the Case Study