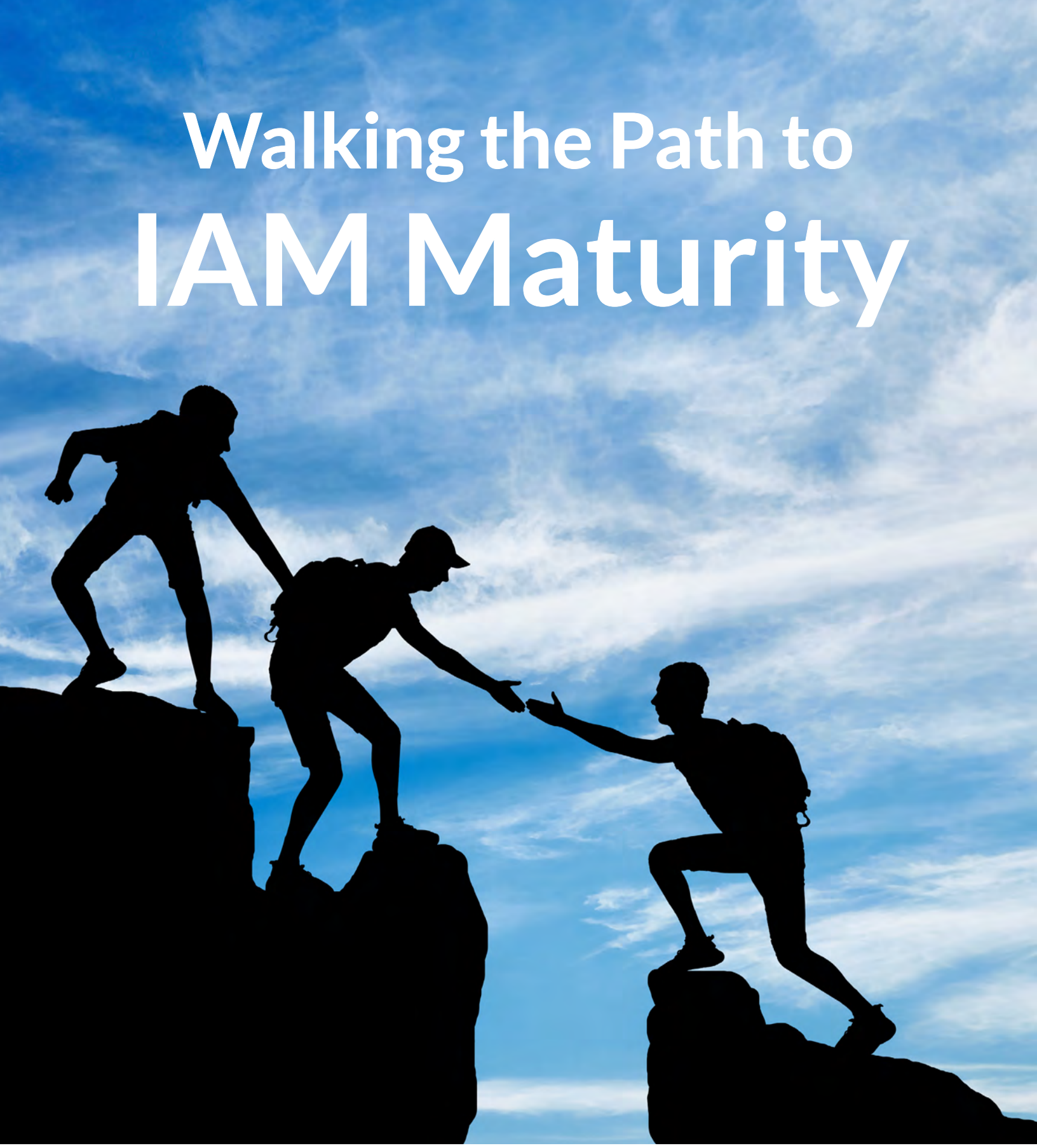
Walking the Path to IAM Maturity



OPTIMAL IdM
Identity & Access Management

Walking the Path to IAM Maturity

Identity access management (IAM) is a relationship. It begins when a user is provisioned and ends when the user is deprovisioned. In between those gateposts, the relationship grows as the user is authenticated, empowered to perform self-service, subjected to password management, and known to be in compliance. The user has needs as well, such as the need to create, read, upload, and delete, and the need to use hardware, software, and licenses.

What is IAM?

Identity access management is the process of defining and managing users' roles and access privileges, including granting, revoking, and denying those privileges.

Organizations are not naturally good at managing their relationships with users. Their struggles begin when they fail to grant the right permissions to the right roles in a manner that doesn't degrade user productivity, while also controlling those permissions tightly enough to keep the organization secure and compliant. To be better relationship partners for their users, they have to mature their IAM capabilities.

But that takes time, a luxury nobody has. Every minute that identity is managed poorly, or not managed at all, is a gift to malicious actors who want to compromise the environment to steal data and IP, sabotage the network, encrypt files for ransom, and cause financial and brand damage. Businesses shouldn't be patient when it comes to getting good at IAM. They should hustle to achieve IAM maturity as fast as possible so their data and businesses remain secure in an era when cybercrime is more profitable than the international drug trade to the tune of $6 trillion per year by 2021.

To reach maturity, businesses need a roadmap – an understanding of where they're going and a knowledge of the milestones they should be meeting along the way. This is called a maturity mode, and it enables businesses to assess the quality and effectiveness of their cybersecurity software and understand where to devote effort and budget in order to climb to the next level, as well as to compare themselves to competitors and provide evidence for compliance and certification purposes.

Applying the capability maturity model to IAM

The capability maturity model (CMM) is a methodology that was originally created to ease software development processes. In the 35 years since its inception, it has evolved to become the accepted standard for measuring and optimizing almost any type of computer technology process.

The CMM defines five stages of maturity. Here's a look at what they are, how they translate to IAM, and how businesses can immediately identify where they currently reside on the scale.

Stages	Description	IAM Specifics	Your Progress
Initial	The "chaotic" or "ad hoc" level, where there are many unknowns and few processes.	• Little infrastructure for identity management • Identity data is kept in discrete repositories with manual updates *Data is so vulnerable that it may be easier for hackers to access data than actual staff members.*	Processes are manual and time-intensive

Stages	Description	IAM Specifics	Your Progress
Repeatable	Processes are documented well enough that the function can be repeated using the same steps.	• Beginning to use disciplined processes for managing and protecting data • Some synchronization of data repositories but no overarching system for governing multiple identity data repositories *This is where most companies get stuck.*	Processes are manual and time-intensive
Defined	Processes are fully defined and are now a standard business procedure.	• Has an established system for collection, storage, archiving and publication of identity data • Consistent synchronization of databases and directories *Effective cloud-based enterprise systems may be at this level.*	
Managed	Consistent, agreed-on metrics for the process are used to manage it quantitatively.	• A high level of identity and access management and data protection • The system completely controls identity data, and governance of databases is locked down *This is a good place to be, but there's room to be even better.*	You use automation, but only in a limited way
Optimized	Part of process management now includes improvement of the process.	• Has a self-sustaining identity and access management system that can accommodate virtually any organizational requirements *The IAM is now in a loop of constant iterative improvement.*	Procedures are automated and your tools are integrated into the environment.

What stands between your businesses and maturity?

Achieving the highest level in a maturity model used to be very difficult, and few organizations were able to do it. Today, gaining maturity is far easier – but even so, most companies still get stuck on Level 2. They have some processes and some synchronization of data, but they can't quite push through the barriers to create an overarching system that governs all of their identity repositories. Where are they going wrong?

Why Businesses Get Stuck

They Lack Strategic Will	They Lack Tactical Ability	They Lack Vision
• No executive sponsor • No cross-organizational buy-in	• No day-to-day project management • No realistic timeframe or budget	• No long-term vision of what their IAM should accomplish
SOLUTION: The correct approach		
IAM impacts every department, so communicate the business value of strong IAM to the C-suite and involve stakeholders across the organization early. HR and Compliance should be key stakeholders.	As with any technology implementation, delivering great IAM depends on a competent project manager who can ensure that milestones are met and budgets managed.	Think about the direction of the business and how IAM should support it. Short-term plans will certainly be necessary, but the long-term is where IAM will deliver the greatest value.
SOLUTION: The correct people		
Every project requires a strong executive sponsor and a good project manager, and most require the ability to gain buy-in across departments. These are familiar steps within the capabilities of any successful business.		This is where the right partner comes in. Choose a vendor who is willing to learn your business and has the experience to share what they've learned from previous experiences with companies like yours.

The rise of cloud-based IAM and advances in automation are putting maturity within the reach of more businesses than ever before. Today, businesses of any size can improve their maturity, and they can do it at a pace no one could have dreamed about just a few years ago.

One word of warning before you begin your journey toward maturity: remember that the end goal is not just to move to a higher level. It's to improve your business's IAM capabilities so you can operate more securely and compliantly. It's easy to get lost in the bullet points, but never forget the true purpose of your efforts.

Leveling Up Your IAM Maturity

Before getting started on an IAM maturity assessment, two things must be known: the typical state of maturity among organizations in your industries and others, and the IAM products and services that are currently available on the market. With that information, you will recognize best practice and understand what is realistically possible for your own organization.

Then you're ready to dig in. Here is the bird's-eye view of what you need to do to become a more secure and compliant organization:

We are at Level 1

To Get To Level 2 We Will

- Perform a maturity assessment
- Get executive sponsorship
- Document manual procedures
- Cross-train personnel

We are at Level 2

To Get To Level 3 We Will

- Document IAM policies, procedures, and standards.
- Inventory privileged accounts, remote users, and cloud apps
- Consolodate directories and single sign-ons
- Research automated provisioning and self-service

We are at Level 3

To Get To Level 4 We Will

- Align provisioning with business processes
- Research integration between IAM and security incident response
- Improve privilege management and remote cloud IAM
- Document IAM metrics

We are at Level 4

To Get To Level 5 We Will

- Improve IAM integration with business process
- Measure and manage improvements
- Update IAM controls and policies, procedures, and standards
- Turn process optimization into a formal business process

Enable Growth With The Right Tools

What maturity means today is automation. Without automation, the volume of work required is simply unmanageable for even the largest of enterprises. Conversely, with automation, businesses of any size can achieve Level 4 or even 5 if they invest their efforts appropriately. Here are the tools and capabilities that will have the greatest impact:

API Security

APIs are now a standard business strategy, but they introduce risk. Their behaviors must be considered in the broader context of identity as a whole, including device identification, access times, geolocation, etc., and they must be subjected to testing by automated security tools.

Customer Identity And Access Management (CIAM)

CIAM is used to deliver seamless digital experiences to customers. Done right, CIAM will enable seamless account management that lets customers use a single sign-on (SSO) to access your environment with one set of credentials, and use multi-factor authentication (MFA) to secure their experience in a simple, easy way. Also look for a non-synchronizing virtual directory that provides instant access to customer identity data, no matter where it exists and without the need to set up a separate master database. Another desirable feature is service management, in which the vendor handles installation and configuration.

Identity As A Service (IDaaS)

IDaaS is easy to deploy and scale. The IDaaS you choose should provide authentication and authorization from any data store and be able to leverage existing technology investments. Also, it should have built-in connection pooling, full support for failover and load balancers, and robust caching options that can cache objects on a connection-by-connection basis or even an object class basis.

Identity Analytics (IA)

Identity analytics enable your organization to analyze your company's access controls. Your IA should provide in-depth audit trails and overview data that can be used to assess the effectiveness of your identity governance and administrative (IGA) service, provide specific detailed reports, and fuel context-based authentication.

Context-Based Authentication (CBA)

Opening your doors to users and devices opens your doors to risk, and previous approaches to controlling authentication were risk-based. However, context-based authentication is a more secure and powerful way to authenticate users. Context-based authentication uses analytic data that an identity platform compiles as part of the authorization and authentication process to improve authentication methods. These analytic-enhanced authentication methods embed dynamic risk assessment into the access decision, calculating risk through the use of behavior and context analytics. CBA offers an advantage over cookie-cutter systems that use the same security authentication methods regardless of risk level, and is therefore even more effective at enhancing consumer safety and reducing online fraud.

Identity Governance And Administration (IGA)

Identity governance and administration enables your organization to manage its digital identities and control access rights across your systems. Your solution should include identity lifecycle and entitlements management, which allows you to create and maintain identity and identity-related attributes; a user-friendly tool to manage access requests; workflow orchestration that follows a logical sequence of steps to ensure the primary functions of the IGA are initiated and approved by necessary stakeholders; automated provisioning and service tickets to establish, update, and delete accounts; role and policy management to control every aspect of the IGA component of your IAM system; and configurable auditing to monitor the lifecycle of your data.

3 Things to Remember on Your Path to IAM Maturity

- The steps to maturity between any one level and the next aren't simple. You need strong organizational will, a clear vision of how your IAM should support your strategic business goals, and a partner who understands how to deploy IAM in a way that helps you achieve those goals.
- Maturity for maturity's sake isn't helpful. Remember the real reasons you're making these improvements: so your organization can be more secure even as it scales, and your users and customers can become more productive through a better experience.
- Automate, automate, automate: Automation enables continuous improvement, increases efficiency, eliminates human error, makes scaling fast and easy, and frees up your IT team to focus on supporting the business instead of changing passwords or chasing down policy changes.

Mature Faster With Optimal IdM

Optimal IdM can catapult your cybersecurity maturity level from a one or two to a four or five, and we can do it almost immediately. With customized identity and access management solutions that can be on-premises or cloud-based, we have the technology you need to automate processes, mitigate security risks, and simplify your data environments. With solutions like our award-winning Virtual Identity Server, our LADP migration solutions, and multifactor identity authentication, we can provide everything you need to manage your data and lock it up tight. If you're interested in giving your data an elite level of protection at a cost-effective price point, contact Optimal IdM today for a free trial of our identity and access management solutions.