



HOW TO ASSESS THE MATURITY OF AN IAM PROGRAM

Introduction

A key component of personal maturity is recognizing one's own limitations and striving to learn how those limitations can be addressed. The maturity of your IAM program is much the same.

Having a "mature" IAM program means identifying the gaps in your identity fabric, establishing your priorities, and are executing on a plan. IAM maturity is arguably the most important metric for your IAM performance. It encompasses all four IAM pillars ([AM](#), [CIAM](#), [IGA](#), and [PAM](#)), [your detection and remediation capabilities](#), and even the cost/benefit analysis of your identity investments.

Yet most enterprises using identity services and solutions do not consider a maturity model when making critical decisions about their identity fabric. By understanding what goes into a maturity model like those offered by [Okta](#) and Simeio, you'll stand to make more informed decisions about what needs to go into your identity program.

The Metrics of a Maturity Model

You may have come across a few maturity models during your investigations into bolstering your identity fabric. However, you should bear in mind that not all models are comprehensive. Some only examine a single facet of your IAM program. These models may be helpful in addressing specific needs, but do not provide you with a full-scale, vendor-agnostic look at your program. When taking the trouble of an [IAM assessment](#), make sure you are putting your time into a suitably sweeping investigation covering all your needs.

You should also make sure that the model you're trusting follows a [Control Objectives for Information and Related Technologies \(COBIT\)](#) framework. This widely utilized model emphasizes three factors: business requirements, IT resources, and IT processes. COBIT can best be understood as a checklist of what should be investigated rather than how the investigation should take place. If the maturity model you've chosen follows a COBIT framework or, better yet, is COBIT certified then you should be well-vindicated in your choice.



The Metrics of a Maturity Model

Is your Maturity Model up to COBIT?

- **Business Requirements:** What does your enterprise hope to achieve? A strong maturity model must quantify your business' integrity, effectiveness, availability, efficiency, compliance, confidentiality, and reliability.
- **IT Resources:** What are the capabilities of your Information Technology sector? Be wary of any model that does not take stock of your infrastructure, applications, information, and IT staff.
- **IT Processes:** What are the parameters of your Information Technology pipeline? Maturity models should identify domains and applications where improvements can be made.

The Metrics of Maturity

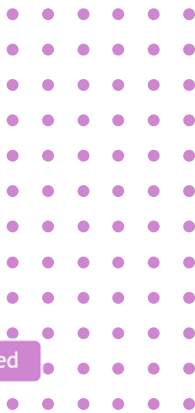
Simeio's maturity model covers your entire identity fabric. Let that be fully emphasized. Maturity assessments should not limit themselves to one or two systems.

Your assessment should cover the full breadth of your identity makeup. This makes a proper maturity audit a substantial undertaking across a vast domain. Therefore, your identity solutions must be examined in terms of how each one impacts the performance, security, and usability of the others.

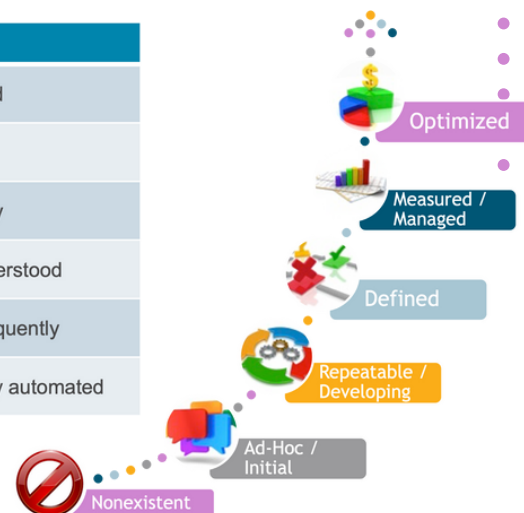
A highly efficient system might be full of security gaps just as a locked-down application might seriously impact user-experience. These interactions exacerbate the already staggering level of complexity within your most technically intensive systems.

This goes a long way towards explaining why enterprises greatly benefit from contracting out to a managed identity service provider to handle their assessment, both for impartiality and to take the burden off internal employees.

The metrics of identity maturity comprise of eight separate domains. As previously mentioned, each requires careful consideration not only of its individual makeup, but how its operation affects its interconnected siblings.



Maturity Level	Description
0 Nonexistent	Not understood, not formalized; need is not recognized
1 Ad-Hoc or Initial	Occasional, not consistent, not planned, disorganized
2 Repeatable or Developing	Intuitive, not documented, occurs only when necessary
3 Defined	Documented, predictable, evaluated occasionally, understood
4 Measured or Managed	Well managed, formal, often automated, evaluated frequently
5 Optimized	Continuous and effective, integrated, proactive, usually automated



The 9 Domains of Maturity

Access Management – The process of controlling which identities have access to an organization’s systems and data. This includes passwords synchronization, federation, and SSO.

Identity Administration – The system used by administrators to manage identities and access for your enterprise. This includes manual and automated provisioning tools, password tools, and role-based entitlements. Basic IT provisioning can be automated, but often requires manual oversight.

Identity Services – The user-facing systems in place for personal identity management. This includes account recovery, password recovery, and automation for both.

Access Governance – The program of monitoring and controlling who within your organization has access to what, as well as when and how. This includes compliance certification, SOX (Sarbanes-Oxley Act) applications, and data synchronization.

Privileged Identity Management – The systems in place to manage privileged identities. This includes segregation of duties, enforcement of minimum access policies, monitoring of privileged accounts, and enforcement.

Risk Analytics and Monitoring – The systems and protocols in place to mitigate and address security issues. This includes active monitoring, security planning, and remediation capabilities.

IAM Governance – Your enterprise’s methodology for managing, tracking, and maintaining the authorized identities’ access to resources. This covers the formal structure and long-term plans for the enterprise’s identity fabric.

Entitlement Services – The process your enterprise uses to delineate roles and entitlements. This includes your enterprise’s approval process and tools.

IAM Program Overall – The blended gestalt of all smaller aspects. This includes identity investments, overall strategy, user buy-in, IT attention, and current level of modernization.





Simeio's Grading Scale

A grading scale helps act as an easily referenced shorthand for how far along your enterprise is in its identity maturity journey. While all models have their own milestones, Simeio's charts specific and actionable stages in keeping with COBIT. These inform clients of not only where they are in their progress, but where they still need to go.

0 – Nonexistent: The domain is neither understood nor formalized. The enterprise does not recognize their needs in this area nor are plans being made to address this.

1 - Ad-Hoc or Initial: Attention paid to the domain is occasional and inconsistent. Planning for future development is either not performed or is highly disorganized.

2 - Repeatable or Developing: Investment in the domain is present and active but is based on under-informed intuition rather than expert advisement. Advancement is undocumented and occurs only when circumstances necessitate it.

3 – Defined: The domain is properly documented, its operation is predictable, it receives occasional but regular evaluation, and is generally understood by pertinent employees and users.

4 - Measured or Managed: The domain is well-managed with little to no user issues. Its structure and planned development are formalized and often benefit from the implementation of automation. Evaluation is frequent, regimented, and informative.

5 – Optimized: The domain receives proactive development and performs effectively at all levels. The domain is fully and smoothly integrated with its sibling domains. Unless benefiting from manual oversight, domains at this level usually employ extensive automated.

IAM Framework Component						Key Notes
<i>IAM Program Overall</i>						Overall IAM has had investment over the years but without any real strategy or focus. Of recent, systems and process have started to descend into atrophy due to lack of people and investment.
1. Access Management						Passwords are synchronized to key systems and AD is used as the basis for federation. Enterprise SSO is a recognized need and is immerging.
2. Identity Administration						BasicIT provisioning is automated but often requires manual oversight. Processes for Extended IT have been defined in Entitlement Services. There is also a proliferation of tools: custom, password sync, provisioning tools, and role administration tools that can be rationalized.
3. Identity Services						Functionality as slowly been reduced for the provisioning engine and more scrips have been created outside of a unified strategy to sync data between systems
4. Access Governance						Security has made inroads into certifying compliance and SOX applications with a small number of security groups.
5. Privileged Identity Management						Only segregation of privileged identities exist today. There are no tools for oversight outside of some rudimentary tools to remind of password reset. Privileged accounts have less controls enforced.
6. Risk Analytics and Monitoring						Further inroads into "Who" did "What" are required.
7. IAM Governance						Leadership recognizes the need for IAM, but has yet to put in place a charter specific to IAM that has formal structure and goals.
8. Entitlement Services						Approval process is a combination of manual and defined and some new tools help automating approvals (once approver is identified) [Excluded from overall]



Boosting your IAM Maturity

If you plan on reaching out to a dedicated managed identity provider for your maturity assessment needs, you can expect to receive the bespoke list you need. Every enterprise should rely on their specialized audit as the final word on actionable improvements. However, there are a few universal identity practices you can begin instituting now to boost your IAM maturity. This gives you a much better initial result from your formal assessment.

How the Four Pillars Contribute to your Maturity



Access Management

Access Management: AM is all about getting access to the things that you need (and preventing access to the things that you don't). AM utilizes tools and mechanisms to validate user credentials against an authentication store. Thus, it confirms or denies the identity's access to resources. Mature AM boasts good integration, strong monitoring, and fast user onboarding.



Customer Identity and Access Management

CIAM enables organizations to securely capture and manage customer identity and profile data, as well as control customer access to applications and services. Mature CIAM provides an excellent user experience while also keeping customer data secure.



Identity Governance and Access

IGA is a set of processes controlling the standards and service levels within the IAM Program. IGA's primary focus is on the user life-cycle processes (joiner, mover, leaver) and fulfillment activities associated with establishment and maintenance of accounts. Mature IGA ensures that newcomers quickly receive the resources they need while outgoers are quickly de-provisioned.



Privileged Access Management

PAM is also more than just a tool controlling accounts. It is a specific set of controls and processes associated with accounts with elevated or administrative access. This manages the "keys to the kingdom," making its efficiency and security a top priority. Mature PAM is locked down by the highest level of authentication and utilizes automatic tools to detect and remediate all breach events.

Individual Practices

The specific recommendations of an identity assessment vary from one enterprise to another. However, there's a few practices any enterprise can adopt to improve their identity maturity. Investigate how your business handles each of these areas and see how you measure up to their optimal outcomes.

Federation

Unifying your applications and identities into a single system should always be at the forefront of your strategy. Doing so allows authorized users to access multiple applications and domains using a single set of credentials. Additionally, federation can span multiple companies or enterprise boundaries. It links a user's identity across multiple identity management systems so they can access different applications securely and efficiently. MFA adds additional level of identity proofing and protection. SSO eases use of resources across multiple systems and applications allowing one authentication to work for many.

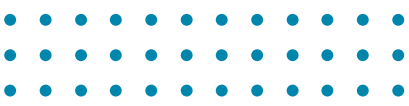
Identity Lifecycle Management

Having a plan for such a crucial investment as identity should be a given. Your Identity Lifecycle Management (ILM) sets out consistent policies for your provisioning processes for your company's joiners, movers, and leavers. Through clear mapping of entitlements based on principles of just-in-time and role-based access, you get users the tools they need quickly and easily. However, a well-structured ILM also provides for real time auditing of user permissions, automatically de-provisioning users who no longer have need of specific applications. The result is a tightly controlled system that keeps powerful tools out of the wrong hands while swiftly putting them into the right ones.

User Awareness

Buy-in is the crucial ingredient for any identity rollout, be it from C-suite during initial planning or with ground-level users practicing good identity hygiene. Your employees must not just be educated directly about how best to use your identity systems but given the tools and incentives to stay up to date and smart. This is a major reason why technical debt is such a rampant issue even among major corporations, as short term shortcuts cause long-lasting issues. Good user-experience greatly contributes to the adoption and continuation of policy adherence, despite how often it is considered a luxury expense by decision-makers. When it's easy for an employee to use their identity tools safely, they are far less likely to make mistakes that leave your identities exposed.





The IAM Maturity Advisory Program

Your IAM protocols need constant updates and maintenance to stay relevant. Your organization can't expect to stay ahead of technology by being reactive. Every security-conscious organization needs a long-term roadmap for their security systems.

One of the best resources available to the improvement of your IAM Maturity is [PathMaker Group's MAP benchmark test](#). The program gauges how your enterprise measures up against industry best practice. By addressing these granular KPIs, you gain an effective roadmap towards improving your 8 Domains of Maturity.

Does your organization's security posture need improvement?

- Are you following current trends and anticipating future needs?
- Do your security measures provide active and flexible control of internal access, as well as prevent outside forces from gaining entry?
- Would your security measures thwart a sophisticated attack, or are your current protocols only effective against low-level threats?

Do you know what components are necessary for a fully mature IAM program?

- Do your systems effectively implement User Identity Stores, User Account Provisioning, Credential Management, and Authentication?
- Do they cover Authorization, Identity Governance, Reporting and Auditing, Operations, and Program Governance?

Can you benchmark your IAM program against your peers?

- Is your IAM program a strategic asset that supports your organization's ability to efficiently utilize your technology stack?
- Does it protect the integrity of your data, secure your intellectual property and give your administration control to actively manage users and applications?
- Are your assets more (or less) protected than your competitors?
- Are you at a strategic advantage now, or do you need to catch up?

Security is not a destination, but a continuous journey. Assess your organization's security posture, follow current trends, and anticipate future needs to stay ahead of potential threats.



The IAM Maturity Advisory Program

Are you able to justify your IAM budget requests with real data?

When you request funding for critical IAM projects, can you illustrate the need using real data?

- Can you easily summarize system utilization, unique users and distinct profile types?
- Can you itemize change requests like user profiles created or new systems integrated within the past month, year, or longer?
- Can you easily show trend data to illustrate change over time?

Can you report your IAM success via a long-term, year over year, progress report?

-Are your systems connected in a meaningful way that supports reporting on critical data points, or is your IAM system just a control mechanism that sits atop your technology stack.

-Does your IAM program offer control and analytics, or just control? Are your analytics meaningful and accessible for future reporting? Does your system allow you to understand how you are advancing or just give you the ability to execute and no useful insights?

Would you like to identify targeted gains for your budget requests?

- When you go to management to request budget, can you clearly articulate the benefits of your projects?
- If your budget requests only cite general benefits like security enhancement or access improvement, will management see them as critical when it's time to allocate funding?





Assessing your Maturity

Carrying out the assessment yourself

If you choose to carry out your own assessment, bear in mind that you will very likely miss several major issues. Because your perspective is as someone inside your own business, it can be difficult to remain objective. What's more, you will likely have difficulty in establishing an accurate baseline. You've probably only ever worked in your role at that one company, perhaps two or three if you're very experienced. The benchmarks you set for yourself should mirror the metrics illustrated above. First, list out all eight domains and perform as comprehensive of an audit for each as possible. You will need to push yourself to not leave out any domains of your IAM, as each is vital to the operation of the others. Consider the resources you have already invested in solutions, the price of maintaining them in their current state, and the return on your investment you have thus far received.


Collect user feedback on pain points they've experienced and the KPIs C-suite wants to see. Then draw out as accurate of an estimate for implementation cost as you can. Investigate tools and applications that address your needs. And finally, research how other companies have tackled their maturity improvement. Performing this laundry list of analysis is likely to take your IAM governance committee several months of dedicated work. Make sure you have a substantial budget set aside for unforeseen costs that come up during the assessment. Temper the expectations of C-suite for the accuracy and comprehensiveness of your assessment.

If you are thinking of attempting the entire evaluation on your own, don't. Even if you think your enterprise is small enough for you to run a full-scale evaluation without a dedicated committee, the sheer complexity and interplay of all the various factors will overwhelm. It may even overwhelm your internal team.

Do the Smart thing: Get an IAM Service

If the above sounds like a tedious, expensive, and ultimately underserving endeavor, then you've recognized what far too many enterprises do not. A single identity domain requires considerable expertise and experience to properly evaluate, much less suggest actionable improvements. Then multiply that challenge by eight and it can become untenable for an inexperienced internal committee. Therefore, forgo the committee. Third parties are where you'll discover your solution. A proven managed identity service provider will have already seen many cases like yours. They bring experience not only with assessing maturity but improving it through intelligent solutions tailored to your specific needs. They also bring to bear teams of identity geniuses ready to perform your evaluation quickly,

effectively, and at a manageable cost. Most identity service providers will give you a free estimate, which you should always take even if you don't plan on engaging their services. The cost and timeframes outlined in the estimates can inform your internal assessment. Additionally, if you find the internal assessment comes up short, you have an avenue to expedite the contract. What's more, service providers rarely restrict themselves to just the evaluation stage. They become intimately familiar with your identity fabric over the course of their assessment, not only gathering metrics, but analyzing them with expert eyes. They stand in the prime spot to advise on maturity improvement, and many include such advisement as part of their assessment offering.



Do the Smart thing: Get an IAM Service Cont.

The best of the best identity service providers go one step further. They back up their advice with direct implementation, putting the necessary improvements into practice within your enterprise. Whether that means federating your identities onto a single platform, bolstering your security through zero trust coverage, or streamlining your application onboarding pipeline, they will execute with the same skill they demonstrated in the assessment stage.

Full end-to-end identity service providers like Simeio will take this even further. They maintain these solutions on an ongoing basis once they're put in place. Considering how important regular identity audits are to maintaining efficiency and a strong risk posture, your enterprise should be engaging such a service even outside of maturity assessments.

Simeio: Expert advice, seamless implementation, ongoing maintenance, and regular audits for optimal identity solutions.



Doing the assessment, yourself versus through an expert service

- Difficult to be objective.
- Likely inexperienced with industry standards.
- Vastness of identity solutions daunting and often untenable for your IAM Governance Committee.
- Long and drawn-out assessment times.
- Substantial operating costs prone to inflation.
- C-suite likely underwhelmed by incomplete or imprecise results.
- Actioning on the results requires an even larger investment.
- Outside perspective and drive to deliver a satisfactory result.
- Extensive experience with identity standards and practices.
- Identity service providers can deal with any enterprise of any size.
- Swift assessment with a clearly demarcated timetable and roadmap to completion.
- Pre-set costs laid out at the onset of an assessment.
- C-suite receives a professional result produced and curated by identity experts.
- The same identity experts can start implementing improvements as soon as the assessment is complete.

Conclusion

Charting out your identity maturity is crucial to your enterprise's success, yet it remains an intimidating undertaking. Fortunately, by approaching the issue intelligently, you can reign in costs, keep the project on schedule, and ensure accurate results. An internal IAM governance committee may be capable of executing the assessment. However, the benefits of contracting to an identity service make investigating potential providers important.

Furthermore, by understanding what goes into a mature identity fabric, you can start taking steps even before an assessment to grown in your maturity. Whether you're preparing for an assessment or acting on the recommendations of your experts, the maturity of your IAM program should always be moving closer and closer to optimization.

Starting on your journey to stronger identity maturity is a challenge in itself. Where do you even begin when every aspect of your identity and access management platform is called into question?

The best place to start is the same as the best place to finish: with a dedicated managed identity service. Simeio can take you by the hand and guide you through your assessment, advise you on improvements, execute your rollout, and maintain your solutions in our end-to-end offerings.

Visit [Simeio.com](https://simeio.com) for 40% off your IAM implementation audit and put the words of this whitepaper into practice!

