ELIMITY

WHITE PAPER

IAM from a CISO's perspective

This guide helps you understand the different disciplines in IAM and the security controls that you should adopt to cover your bases for all of them.

Identity and Access Management from a CISO's perspective

www.elimity.com

Introduction by our CEO

Over the past decade, trends such as cloud, SaaS, bring your own device and working from home have rendered the perimeter-based security model obsolete.

The only piece that still connects all the pieces in your IT environment is identity, i.e., your user accounts and there accesses.

Therefore, it is paramount from a cybersecurity perspective that every organization takes control of its users and access by applying the discipling called Identity and Access Management (IAM).

Many security professionals face challenges with IAM however. Firstly, IAM is a complex field full of terminology. Secondly, the best approach to IAM heavily depends on your IT environment and the maturity of your organization. And thirdly, a typical IT environment is far from trivial these days. As such, there are no quick answers when it comes to IAM, there are no silver bullets. Unfortunately.

That's why we've created this guide.

In this document, we disect the topic of IAM from a cybersecurity perspective. The guide discusses the different disciplines in IAM and the controls that you should apply to cover your bases for all of them.

It is our aspiration that this guide will help cybersecurity professionals start their IAM journey. And should you still have questions or comments, we are happy to help you.

Happy reading!

Maarten Decat

About Elimity

Elimity has built the most cost-effective platform for identity governance in the market. CISOs of companies from many industries use Elimity Insights to take control of the users and accesses in their IT environment in a matter of days, not months.

You can get started today at elimity.com/en/start-now

1. Why should you care about IAM?

And why should your manager give you a budget to improve it?

Cybersecurity has changed a lot over the past decade and the reason is that the IT landscape itself is not the same as 10 years ago. Back then, the core of IT security was the corporate network within which a lot was permitted, but data wasn't supposed to leave that perimeter.

Now however, we all use cloud and SaaS, in which case a part of your data is outside your network perimeter, by definition. We all collaborate with business partners, which forces you to open up your perimeter. Our employees all use personal devices and COVID has opened up the perimeter for working from home.

All these factors are the reason that a perimeter-based defence approach has become obsolete.

What remains, what still connects all the pieces in your IT landscape, is identity, that is: your accounts & their permissions.

Because of this, identity is a central part of almost every hack. Whether you look at renowned hacks such as the Uber hack or the Okta hack, or you look at a hack closer to your home, the *modus operandi* always involves a user's credentials being stolen at some point and then the attacker moves up throughout the infrastructure.

It's clear, therefore, that taking control over who can access which data and application is essential for cybersecurity.

Perimeter-based cyber defence has become obsolete. The one thing that remains is identity: your user accounts and their permissions.

94%

of organizations have had an identity-related security breach

Side note: The business case for IAM, more than cybersecurity alone

This guide explains the importance of IAM from a cybersecurity perspective. Cybersecurity is not the only driver for IAM however.

There is also a clear link to **compliance**, as all major cybersecurity standards require organizations to prove control over access to critical data and systems.

And, on the other side of the IT spectrum, having proper IAM can have a big impact on **operational efficiency**: it can bring down the time-to-work for new employees from months to days, it can decrease the burden on your helpdesk for password resets etc.

Finally, cleaning up excessive accounts and permissions can also lower your license spending and save you money.

In summary, IAM might not be a trivial field, but proper IAM will not only improve cybersecurity and compliance, but also operational efficiency and license spend, making it a very good business case.

ISO 27001	A.9 Access Control
NIST 800-53	Control family: Access Control
CIS CONTROLS	14. Controlled Access Based on the Need to Know

ISO27001 NIST SOC2 NIS SOX GDPR CIS

2. Unraveling IAM

Many CISOs are faced with the challenge of deciding what to spend their budget on regarding IAM. To help you get your priorities straight, let's first unravel what IAM encompasses.

From a high-level point of view, IAM consists of three disciplines:

Discipline	Role in cybersecurity	Common activities
Authentication	Minimize the changes of credential theft	Single sign-on (SSO) Multi-factor authentication (MFA) User provisioning
IGA Identity Governance & Administration	Manage the lifecycle of the identities of your employees and their access privileges	Joiner/mover/leaver processes Access requests & approvals Access reviews & revocations
PAM Privileged access management	Govern the highly-privileged accounts (admins) in your IT systems	Password vaulting Password rotation Session management & monitoring

Of these three disciplines, authentication is the most technical. IGA is typically regarded as the most complex however because it involves much more people than just IT, but also HR, the business etc. The solutions in PAM typically have a smaller impact on the organization than IGA, but the introduction of PAM processes can be challenging as well because the involved admins have to change their way of working.

Note: Apart from these three, **CIAM (Consumer IAM)** is often regarded as a fourth discipline of IAM. This discipline entails IAM for external identities such as you customers. This discipline is mainly relevant if you are a software provider and its main challenge typically is the amount of consumer identities that have to be managed. Because this is such a specific discipline that only applies to specific types of companies, this guide will not cover CIAM further.

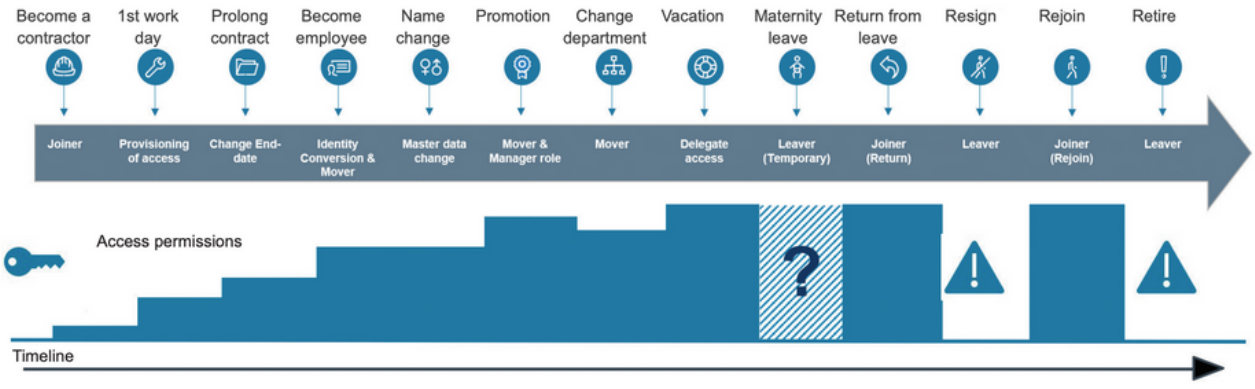
IAM Discipline 1: Authentication

Authentication covers how your users log in to your systems. This discipline focuses on activities such as password management, single sign-on (SSO), multi-factor authentication (MFA), passwordless authentication and user provisioning. This discipline is also called Access Management.

IAM Discipline 2: Identity Governance & Administration (IGA)

The discipline of IGA covers managing the lifecycle of the user accounts in an organization.

The first part of IGA is **identity governance**. Identity governance focuses on the digital identities of the employees in an organization from the moment that they join your organization to the moment that they leave. The reason that this is a discipline by itself, is that an employee's journey is much more complicated than one might think. People might join as a contractor, prolong their contract, become an employee, get promoted, change departments, go on extended vacation, return, resign, rejoin, retire and so on. The discipline of IGA wants to bring structure to this challenge with joiner-mover-leaver (JML) processes for your employees and their digital identities.



An employee's journey throughout your organization is more complicated than one might think. (Source: Omada IdentityPROCESS+, Version 2.0)

As the second part of IGA, **access governance** then also covers what these digital identities can actually access. This sub-discipline covers processes like requesting, approving, and reviewing access entitlements, all to make sure that your employees have the necessary access privileges to do their jobs, but nothing more.

IAM Discipline 3: Privileged Account Management (PAM)

The third discipline of IAM is PAM. PAM is a specialization of IGA and deals with the specifics of highly privileged users such as Windows administrators, root users on Linux or admin users in a database.

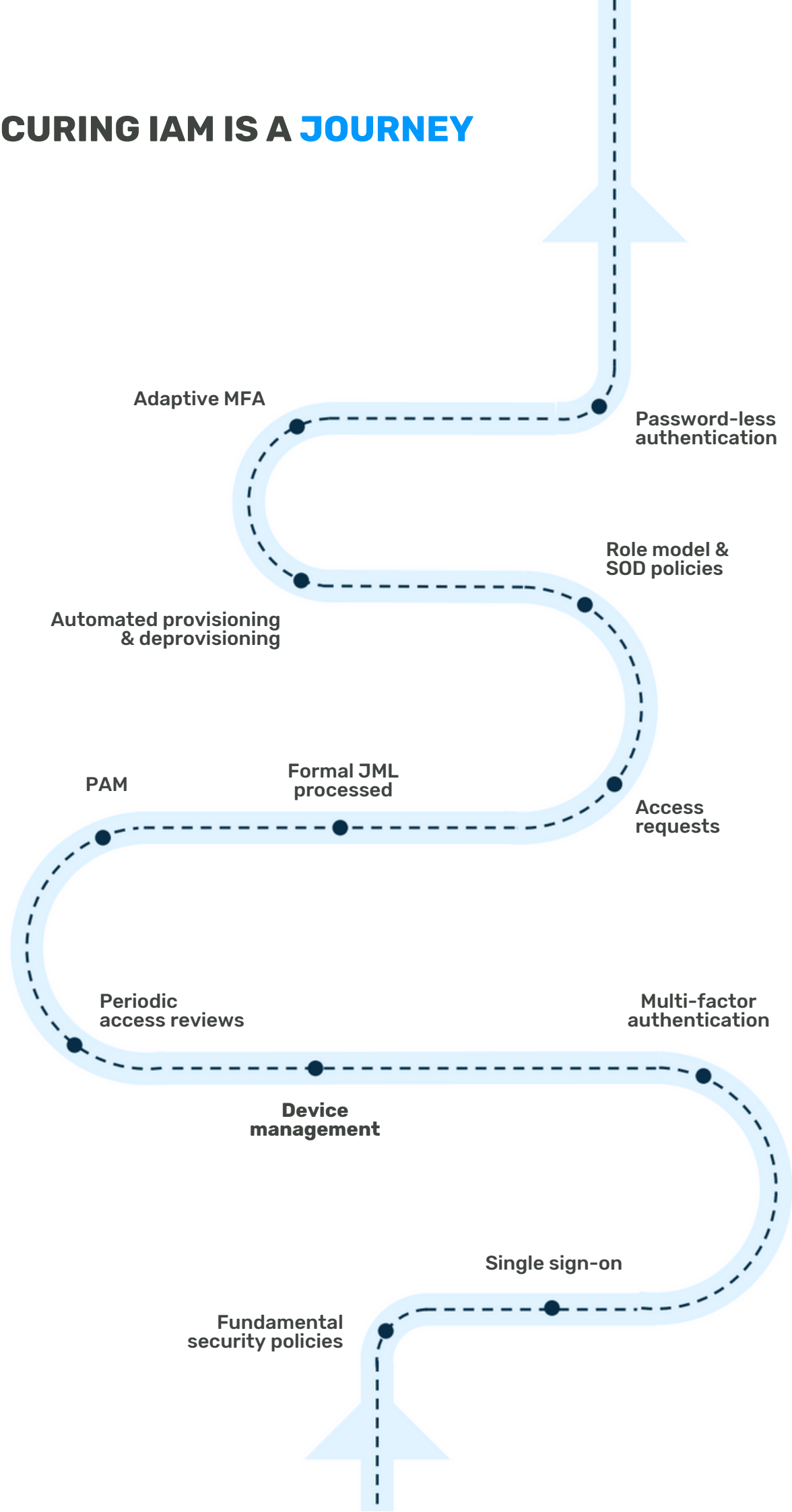
These accounts are especially critical to your cybersecurity and PAM tries to avoid dangerous situations such as hard-coded passwords or shared admin accounts because these situations increase the likelihood and the impact of admin credentials being stolen. Instead, PAM introduces more secure ways of working with password vaulting, automated password rotation, JIT provisioning and session management.

8 CATEGORIES OF KEY RISK INDICATORS

Want to know more?

GET THE GUIDE

SECURING IAM IS A JOURNEY



3. How to start

The previous part of this guide discussed the multiple disciplines of IAM. From a cybersecurity perspective, this is an and-story, not an or-story, meaning that you should cover your bases on authentication, IGA and PAM, not just one of them.

The question then becomes: what do you actually do? How do you start with IAM?

What is best done first will largely depend on your IT environment and the IT maturity of your organization From a cybersecurity perspective, **the best approach is to work risk-driven and optimize for maximal risk reduction at lowest effort.**

The approach is similar to more general approaches in cybersecurity:

1. First identify your critical systems. In this field, those typically are AD, AAD, Windows File Shares, production databases, production servers, maybe accounting, ...
2. Make a list of these systems and work from there for each of the three disciplines.

Must-do's for securing IAM

1. Authentication

Deploy SSO where possible

Enforce MFA where possible (definitely on the SSO account!)

Enforce password policies

2. IGA

Enforce a leaver process

Fundamental access governance: inventorize user accounts & accesses, review, clean up, monitor, repeat

Next: introduce access requests and approvals

Afterwards: role model

3. PAM

Identify privileged accounts on critical systems

Avoid shared, known or hardcoded passwords. Ideally use a secure password vault

Fundamental governance: inventorize, review, clean up, monitor, repeat

1. Authentication

For authentication, we strongly recommend doing two things:

1. Deploy SSO for your critical systems: integrate with AD for on-prem and Azure AD for cloud, sync between both ideally. This also makes it a lot easier to enforce password policies and password reset/recovery processes later on.
2. Deploy MFA: add MFA where possible, but definitely on the central SSO account. Regarding the different options as a second factor, experience shows that push notifications work best. If you have the advantage of a green-field deployment, you might opt for going passwordless from the start, for example with Microsoft Hello.

2. IGA

For IGA, the first thing to do is to enforce a leaver process: users will request access when they need it, don't worry about that, but removing access is the most important part for cybersecurity and this is often overlooked. And if you already have deployed SSO, this process becomes a lot easier.

Secondly, introduce fundamental access governance. This means:

1. at least having a central view of users and permissions so you understand who can access what,
2. then cleaning up orphaned accounts, unused accounts, test accounts, admin accounts and unneeded accesses,
3. and repeating this process every 3-6 months.

There are proprietary products out there to facilitate this process, gather the data from the different systems, show you where your risks are and clean these up.

Once you have that, you might introduce processes to request and approve access as well. In this case, don't immediately start looking for specialized products. Think of your processes first and start off with using your Jira or ServiceNow.

3. PAM

For PAM, we recommend a similar way of working as for IGA: identify privileged accounts and apply fundamental governance.

In addition, specifically for PAM, avoid shared or hardcoded passwords. This is how attackers eventually become admin in your systems. Educate your sysadmins in this and maybe introduce a secure password vault to shield passwords from sysadmins altogether.

Additional advice

1. Don't think that a product is the answer.

Sure, you need software for some things like SSO or building visibility of your current users but, especially for IGA and PAM, the basis is still that your employees think of their accesses. So also invest in education and training.

2. Involve all parties

When you approach these topics, involve all parties, not just IT. This means educating end-users, IT security teams, HR, application owners etc. Allocate time and budget in your project for this or it will fail!

3. Think big, but act small

You should have a sense of your ideal future IT architecture, but don't try to implement it at once. Try to work in smaller steps, optimize for risk reduction, show value early on and work from there.

Conclusion

IAM is a specific and complex field within IT, but critical to any company's cybersecurity. This guide explained the different disciplines of IAM and the basic controls you should apply for each of them.

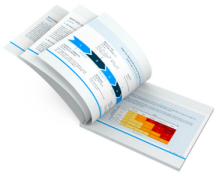
If you have any questions or comments, get in touch!

Additional resources

Elimity Insights: Platform for light-weight identity governance

START SaaS

Download and run locally



How to build the perfect risk cockpit for Microsoft AD

GET THE GUIDE

How to prove that you are in control

GET THE GUIDE

Any questions or comments? Get in touch!

Maarten Decat
Helping companies get in control of who can access what
maarten@elimity.com linkedin.com/in/maartendecat/

ELIMITY

Get started today at
elimity.com

Corporate Headquarters
Motstraat 30
2800 Mechelen, Belgium

Reach us by mail
info@elimity.com
sales@elimity.com