Jatin Shetty

7 min read · May 22, 2024

IGA & Identity Management- Simplified

Don’t know what IAM means? Neither did I for a long time.

While I was spending a few weeks thinking about what complicated, super cool topic I can write about in my first article, I realized that the field I am an expert in—Identity and Access Management, is something that a lot of people have never heard about, let alone understand it.

Even my wife, who is a fancy data scientist, doesn’t really understand what I do and why my role is critical in many organizations.

So decided to start with the basics :)

While IAM involves way too many topics when you dive deep, we will be focusing this article mostly on the IGA and Identity Management side of things.

What is Identity Management?

To understand what Identity Management is, there are a few concepts that you need to understand first

Like the name suggests, its about managing the life of an object. Usually referred to as LCM.

A lifecycle is basically different stages of an object. From the time its created, through the times it gets updated, moved around and all the way to the time it is deleted.

The term lifecycle gets applied to multiple things, from software, to projects, to cloud resources, to **user accounts** and many more.

For our topic here, we will bring User Account Lifecycle Management into the spotlight.

Terminology Alert! (but explained with a scenario)

Lets say you get hired at an organization. Once you accept the offer, there are a series of events that get fired off, mostly invisible to you.

- You get automated emails with details of tasks you have to complete to begin your hiring process.
- Background checks initiated.
- Laptops or mobile devices shipped to your home. (hopefully with some goodies)
- Username and password will be securely shared with you to login to your device.
- Once logged in, your email would have magically been set up and there are 173 emails that you need to go through!
- Your team shared pinging you links and resources on Slack/Teams/Hangouts

You somehow seem to have access to most of the systems need to work on. And that ladies & gentlemen is the **Joiner** process at work. (Atleast that is what its called as in the IAM world).

It is the process developed that enables all the listed tasks above to be executed in a clean, systematic way.

Alright lets keep going!

Now that you have joined the organization, you really like working there. You have built, managed and administered various tools and systems as a part of your role.

You learnt everything there is to learn in your team and now you want to move to a different team. You know, to keep life interesting. However, when you move to your new team, the systems that you will be working with will be completely different from your previous ones. And to add to this, you no longer need access to the systems from your previous team.

But wait! The morning you officially move teams, you login into your laptop and you feel different.

- Your manager has now changed to the new manager.
- You are now a part of the new team's email distribution list and have 1172 emails to go through.
- Its déjà vu! You magically have access to all the new systems and tools that your teammates are sending links to.
- You no longer are able to access the tools and links you had from your previous team!

Well, that is the **Mover** process in action. While the mover process would not be as drastic as what is mentioned above, this is one process a lot of organizations either completely skip, or have very different implementations from one another.

The story continues…

One fine day you buy a home you can't afford and your pay at your current company just aint doing it anymore.

So you decide to look for greener pastures and leave.

After you finish up your notice period, the next day you realized that you wanted to refer some document or code that you had created at your now ex-employer's application. You have all the links memorized so you hit the application, put in your credentials. You realize:

- Your credentials don't work anymore
- The laptop that your have to ship back to the company that evening isnt letting you in either
- All apps on your phone for messaging and emails don't let you in

What just happened?

What happened was arguably one of the most important part of IAM, the **Leaver** process. You would have lost all access to the system and your account would probably be disabled.

These 3 processes are core to LCM. Sometimes abbreviated as JML, the Joiner, Mover and Leaver processes have been around decades, but defining standards for these is a fairly new thing. You can read about these standards on the NIST website, but that might be too much at this stage.

There are also a multitude of companies that have tools to codify these processes. Prominent among them are Okta, Sailpoint, Auth0, OneLogin etc.

Now that you have a fair idea of what User Lifecycle Management is. There is one more important concept that needs to be explained to tie of this together.

Access Reviews / Access Certifications

Simply put, access reviews is when your manager comes and looks at the systems you have access to. The manager is then responsible to make a decision on whether you can continue to keep that access or remove some or all of the access. This is usually an Audit requirement and it is done on a regular basis. Quarterly or twice a year or sometimes monthly. All of these vary depending on how sensitive the access is and/or who's access is being reviewed.

Why is IAM important?

The above sections might have explained what some concept within IAM means, but it doesn't not clearly mention why its important and what the drawbacks of not having IAM implemented within an organization is.

Lets look at these in the same format as the sections above:

- **Joiner:** Not having a Joiner process defined, cause a lot of confusion and waste of time and resources every time a new employee is hired. I remember the time, more than a decade ago, where I joined a small organization, and it took 4weeks for me to get setup. To add to that, every new hire cannot be hired the same way. Each department hire needs to follow a different process entirely. You cannot give an Legal Department new hire access to an Account Team's application and vice versa.
- **Mover:** Imagine being the same organization for about 15years and think about all the systems, tools and teams you would have gained access to during this time. It'll usually be a lot. Now imagine, this user's account gets hacked! Your blast radius would be huge! Your access would not have been removed when you moved into an entirely different team and different role.
- **Leaver:** Like mentioned above, while Joiner and Mover are important processes to have, not having a leaver process (even a manual legacy process) could mean disaster and you wouldn't have to wait too long. Terminations that are immediate are usually rocky and disgruntled employees would want to cause harm or steal valuable information if their accounts are not disabled in a timely manner.

A Mature IAM System

There are different levels of maturities an organization can reach in its IAM implementation. Not all organization need to reach the high maturity level. But below are some of the key features an average maturity level of IAM implementation looks like:

- New hires are granted all the necessary roles and permissions needed to perform their duties on day 1. And each department new-hire is treated

different in terms of the types of access they need.

- When a user in the organization needs access to an application/database/shared folder etc., they can submit a request to gain access, and the request flow through the system and automagically grants them the access (after approvals) without any manual intervention.
- A user moves to a different team, and as long as the HR system reflects the team change, the user should have gained access to the new team's resources. Again, without any manual interventions.
- Auditor should be able to easily trace down how and when a user gained access to a system, who approved it, and what was the justification of the request.
- People managers would be able to review and certify the access of all their direct hires on a regular basis and revoke access as needed. Helps with access blot

Other Concepts:

There are other concepts in this space that are worth mentioning.

- Role Based Access Controls (RBAC)
- Attributes Based Access Controls (ABAC)
- Segregation (Separation) of Duties (SODs)

Summary

You will come across IAM as one of the domains in Cyber Security if you ever find yourself preparing for a CISSP certification. But, it is something that you touching everyday without even realizing it.

Note: This is definitely not everything that IAM has, but I'll leave it at this. Keep an eye out for more articles around this topic.

Resources

- https://www.nist.gov/identity-access-management
- https://en.wikipedia.org/wiki/Lifecycle_management

Identity Management | Iam Roles

Written by Jatin Shetty

4 Followers · 19 Following

Soldier in the Cyber Security Warfare.

Edit profile

No responses yet

What are your thoughts?

Respond

More from Jatin Shetty

Jatin Shetty

Database vs Data Warehouse vs Data Lake

Its confusing at first, but all it takes is a few minutes to understand what they are and the differences.

Aug 28

See all from Jatin Shetty

Recommended from Medium