Identity Access Management (IAM)

Identity Access Management (IAM)

Identity Access Management is the process of managing, recording, and controlling all the ways people interact with your company's network. It's a complex system that controls authorization and authentication, which is essential to minimizing risk.

Authorization is when you grant access to certain parts of your company's network and infrastructure to certain people. This can mean giving employees or third parties access to accounts on your website or allowing them to use your software programs in specific ways. Authentication is verifying whether someone is who they say they are before you grant them access (for example, by entering a password).

IAM software helps you do this for every person who interacts with your company's network—so you can rest easy knowing that only the people who should have access to sensitive information do.

How does IAM work?

IAM is the answer to a question that has plagued mankind for ages: What about the people?

Today, organizations are using more and more devices to accomplish their work. That means that more of their work is being done on more devices than ever before. And so, naturally, they have an increasing need for a way to ensure that only the right people have access to the right devices and data. But how?

When you create an account for yourself on Google or Facebook, those sites ask you some questions about who you are and what kinds of things you like so they can tailor their services specifically for you. They also assign each person who signs up a unique username and password combination so no one else can use their account without knowing those login details first. This means that only people who the owner of an account has permitted will be able to view its contents—which makes it much easier for them to keep their information private.

When IAM solutions are implemented thoroughly, they can help companies comply with government regulations and industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS). IAM also provides greater control over user access and can help reduce the risk of lost, stolen, or compromised credentials. Adopting IAM solutions can also enable an organization to implement single sign-on (SSO) solutions more effectively, which can further reduce risks by eliminating the need for users to memorize multiple passwords.

Why does an organization need IAM?

It's simple. To protect what matters most.

Your employees' data. Your customers' data. Your business's data. The very lifeblood of your organization. It all lives in the heart of your company's technology infrastructure and network, often on multiple devices and platforms. That makes it incredibly valuable—but also vulnerable to attack by malicious forces looking to steal or compromise that data, whether individuals with a grudge or black-hat groups trying to make a buck off of stolen information.

Once upon a time, protecting your data was as simple as ensuring that your physical space was protected, and any sensitive documents were locked up securely in filing cabinets. However, if you think about it, the real heart of your business isn't those documents—it's the software that processes them, the servers that store them, and the computers that work with them. And those digital assets are far more vulnerable than a locked cabinet in a locked room in a locked building ever could be—because they can be accessed from anywhere on earth by anyone who knows how to do it.

Relevant industries and use cases

IAM is more than just a tool for businesses to protect their users and customers. It's an opportunity for companies to reevaluate their processes and create a more holistic, cohesive experience for the people who use the company's services.

What does that mean, exactly? Let's take a look at some real-world use cases that illustrate what this can look like:

- A major auto manufacturer has introduced new technology into its vehicles to offer consumers an unprecedented user experience. Because of the sensitive nature of these new technologies, the auto manufacturer needed a way to ensure that only authorized users were accessing the vehicle and using its features.
- A large healthcare provider wanted to ensure patient confidentiality by limiting access to electronic medical records only to authorized staff members. They had previously tried several other methods of monitoring access but found it difficult to monitor in real-time and keep up with audit requirements.

Identity access management is highly important for a variety of industries. Here are some examples:

- Healthcare
- Retail banking
- Government
- Education

But why is this so important? Because securing your digital resources is the foundation of protecting your physical resources. Suppose someone gains unauthorized access to your company network. In that case, they could steal not only sensitive information but also cause physical damage (imagine what would happen if they could shut down your manufacturing line remotely!).

As long as there are people in the world trying to get their hands on what isn't theirs, Identity and Access Management will be critical for ensuring our safety.

How does the IAM process work?

IAM addresses the need for:

- User Provisioning
- Access Control and Authorization
- Password Management
- Single Sign-On (SSO)
- Multi-factor Authentication
- Audit Management
- Compliance Reporting

There are four main IAM processes:

1) **Provisioning:** Provisioning is one of the most critical aspects of IAM. It's creating and configuring user accounts, groups, roles, policies, and other objects in a directory service such as Active Directory or LDAP.

2) **Access Control:** These policies and technologies help protect your data by ensuring only the right people (and devices) have access to the correct information. It also mitigates risks by monitoring suspicious behavior such as anomalous login patterns or logins from unfamiliar locations. IAM accomplishes this through authentication protocols like multi-factor authentication (MFA) and Single Sign-On.

3) **Reporting & Alerting:** The IAM Reporting & Alerting process allows for the automatic generation of reports and alerts that help identify potentially inappropriate access to IT resources. The process uses a defined set of criteria to proactively identify, assess and mitigate risks associated with the use of privileged accounts within the enterprise.

In addition to performing scheduled scans, Risk Management can also perform on-demand scans. The IAM Reporting & Alerting process can provide real-time reports and alerts about potentially inappropriate user access.

4) **Delegation:** The delegation process refers to handing over the responsibility for decision-making to another person or entity. For example, an organization can delegate rights and duties to an individual or group of individuals to reduce workload or ensure that tasks get done efficiently. Delegation is a vital part of effective management, which allows managers/supervisors to focus on more important tasks while employees handle routine tasks themselves with minimal supervision.

Does IAM improve regulatory compliance?

IAM is often thought of as the ultimate security solution. And while it is undoubtedly a powerful tool, it's not quite the one-stop answer to cybercrime.

It's important to remember that security solutions are layered and that IAM works best when combined with other tools like data encryption,

firewalls, and PKI.

This is because IAM doesn't stop hackers from getting into your system—it just makes it more difficult for them to make off with any user data once they're there.

That's why it's so important to look at IAM as part of a more extensive security system rather than merely a solution in and of itself. That way, you can ensure both compliance and safety for your organization.

How does IAM improve regulatory compliance? The answer is simple: With more precise control over who has access to what within your company, you can ensure that all users are only accessing data and functions for which they are authorized—and not for any other reason.

In fact, Identity Access Management (IAM) is one of the most effective ways to improve regulatory compliance in your organization. It can help you establish and enforce consistent security policies across all users and systems, from the moment they join your organization through the termination of their access.

That's because IAM lets you automate the process of onboarding new employees and contractors, giving them access to the specific systems and data necessary for the performance of their jobs. Automating these processes ensures that everyone gets convenient access at the right time and reduces the risk that someone will be given too much access—which can happen when an IT admin has to grant permissions manually.

IAM also helps you manage user access through every stage of their lifecycle with your company, which makes it easier to ensure that everyone has access to precisely what they need—and nothing more. IAM solutions allow you to automatically remove excess privileges after a user leaves your organization or changes departments or roles.

This type of granular control is critical for regulatory compliance—both because it ensures that you have a comprehensive audit trail and because it keeps unauthorized parties from accessing sensitive data.

What tools do you need to implement IAM?

When you're implementing an Identity Access Management (IAM) system, there are a few technology tools you'll need to have in place. These tools will help you manage your system and keep it secure once it's up and running. Here are some of the tools you'll need:

- **An IAM System**. Many different vendors offer IAM systems, so take time to think about what your company needs before deciding which vendor to go with. It's worth shopping around because the right system will save you a ton of time and money in the long run.
- **Access Management Software.** This software is used to control who has access to your IAM system and what they can do.
- **A Segregation of Duties Policy.** This policy dictates how many people should be involved in various processes (like approving a change) so that not one person has too much control over things like changing passwords or approving access requests—this helps prevent fraud and abuse of power by employees.
- **Auditing Tools for Compliance and Security Purposes**. These tools can help you keep track of who has access to your IAM system, when they log in, what actions they take, etc., which will make it easier for you to monitor access and compliance.

BACK TO INDUSTRY GLOSSARY