**Identity and Access Management**

In a recent study by Verizon, 63% of the confirmed data breaches are due to either weak, stolen, or default passwords used. There is a saying in the cybersecurity world that goes like this “No matter how good your chain is it’s only as strong as your weakest link.” and exactly hackers use the weakest links in the organization to infiltrate. They usually use phishing attacks to infiltrate an organization and if they get at least one person to fall for it, it’s a serious turn of events from thereon. They use the stolen credentials to plant back doors, install malware or exfiltrate confidential data, all of which will cause serious losses for an organization. And so Identity and Access Management (IAM) is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required. There has been a burst in the market with new applications, and the requirement for an organization to use these applications has increased drastically. The services and resources you want to access can be specified in IAM. IAM doesn’t provide any replica or backup.  IAM can be used for many purposes such as, if one wants to control access of individual and group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least-privilege permissions becomes easier. The AWS IAM is a global service.

**Components of IAM**

* Users
* Roles
* Groups
* Policies

 With these new applications being created over the cloud, mobile and on-premise can hold sensitive and regulated information. It’s no longer acceptable and feasible to just create an Identity server and provide access based on the requests. In current times an organization should be able to track the flow of information and provide least privileged access as and when required, obviously with a large workforce and new applications being added every day it becomes quite difficult to do the same. So organizations specifically concentrate on managing identity and its access with the help of a few IAM tools. It’s quite obvious that it is very difficult for a single tool to manage everything but there are multiple IAM tools in the market that help the organizations with any of the few services given below.

**Services By IAM**

* Identity management
* Access management
* Federation
* Multi-Factor authentication
* Access governance
* Customer IAM
* API Security
* IDaaS – Identity as a service
* Granular permissions
* Privileged Identity management



**Figure –** Services under IAM

**More About the Services:** Looking into the services on brief, Identity management is purely responsible for managing the identity lifecycle. Access management is responsible for the access to the resources, access governance is responsible for access request grant and audits. PIM or PAM is responsible for managing all the privileged access to the resources. The remaining services either help these services or help in increasing the productivity of these services.

**Market for IAM:** Current situation of the market, there are three market leaders (Okta, SailPoint and Cyberark) who master one of the three domains (Identity Management, Identity Governance and Privilege access management), according to Gartner and Forrester reports. These companies have developed solutions and are still developing new solutions that allow an organization to manage identity and its access securely without any hindrances in the workflow. There are other IAM tools, Beyond Trust, Ping, One login, Centrify, Azure Active Directory, Oracle Identity Cloud Services and many more.

**Identity and Access Management (IAM) in Cyber Security Roles**

Identity Access and Management is abbreviated as IAM. In simple words, it restricts access to sensitive data while allowing employees to view, copy and change content related to their jobs. This information can range from sensitive information to company-specific information.

It refers to the IAM IT security discipline as well as the framework for managing digital identities. It also deprives the provision of identity, which allows access to resources and performing particular activities.

When you exceed your target, IAM ensures that the appropriate resources, such as the database, application, and network, are accessible. Everything is proceeding according to plan.

**IAM’s objectives are as follows :**

* To prevent unauthorized parties from exiting the system, the purpose of this IAM should be to ensure that legitimate parties have adequate access to the right resources at the right time.
* It only gives access to a certain group of people, such as contractors, employees, customers, and vendors. You’ll also need the key to verify their identities and provide them access to everything throughout the onboarding process.
* To revoke access and begin monitoring activities in order to safeguard the system and data. IAM goals include operational efficiency in regulatory compliance, fraud detection, and lifecycle management, in addition to protection against cyber intrusions.
* When it comes to fraud protection, IAM is the best way to reduce fraud losses. Since a crime has been committed, the insider who has abused his access rights has been identified as corrupt. IAM assists in hiding traces to evade discovery. IAM is an automated system that analyses transactions for fraud detection using preset criteria.
* It also guarantees that the Company meets various regulatory criteria for the detection and identification of suspicious behavior and money-laundering situations.

**Benefits of Using an Identity and Access Management System :**  
We will learn about the various organizational benefits in this section. These are listed below –

* **Reduce risk**

You’ll have more user control, which means you’ll be less vulnerable to internal and external data breaches. When hackers utilize the user credential as a crucial technique to obtain access to the business network and resources, this is critical.

* **Secure access**

When your company grows, you will have additional employees, customers, contractors, partners, etc. Your company’s risk will increase at the same time, and you will have higher efficiency and production overall. IAM allows you to expand your business without compromising on security at the moment.

* **Meeting Compliance**

A good IAM system can help a company meet its compliance requirements as well as meet the rapidly expanding data protection regulations.

* **Minimize Help Desk Requests**

IAM looks into the user’s needs and then resets the password and the help desk will help them automate the same. Getting the authentication requires the user to verify their identity without bothering the system administrator as they need to focus on other things in the business, which gives more profit to the business.

Another advantage of the IAM framework is that it can provide businesses with an advantage over their competitors. Without jeopardizing security standards, IAM technology can give users outside the organization access to the data they need to perform their tasks.

**Implementation Guide for IAM :**

**1. Consider your company’s size and type**

IAM is important for company authentication and handles identity to allow users to exercise their rights from a remote location. It also aids in calculating the surroundings when multiple devices are used. IAM is highly successful for all types of organizations, large, small, and medium. Additional options are available for larger organizations, and you can choose the tool that streamlines user access.

**2. Create a strategy for IAM integration**

This is a well-known story with risks, and it has been implemented with IAM and moved to the cloud. Employees must use tools that are permitted by the company, sometimes called shadow IT. IAM will devote time and resources to developing a comprehensive identity management strategy.

**3. Find the best IAM solution for you**

There are a few key components of IAM that you may use to keep your business from collapsing, which are listed below :

* Access management products control a user’s identification while also enabling a few tools such as the network, web resources, cloud, and so on.
* Multi-factor and risk authentication method helps in verification of the identity of an individual.
* Where passwords fail, password tokens provide additional security.

As a business owner, you must learn about all of the IAM tools available to protect your company’s identity and access management.

**The rise in prominence of IAM**

In today’s environment, measuring organizational maturity against the basics of IAM is one of the most important parts of cybersecurity for organizations. It will provide you with an overview of the current security situation of your company when it comes to digital assets and infrastructure.

Here are some key ideas:

* **Identity data management**

This includes a review of the organization’s identification and data management processes as well as the technologies, networks, and systems used to handle the data.

* **Access management**

Instead of relying on a single password login, stronger authentication techniques are being used, such as multifactor authentication, union, and passport management.

* **Access governance**

Is required system access properly regulated? It is important to make sure everything is in working order. For this, security administrators must ensure that policies exist that allow IAM functions to be implemented, evaluated, and audited, as well as the appropriateness of the policies.

* **Identity management**

Is it possible to regulate access to critical systems? It is important to double-check that everything is in working order. For this purpose, security administrators should ensure that policies exist that allow IAM functions to be implemented, evaluated, and audited, as well as the appropriateness of the policies.

* **Data security and analysis**

Is required system access properly regulated? It is important to make sure everything is in working order. For this, security administrators must ensure that policies exist that allow IAM functions to be implemented, evaluated, and audited, as well as the appropriateness of the policies.