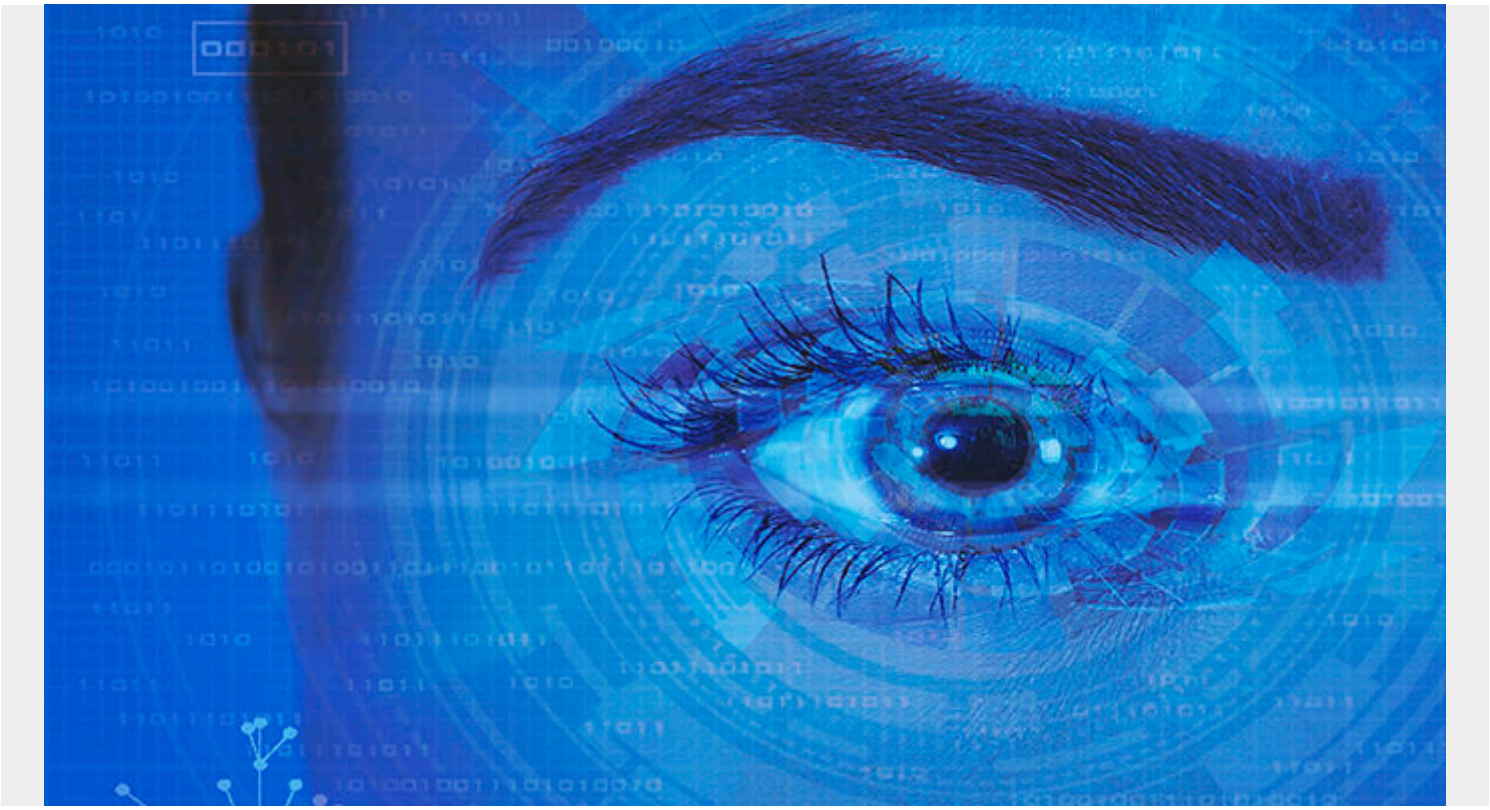
INTRODUCTION TO IDENTITY AND ACCESS MANAGEMENT



The complexity of modern IT systems cannot be overstated as things like machine learning, big data, and artificial intelligence gradually make their way from the realm of sci-fi to the world we live in today. In the Information Age, one of the world's biggest concerns from Bangkok to Boston is security.

Providing users with the access they need to accomplish their tasks while ensuring sensitive information remains protected is a delicate balancing act. No two users are exactly alike, and their access and permissions should reflect that to bolster the security of the entire system. This is the function served by identity and access management systems.

What is Identity and Access Management?

Identity and access management (IAM) is an enterprise system which defines and designates roles and access privileges of individuals on the network. The IAM system creates roles and dictates what resources those roles have access to and then manages the assignment of roles to individuals and ensures each individual can only access the resources which they have been approved to use.

This applies to both customer identity management as well as employee identity management. The primary goal of IAM is to ensure each user is assigned a single digital identity, and each identity is assigned the roles that apply to them and the access that each role permits them. Each user is assigned a digital identity (a unique username and password) and this identity is then assigned the roles which provide them with access to the data and applications they require.

IAM is also sometimes called identity management or rights management and is responsible for processing user requests to access resources. IAM systems are also responsible for reviewing the roles and access permissions to ensure all users have access to what they need and nothing they don't. Access management establishes permissions and is also responsible for revoking rights when users transfer to different roles within the organization or leave the business altogether.

Access management operates on the security principle of "least authority." This is essentially like operating on a "need to know" basis, where users are only given access to the information and resources they require to perform their job. This type of security baseline may seem cumbersome, but it is the best way to provide optimal security for the entire network. Maintaining a secure network is a top priority for organizations in today's world where data breaches are all too common. Breaches pose the risk of the organization incurring financial penalties in addition to resulting in damage to the enterprise's reputation.

What are the Benefits of IAM?

The implementation of IAM systems and best practices allows you to open up your network to employees and customers alike without exposing the network to undue risk. This can help to increase efficiency and reduce operating costs by allowing the enterprise to utilize a single network for internal operations and client-facing purposes. Identity management allows access to be extended for on-premises applications as well as mobile apps and SaaS tools without negatively impacting network security.

Properly managed identities provide administrators with enhanced control over user activities and permissions. This helps greatly in the reduction of internal and external breaches. Internal breaches are fairly common, but about one fourth of internal breaches are accidental. Whether intentional or otherwise, the impact of breaches is lessened when identity access management systems are in place that ensure each user only has access to the bare essentials for performing their job. IAM helps to ensure organizational networks remain secure and compliant with regulations.

Identity Access Management Key Terms

Here is a list of common IAM terms that will help you get a better overview of the how the system works and will aid you in navigating conversations regarding identity management:

- **Access:** The security clearance or extent of permissions given to a user. This can be thought of as key cards for secure facilities where each sector has a minimum level required and the level of clearance an identity has dictates how much of the facility they have permission to access.
- **Biometrics:** A type of authentication which scans a user's unique characteristics like fingerprint scans, facial recognition, voice recognition, or iris and retina scans. This is an added layer of security which helps to ensure the only person accessing each user's data is the user.
- **Credentials:** A user's credentials are the details they use to gain access to the network such as their password or biometric data.
- **Digital Identity:** The user's unique identifier that is connected to all their pertinent information such as which roles they are assigned to as well as the devices from which they access the network.
- **Multi-factor Authentication (MFA or 2FA):** When multiple forms of authentication are used to confirm the user attempting to access the network through the digital identity is, in fact, that

user. An example of MFA would be requiring users to supply their password as well as biometric data like a fingerprint scan, supplying a code sent via SMS to their smartphone or email, or even a physical "key" such as a smart card or USB stick that has access codes stored inside the medium.

- **Risk-based Authentication (RBA):** This type of authentication adjusts dynamically depending on the environment in which the user is attempting to access the network. RBA might request the user to provide additional forms of authentication if a user is attempting to sign onto the network from a previously unused IP address or from a geographic area from which they don't typically access the network. These are cases when MFA approaches are especially useful for avoiding potential risks.
- **Single Sign-on (SSO):** This access control provides users with the ability to enter their credentials to access the network and then provides them permissions to access any other services or resources within the network for which they have privileges without requiring additional authentication for each service they wish to utilize.

IAM best practices will help increase organizational network security by simplifying the management process through secure authentication and authorization methods. Access management systems allow enterprises to provide employees and customers alike with the tools they need without putting sensitive data at risk.

IT Management: Solutions for You

BMC offers solution implementation and consultation services to help you make the most of your ITIL investments. BMC offers automation and security solutions for IT networks and operations. BMC helps your organization embrace the power of automation to increase your speed and agility. Learn how automation can deliver your organization the data, insight, and tools it needs to make the most of its assets with BMC's Helix Discovery Datasheet.