Identity & Access Management (IAM)

Efficiently and Securely Manage Users, Roles, and Access Permissions

Enterprise Identity & Access Management is one of the most critical factors of a company's success in the digital age and is a key component of any professional IT security strategy.

IAM – Indispensable for Enterprises!

The primary objective of an IAM solution is to create and manage unique digital identities for employees, contractors, and other individuals with access to company assets. The creation of a new user is usually initiated by Human Resources (HR), then forwarded to Identity Management (IDM). This unique digital identity makes it possible to manage, update, and systematically organize the roles, groups, and access permissions of each user, as well as monitor individual activity throughout the user's access lifecycle.

Enterprise IAM systems provide the tools and technologies needed to achieve this, enabling large, complex organizations to consistently implement and enforce security policies, as well as any internal or external compliance requirements. Companies face a multitude of legal requirements and country-specific regulations, so a robust approach to identity and access management is essential. For example, companies based in Europe are subject to strict new requirements introduced by the EU General Data Protection Regulation (GDPR), effective May 25, 2018. Violations of these requirements may incur damaging or potentially even business-threatening fines. In the US, the Sarbanes-Oxley Act, the Gramm-Leach-Biley Act, and the HIPAA Act represent a few of the regulatory drivers for enterprise identity and access management.

Core Functionality: Authentication and Authorization

To properly enforce access rights, the system must first authenticate the user before granting any permissions. User authentication can be performed via biometric features, username and password queries, and other methods. Privileged users such as system and database administrators should always require multifactor authentication (e.g. with additional hardware or software tokens).

The authorization process determines the systems and resources that each user is allowed to access. The extent of any given user's access depends on the rules, policies, and roles defined by the company.

The overarching goal of any authentication and authorization system is to protect the company's assets and

productivity against any attack, whether from internal or external sources. Unfortunately, it is extremely common for users to have more privileges in the company systems than they need and use. Enterprise IAM provides an additional safety net that minimizes the risk of unauthorized access by ensuring that access authorizations, rules, and checks have been clearly defined and established. This applies to both hybrid cloud and IT landscapes as part of Software-as-a-Service (SaaS) models and on-premise solutions operated locally by the customer. Many benefits of enterprise IAM are listed below in more detail.

The benefits of IAM at a glance

Process automation

The first step in implementing IAM is to host a workshop to develop detailed definitions and descriptions of every IT business process. This is done in collaboration with the process managers, guided by a consultant or system architect. Any processes defined for an automated procedure can be scheduled with a set of triggers or manually executed. The workflow of this process then runs automatically in the background.

Simplified administration and improved data consistency

With IAM, employee information only needs to be entered once, e.g. by the department responsible for personnel management. Every connected system can then access this information (metadirectory). Self-service interfaces for users and automatic processes significantly reduce the administrative burden. When an employee's data - such as department - changes, his or her permissions are automatically updated according to the business rules configured in the system. Similarly, when employees leave the company, their user accounts are automatically locked and disabled, their permissions are suspended, their laptop and mobile phone are recalled, etc.

Rapid response times in an emergency

In the case of emergency, users can be blocked quickly and easily on all systems (email, fileserver, intranet, PC, etc.), significantly reducing organizational risk.

Increased productivity and efficiency thanks to central provisioning

Central administration and provisioning through IAM simplifies role and permission management of users on all connected systems. This eliminates the need to update each user's status on individual applications, which can be extremely time-consuming. Employee access can be approved quickly and automatically on every connected system by authorized approvers, allowing them to become productive immediately. This significantly relieves the burden on the IT department and eliminates costly delays.

Simplified login process thanks to Single-Sign On (SSO)

With the implementation of a SSO solution, users only need to log into the system once. All other login processes occur automatically in the background. This improves user satisfaction, increases security, reduces help desk volume, and lowers costs.

Reduced workload for the help desk

Systematically managing and administering all accounts and permissions significantly reduces help desk burden.

Secure access even for customers and business partners

There is often a need for customers or business partners to access your systems. IAM allows user access, access rights, data, and resources to be reliably managed even for non-employees and other external users.

Implementation of compliance requirements

Every operation performed within IAM is archived and accessible using auditing and reporting tools. This supports compliance with legal or regulatory measures relating to the transparency of access rights.

More straightforward recertification in the context of IT governance

Access certifications that your company needs to review periodically will be simplified by an Enterprise Identity & Access Management strategy.

Cost savings

The introduction of enterprise IAM greatly reduces the workload associated with managing users and their permissions. Additional savings may be seen in licensing costs, since each user is only given access to the applications that he or she actually needs in practice.

ASCONSIT: Enterprise IAM with a Proven Process!

To successfully design an Enterprise Identity & Access Management solution, the first step is to formulate a carefully thought-out strategy based on interdepartmental collaboration. Developing an overall picture of the existing business processes and system landscape is essential to the success of the solution. This global perspective helps to analyse and understand the key processes of the organization, so that existing workflows can be addressed, or new procedures can be proposed to improve processes. Another important

objective is the synchronization of user identities from each data source across all systems according to a policy that is sustainable in the long term. This requires careful planning and good process design. Most importantly, IAM will empower the company to efficiently manage a larger number of users, as well as all of their devices, across a range of different environments, in a manner compatible with automation, while ensuring that the highest security standards are met.

We at ASCONSIT support you in process design with our more than 15 years of expertise!