_betasystems

Methodology of an IAM introduction

White Paper from Beta Systems IAM Software AG

Bridging the gap between business and IT: the right approach
in the implementation of Identity Access Management (IAM) systems

www.betasystems-iam.com

METHODOLOGY OF AN IAM INTRODUCTION

Content

What is Identity and Access Management? 2

Why do you need IAM? 3

Approach to implementation 5

A Successful Project starts with a cleanup 6

Introduction of authorization roles 6

Iterative role modeling 8

Process design 10

System Connections 11

Recertification 13

Conclusion 13

What is Identity and Access Management?

Whether Identity and Access Management (IAM) or the simpler variant Identity Management - both terms basically refer to the same thing: systems that centrally control and monitor access to data and applications in the corporate environment according to the organizational requirements and professional role of each user. IAM thus includes all functions and work steps in connection with the administration of identities and the management of access rights.

Digital Identities

In order to provide an individual with the access rights that are needed in the context of their work for the company, a digital identity is first created for the individual in the IAM. With this digital identity, the person and their characteristics are then known in the IAM system. If this identity is directly assigned access rights by the IT systems by circumventing an IAM system, the management of the digital identity can be difficult to achieve due to the quantity and the lack of intuitive description quickly becomes confusing. With the help of a role concept, groups of access rights are combined into individual authorization roles. These bundled access rights can then be assigned to the identities in a comprehensible and traceable manner.

The digital identity is monitored and updated throughout its access lifecycle as the user continues to belong to the company as necessary. The IAM system is therefore not only able to define identities and grant them access rights (provisioning), but also to withdraw or change the rights again (de-provisioning) if the person's task changes. Typical reasons for these changes are entry, transfer or leaving of an employee. These changes are referred to as IAM standard processes.

The IT department allocates, changes and revokes rights manually in the IAM system or , the more common case, revokes rights automatically on the basis of predefined rules. Modern IAM systems have self-service portals where users can manually request which permissions you need. Approval for these requests is then granted by the respective responsible persons via automated application and release procedures.

Identity and Access Management has two areas of responsibility: Authentication - Access Management - in which the system ensures that the user really is who he claims to be. Various techniques are used here, although simple username/password queries are no longer sufficient in today's ever-increasing threat situation and complex IT landscapes. Therefore, methods such as two- or multi-factor procedures with security tokens, biometrics, machine learning or risk-based authentication are now standard features of a powerful IAM system. Once the user's identity has been clearly established, Identity Management comes into play. Identity Management authorizes the logged-on user with the desired access rights for the requested systems and resources.

Why do you need IAM?

Compliance

In recent years, the number of laws and regulatory requirements placed on companies has grown rapidly - from the **Sarbanes-Oxley Act** in the USA to European regulations such as the **GDPR** and the Minimum Requirements for Risk Management (**MaRisk**) of the Federal Institute for Financial Services supervision and others. The observance of such regulations, as well as self-imposed internal standards and requirements, is summarized under the term "compliance".

Compliance reasons are those that oblige companies, for example, to consistently store personal data while maintaining information security. Other regulations require compliance with the so-called least privilege principle or the separation of duties.

Significant risks

An indispensable component of the compliance strategy should therefore be a software solution for Identity Access Management. Without an IAM solution, companies are not able to reliably protect their data and demonstrate compliance with all relevant regulations. If data security is not guaranteed, especially in compliance-critical areas, considerable risks arise, both financially and in terms of their image.

Increasing compliance requirements "force" companies de facto to deal with the topic of identity and access management.

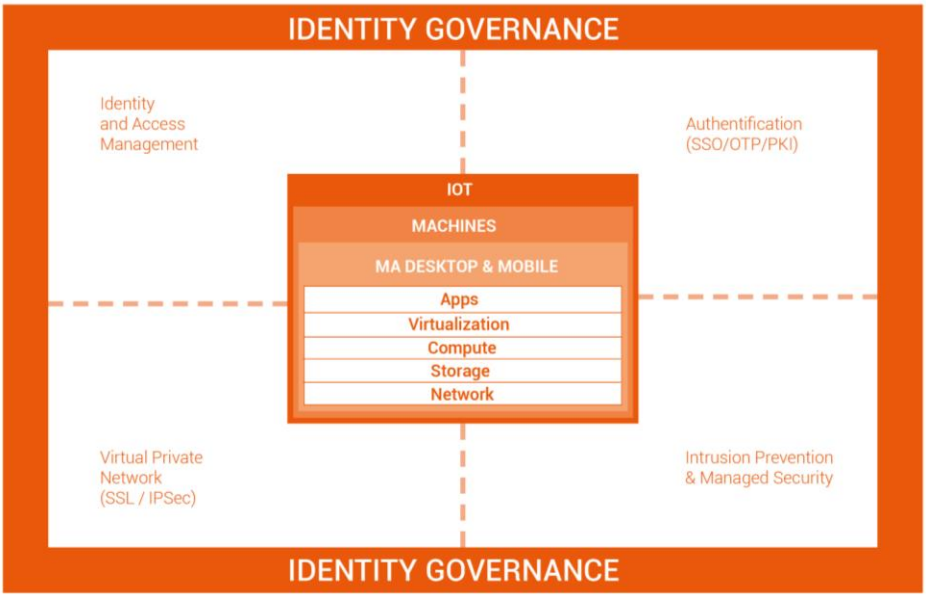
IAM is also gaining in importance due to the increasing decentralization of systems, the inclusion of cloud infrastructures and the increased use of mobile devices.

Without such a system, it is nearly impossible to track who uses which rights on which device and when. What's more, the larger a company organization is, the more identities and authorizations need to be managed. Identity Management no longer works reliably with traditional means such as decentrally created and stored Excel lists.

IAM in the context of Identity Governance

Identity Governance

The increasing compliance requirements lead to the necessary embedding of the IAM system in the superordinate Identity Governance (IG) strategy of a company. Identity Governance addresses the dependence of the centralized control of identity management and access controls on the regulations that apply to the company. At IG, it directly links IAM functions to compliance regulations.



IT Security

The market observation institute Cybersecurity Ventures forecasts that the worldwide damage caused by ransomware (**extortion Trojans, extortion software)** will amount to more than 20 billion US dollars in 2021. IAM supports the protection of digital company's assets against threats to its corporate IT.

By restricting access rights to the minimum required, the threat of phishing or ransomware is also significantly reduced because employees will only have access to assets they must have access to in order to do their work – and nothing more. Also, the unauthorized access of company employees themselves means that employees cannot add to risks with assets to which they do not need access.

Employees as a risk

According to the IDC study "IT Security in Germany 2018" , the company's own employees are now considered the greatest security risk for companies. Cleanly managed identities therefore mean the greatest possible control over access to corporate IT, whether from external or internal sources.

Cost reduction

From the controlled management of access to information systems and data not only reduces the risk of fraud and data loss - it also cuts costs.

This is because it establishes structured management processes whose individual components can be ported and reused. And the automation of authorization assignment reduces the previously required manual administration effort by orders of magnitude.

Approach to implementation

IAM projects **fail more often than one thinks**. There are many reasons for this. Sometimes people think "too big", sometimes they plan "too small", sometimes they don't plan at all and often they simply underestimate the complexity of the overall project.

The introduction of an IAM system is a highly individual process tailored to the requirements and conditions of the company. Nevertheless, the following basic work steps can essentially be classified:

- Creation of a well-founded overall concept
- Awareness and buy-in by all stakeholders
- Development and introduction of a central user repository
- Automated authorization management for processes such as entry of an employee, change of department and leaving the organization according to existing data basis
- Introduction of application processes and recertification
- Connection to target systems via standard connectors or "loose" connection (order-to-admin)
- Support of the system introduction

In the planning and development of IAM concepts, too, modern approaches of iterative, benefit-oriented software development are now used wherever possible. The projects are characterized by self-organizing teams and an incremental approach. Risks and errors are more likely to be identified, and transparency and flexibility increase. Overall, this leads to a faster deployment of the system, while at the same time reducing costs. The Scrum method, a form of project management that does not require a project manager, or the Kanban principle, with which task management can be made more agile, is used here.

IAM projects are not purely IT projects

Although IAM is software, IAM projects are not primarily IT projects, but require a holistic approach.

Developing a coherent IAM strategy before the project begins

Integration of the business departments

The development of a conclusive IAM strategy before the start of the project is decisive for project success. IT management must be involved in the development and implementation, as well as the IT managers for individual applications and the respective contact persons and key users in the specialist departments. The question of who has or should have access to what intervenes deeply in the business. It must therefore not be decided solely from the IT perspective, otherwise the introduction of IAM risks failing or getting stuck halfway through. **Access and role concepts** must be developed in order to link departments, groups and individuals meaningfully with their respective competencies. The different requirements of **regulators and auditors must** also **be considered, often depending on the industry**.

A Successful Project starts with a cleanup

Cleanup means 'tidying up' and creates the conditions for a clean authorization management basis. In order to answer the question of which authorizations a user has in the company network; the individual accounts of the user can be assigned to physical users or their digital identities.

A company should be able to assign all existing user accounts in Active Directory, SAP, Lotus Notes or other business-critical applications to a real person employed in the company. Experience shows, however, that about 1/3 of the accounts of a system not controlled by IAM are orphaned accounts for which there is no committed owner.

Orphaned accounts

The process of so-called User ID consolidation is a first important step. Security vulnerabilities such as orphaned accounts or users without authorizations can be quickly discovered in a further step. There are special tools that take over this task and very quickly show the 'authorization corpses' in a separate report.

User ID Consolidation

Introduction of authorization roles

Role concept

Roles are bundles of permissions, in which individual permissions of users with identical tasks in the company are combined. Their use significantly reduces the administration effort. By automating authorization management through the introduction and use of roles, a company can achieve high savings potentials.

Experience shows that a degree of automation of more than 90 percent can be achieved through the role-based administration of authorizations. For this reason, setting up a role model should be done right at the beginning of the introduction of an IAM system.

Role Mining

So-called role mining concepts in the IAM system support the definition and continuous optimization of authorization roles. The cleansed authorization data is transparently displayed in relation to the existing organizational and process structure. The good visualization of the analysis scenarios in the role-mining process then creates the necessary transparency and traceability.

Roles must come from the specialist department

"With an IAM system, in contrast to manual procedures, you can implement a comprehensive approach and set up specialist roles across all systems," explains Jochen Schneider. The external consultant and specialist for quality projects in IT has supported an IAM project at ***Hamburgische Investitions- und Förderbank****, among others. "Although there were roles for the various applications, this did not mean that all employees automatically had the same authorizations. The roles were combined individually. "*

If an employee was given a new task, his or her entitlement was more person-related than role-related. Thus, various individual and group authorizations existed in parallel. Jochen Schneider: "However, BAIT demands that rights are derived from the tasks of the employees. For this reason, the roles should come from the specialist departments, which are thus responsible for their definition". (GINNY: WHAT IS BAIT?)

The role concept was developed in 1992 by David F. Ferraiolo and D. Richard Kuhn of the National Institute of Standards and Technology (NIST); 14 years later, the ANSI standard 359-2004 was adopted. The authors describe how permissions are encapsulated in roles and define role hierarchies.

IT roles vs. business roles

Due to their tendency to be theoretical and technical, these models are not necessarily tailored to concrete applications of today's identity management. Therefore, from a practical point of view, roles are now divided into IT roles (assigned authorization from a technical point of view) and business roles (functional point of view). This avoids overly complex role hierarchies; the role modeling is performed by the respective responsible department in the company.

Separation of functions (Segregation of Duties)

Functional separation, also known as 'Segregation of Duties', is another important requirement in IAM projects. This means defining mutually exclusive authorization assignments for employees. In the banking sector, for example, an employee may not have authorizations that allow access in both the front and back office. The background to such demands for separation of functions is the distribution of process responsibility to several people in order to prevent misuse. For example, the possible application for and release of a loan by one and the same person would pose a risk for the intentional and/or accidental circumvention of the dual control principle.

Types of roles: Basic, professional, functional...

In addition to the above-mentioned division into IT and business roles, a distinction is also made between three basic role types:

- **Basic roles** are generally assigned to all persons (which is why they are generally not subject to segregation of duties),

- **Organizational roles** are assigned based on the affiliation of a person to an organization and
- **Functional roles** are needed to perform a certain function.
- In addition, there are **special roles** that are generally assigned manually

Before the introduction of the IAM system GARANCY Identity Manager Business roles define which authorizations are bundled on the basis of a function or job type: for example, the 'motor vehicle claims clerk'. In addition, application roles were created, which bundle authorizations from the perspective of an application - i.e. dedicated roles for specific steps or work packages that must be performed with an application. GITU: what is this block? What is it proving or supporting?

Iterative role modeling

Employees must be viewed and administered in a holistic life cycle, based on their tasks and roles in the company. IAM solutions have therefore moved a long way from managing purely technical authorizations. They must be much more business process-oriented and integrated into the complex corporate structures via business-oriented roles. In short, they must build a bridge between business and IT.

Bridge between business and IT

The basis for an efficient IAM-system is a transparent role model for the assignment of authorizations. For the modeling of roles and the establishment of access and role concepts, one must therefore first consider the requirements of the business units and departments, down to the level of teams and individuals.

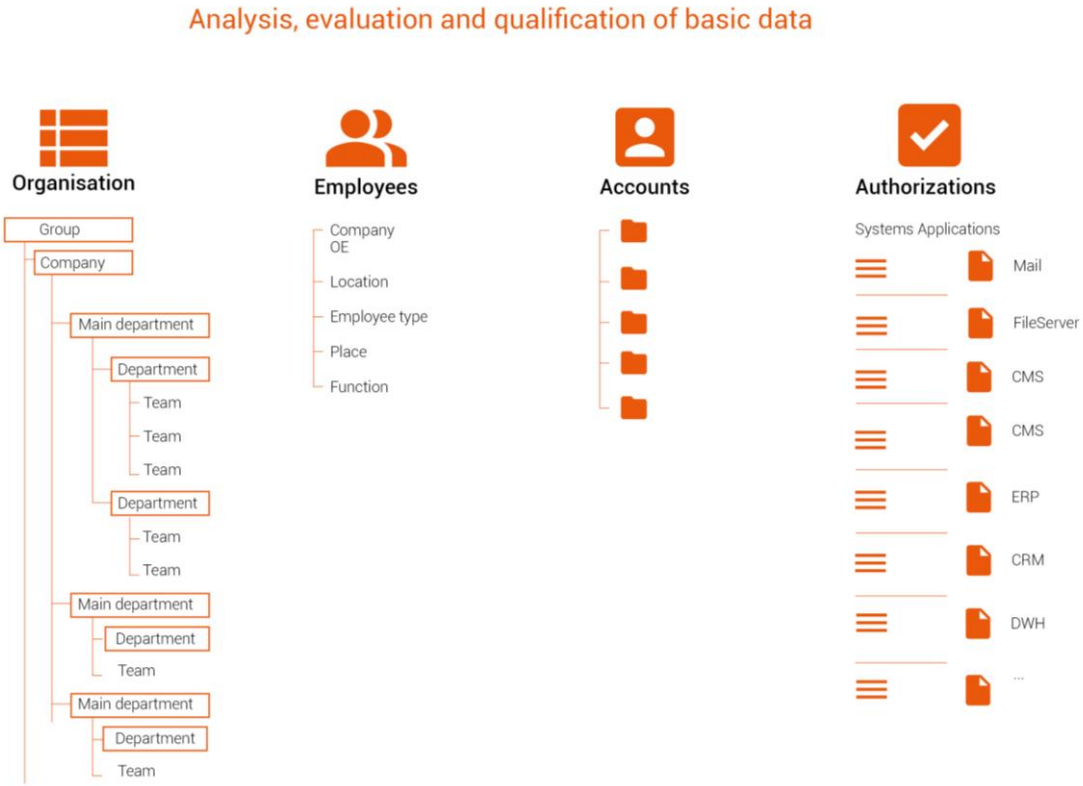
The **life cycle of a role** has different phases:

1. The specification and creation of a role
2. The provision or assignment of a role
3. Maintaining and checking a role

The starting point, the creation of a role, can be based on different activities. Roles are either **imported** from target systems during application onboarding by identifying **application and system roles** in the target systems and classifying them for application. For example, ERP or other core systems often already use "standard, best practice system roles" for authorization assignment. Existing group hierarchies and nesting can be taken over from **AD-/LDAP directories** for the authorization assignment. It is also possible to import from existing IAM solutions that are to be replaced.

If there is no possibility of importing, the role is **modeled** by the IAM system. Every powerful IAM system has corresponding functions for role analysis and modeling. Based on the existing authorization basis of all imported data, authorization clusters in
defined systems and organizational contexts are displayed.

- To develop or optimize a role model, individual authorizations are first analyzed, evaluated, qualified and, if necessary, additionally classified according to type, risk and function assignment (*see figure "Analysis, evaluation and qualification of basic data"*).
- This is followed by the definition of the role concept (determination of role types, conventions, attribution, assignment rules)
- Next, the modeling, verification and import of roles
- The analysis phase refers to employee, organizational and system data
- Finally, in some cases system authorizations need to be classified with regard to their risk class and function.



Types of roles: Basic, specialist, functional

Role modeling is done by clustering, which visualizes equal authorizations of a group of users and forms the basis for role definition. Based on the organizational chart, job descriptions and workshops with all departments, professional task packages are thus identified. They are bundled in such a way that they can lead to specialist roles.

The procedure is iterative and takes place first for basic roles and then for specialist and functional roles, which can be carried out on a department-specific basis.

Process design

Application, life-cycle processes

A key feature of IAM systems today is that they allow individual divisions to administer their user rights themselves, to submit applications and approve them - without the need for extensive technical expertise. This creates the need to take an additional security aspect into account, but by shifting these central governance tasks to the specialist department, a company can better meet the increasing and more complex regulations.

Release processes as workflow

Approval processes for the assignment of authorizations (i.e. how, for example, specialist roles are distributed to individual employees) should be stored in workflow charts during the introduction of an IAM system, even before the actual software implementation begins. Project times are shortened considerably if such specified processes - and thus the entire set of rules - only have to be mapped in the software during customizing. If the processes were deliberately kept simple, they can also be represented with the standard transactions of the software.

A further advantage is that you can work with real processes in advance and test them. The rule of thumb is therefore: first define the internal processes, only then select the technology. All too often, however, the opposite approach is taken. This unnecessarily drives up the costs of an IAM introduction.

For the administration of authorizations and standard tasks the IAM system provides the specialist departments with business process-oriented approval workflows. The workflow then only specifies which new employees are to complete which tasks and which specialist role is assigned. If a manager requests a specific access for a person, he or she will only see his or her own team members in the software and can only request the roles that have been defined for his or her own department. In the second stage, approval is often obtained from the owner of the role.

User access to the application processes is via a web-based portal. According to the individual authorization, the available interface modules and functions are presented to a user. For each of the roles, groups of approvers can be defined in the IAM system so that the process does not come to a standstill if the main approver is absent. There is therefore a technical and a human component that ensures that no one is given rights that they are not allowed to have.

Self-Service Request

Relief of the helpdesk

User satisfaction and comfort are also important in the IAM context. Tools such as a **self-service for password reset** or **password synchronization** are therefore part of the standard repertoire of a powerful IAM solution. They increase user comfort and improve the performance of employees, who do not have to wait long for a new password. They also reduce the costs and administrative workload of the helpdesk.

Statistical surveys in companies show that every third call to the helpdesk is assigned to password resetting. Reducing this number results in significant cost savings. The benefit of self-service request tools is equal to the number of requests saved multiplied by the average duration of a helpdesk session and the associated costs e.g. the costs of downtime for the user as they await assistance from the helpdesk.

System Connections

Connection of HR systems

The HR system is often the leading source of all personal information in the company: Who has been performing which job since when, what tasks are associated with it. This leads to the question: Which applications does the person need access to? HR data should therefore be connected to the IAM software as a first step.

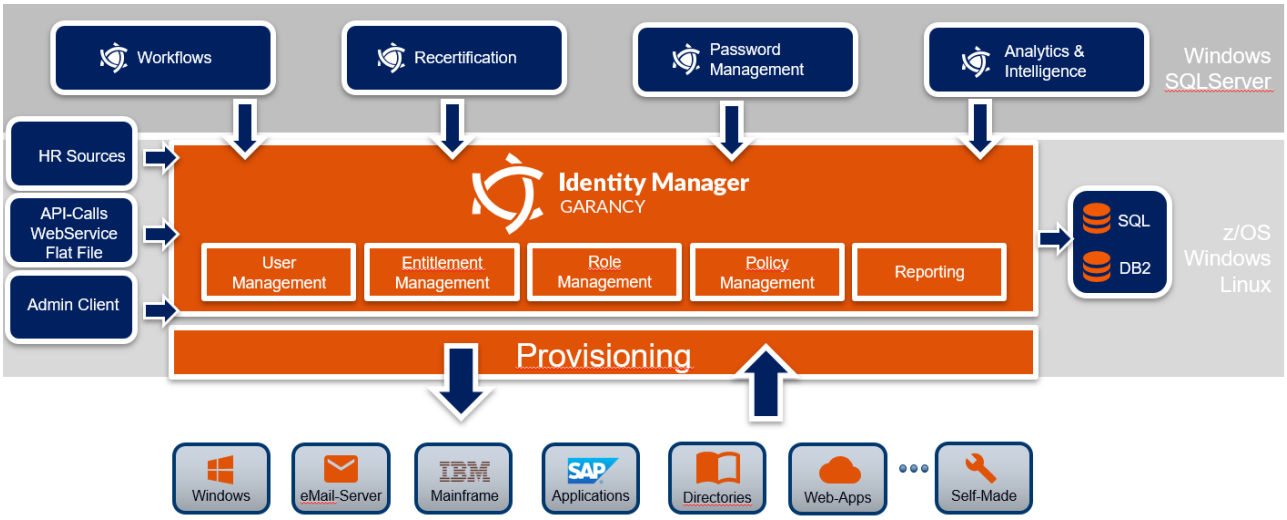
Problems often start in the lack of or incomplete coordination between the HR department and IT. They then spread to the entire company. Personnel changes are not made, are too late, or incompletely communicated to the IT reported.

Error sources

The error rate also increases due to manual and area-specific decentralized processing. Unclear responsibilities due to poorly communicated changes during reorganizations and a lack of monitoring give an idea of how little secure and transparent as well as difficult to understand authorization assignments in IT can be administered.

Standard Connectors

An IAM system usually offers so-called "Target System Interfaces" to connect the important standard applications in the company - ERP (SAP), RACF, Windows Active Directory/Exchange, DB2 ... -.



Individual IT systems are integrated via standard connectors or flexible interfaces like CSV.

These connectors are used to connect the IT systems for fully automatic data exchange with the IAM system:

Changes made within the IAM system to users' authorizations and accounts are implemented directly in these IT systems.

At the same time, changes in the authorization structures in the IT systems are automatically transferred to the IAM system and processed there in a rule-based manner.

Order-to-Admin

The Order-to-Admin process ("loose system connection") is used for requirements that require authorization in systems that are not technically connected. Here the administrator is requested to manually grant defined rights to a person.

Modern IAM systems include a special process workflow for this purpose, which can be individually configured for use by the customer.

The participants in an IAM project

Manager Authorization Management

...has overall responsibility for the specifications, execution and efficiency of the IAM implementation and ensures its conformity and efficiency. They represent the process to all other service management processes as well as external groups and is the primary contact person for all IAM-relevant requests.

IAM Coordinator

... supports and monitors the operative execution of the processes and functions of the defined authorization management and is the central contact for the users of the IAM solution.

IAM Administrator

...carries out the professional and technical configuration and administration of the IAM solution. In addition to operational monitoring and system maintenance, he develops technical concepts and implements them or controls their implementation.

External consultant

...provides support in setting up IAM concepts and advises on industry-specific issues, recurring challenges/problems.

Business departments

… provides the information about the needed access rights and manages the access rights entitlements.

Recertification

Personnel or structural changes in the company constantly influence the access rights of employees to information. This requires the continuous checking and updating of existing authorization structures. The process of regularly performing such an attestation is called recertification. In some industries it is even required by law, for example by MaRisk (Minimum Requirements for Risk Management) in the financial sector in Germany.

MaRisk

During recertification, authorizations that have already been attested or approved once are reconfirmed at fixed intervals. This takes place at the level of divisional managers or management and is implemented in a certification process. The responsible person receives a link to an IAM website, where it is self-explanatory which employee has what authorizations, which systems they use and why. This helps to make a quick decision on whether to reassign or withdraw permissions.

Using the same methodology of a recertification campaign, it is also possible to periodically check authorization structures like role objects. Roles are also subject to changes over time and must therefore be regularly confirmed with the recertification tools of the IAM system.

Conclusion

Identity Access Management (IAM) serves as a collective term for all aspects of digital identity administration. It requires an appropriate infrastructure in the organization. In addition, effective administrative authorization processes must be introduced to ensure a high level of data security and efficient business processes.

To ensure that IAM solutions contribute to improving the quality of user and authorization data through automation and data synchronization, their implementation should follow a predefined methodology. It starts with a basic inventory, continues with the definition of roles and approval workflows, and extends to ensuring recurring attestation through recertification.

In principle, "processes before technology" should always be adhered to in order to ensure the IAM introduction does not drag on unnecessarily, but the company quickly achieves a functioning IAM system with all the positive effects: Adherence to compliance requirements, increased operational and IT security and cost reduction.

Beta Systems IAM Software AG
Alt-Moabit 90d
10559 Berlin, Germany

+49 (0) 30 726 118 0
iam@betasystems.com

www.betasystems-iam.com