ACCESS INTELLIGENCE
an intelligent step beyond Access Management

White Paper
# Table of Contents

Access Intelligence – an intelligent step beyond Access Management ............................................. 3

The new Identity Access Management paradigm ........................................................................... 3

From Identity Access Management to Identity Access Governance ............................................. 4

Adding a business layer to Identity Access Management ............................................................... 6

The challenge is in data volume and complexity ............................................................................. 6

Access Intelligence fulfils the need for more a comprehensible Access Rights Management ................................................................. 7

The advantage of established BI platforms ..................................................................................... 8

Better analyses and reports ............................................................................................................ 10

Provision of relevant content for a BI infrastructure ..................................................................... 10

Summary ..................................................................................................................................... 11
Access Intelligence – an intelligent step beyond Access Management

Governance in access management – also called “Identity and Access Governance” (IAG) – means that the business departments take on more responsibility for safeguarding resources and restricting activities. In consequence, the assignment of access rights must be controlled more tightly, and existing rights must be confirmed (recertified) at regular intervals. One of the main challenges of Access Governance is presented by the need to handle huge quantities of data and their extremely complex structures. A solution is achieved by aggregating and visualizing these data in a business understandable form.

Established procedures and methods in Business Intelligence (BI) have become the cornerstone for achieving this. The use of BI methods to prepare authorization structures leads the way to Access Intelligence. The basic, mature principles that make business intelligence successful for business decisions can be applied in IAG to achieve real transparency of activities involving access in the enterprise. As a result, well-proven methods are finding their way into new areas of application.

The new Identity Access Management paradigm

As with everything else in IT, Identity Access Management (IAM) must respond to the fast-moving demands of its market. For example, a parallel can be drawn between the community collaboration approach that Web 2.0 uses to create content, and the capabilities of IAM in an environment influenced by Access Governance through Access Intelligence. That’s why we think about IAM today as IAM 2.0.

IAM 1.0 was IT driven and administrator oriented. Its focus was single-point of administration, Human Resources driven provisioning and Role Base Access Control (RBAC). In contrast, IAM 2.0 systems are business collaboration platforms that enable the wider involvement of the business units in access management. The way the business user perceives and uses these systems has changed. The business units are integral in the IAM decision-making process. The IAM 2.0 systems provide extensive self-service functions, making each individual user personally involved in the secure, rule compliant management of access rights.

In the past, factors such as cost reduction and efficient user management were of central importance. Today, enterprises are looking for systems that will keep them compliant with laws and regulations and provide the basis for risk management. This is why we talk about “Access Governance” when we think of IAM 2.0.
From Identity Access Management to Identity Access Governance

The paradigm shift from IAM to IAG has resulted in new tasks and functions. Some of the most important building blocks are the request and approval workflow for new access rights, and the review and certification of existing access rights. The basis for this is modeling user access information based on a user’s role in the organization. This modeling may also include information about what level of risk is taken when a user has access to sensitive information.

The simple assignment of access rights to users no longer meets its intended purpose. Instead, the need has arisen for a request and approval procedure that assigns roles and grants access rights. This procedure can be supported by an automated workflow in larger organizations.

Greater transparency in existing access rights is another essential factor. It is a major prerequisite for the recertification process. Certification requires that heads of department regularly check and reconfirm the necessity for specific employees to retain specific access rights. This reduces the risk of employees accumulating more rights than they need. Here, the principle of “least privileged” should be the yardstick, so that rights are limited to a necessary minimum.
Business-oriented role modeling includes the creation of roles that the business unit can understand. It is the prerequisite for the request and approval workflow and for certification. Business units cannot request, approve or recertify roles unless they have a clear understanding of what these roles are. Therefore in addition to their original task of encapsulating rights, roles must now be designed to additionally meet the needs of the request and approval workflow, including review and certification.

The assignment of access rights must take several types of principles supporting IAM 2.0 into account. One of the most important of these is the segregation of duties – SoD. To avoid creating “toxic combinations”, it is essential to rule out the existence of certain combinations of access rights. In Identity Access Governance, the underlying SoD rules must be defined and applied when assigning access rights. Additionally, it must be possible to check existing rights for compliance with this rule.

When examining access rights, it is also important to consider historical situations. This means that simply examining current permissions is not sufficient. It must also be possible to look at them in the context of a timeline. One basic question is: Which access rights did this user have in the past? Moreover, it is important to find out who requested, approved and recertified these access rights. This is one of the main prerequisites for forensic investigation into irregularities in business operations, for example. These historical analyses make it also possible to detect trends and patterns, e.g. by showing if someone is accumulating more and more access rights over time.

User activity monitoring enables the correlation of user activities with permission structures. The system log files are used for this purpose. User Activity Monitoring enables us to say, for example, how often and when users actually used their permissions. As a result, permission structures can be adjusted to meet business requirements more closely.
Adding a business layer to Identity Access Management

The additional requirements arising from Access Governance must be reflected by new procedures in access rights management. This means that a classic IAM system needs a business-oriented component to give the members of the business units an understandable view of identities and rights that is directly related to the business process.

To achieve this, existing IAM systems must be expanded to include business-oriented strategies. This could be done by adding an additional layer to the IAM system, one that should also include functions for the analysis of access rights, reporting functions, and checking routines for the regular monitoring of accesses. A web portal would also make access easier for employees from the business units.

The challenge is in data volume and complexity

The fine granularity of rights and the monitoring of these rights, which also takes their histories into consideration, present a special challenge: the sheer quantities and complexity of data. For example, IAM solutions in the banking sector have to handle up to 100,000 users with a total of 500,000 accounts and 35,000 roles, as well as 700,000 authorization groups from a large number of applications. Furthermore, the system activity logs with more than 250 million log records per year show that the structure of this data is not static.
As a result, incredible volumes of data need to be processed, and complexity of immense dimensions has to be managed. Moreover, the access rights and the data they generate are subject to permanent change. Changes to the organizational structure, new applications and new regulations mean that the volume of data is continually expanding, making manual analysis impossible. Once volumes of data reach these dimensions and these complexities, they can only be tackled successfully by automated systems.

**Access Intelligence fulfils the need for more a comprehensible Access Rights Management**

Instead of the usual “make or buy”, the question now is “build or re-use”. IT already offers a lot of reusable technologies for processing large quantities of data fast and efficiently. In contrast, developing home-made software systems is costly and time-consuming. This holds particularly true in the Business Intelligence (BI) sector. Its core functions include preparing data by means of ETL tools (ETL = Extract, Transform and Load), storing data in a data warehouse, followed by analyses that produce reports in the form of graphics, pivot tables and KPIs.

Then why shouldn’t these technologies also be used to analyze access rights? Instead of analyzing turnover and market data, why not analyze access rights structures? It certainly doesn’t make any difference to the methods and procedures integrated into BI tools.

Business Intelligence delivers the important infrastructure for the analysis of access data. Our IAM solution, however, delivers the content: the underlying data model with its analytical capabilities. Our approach is to provide the data needed by retrieving it from all the various significant IT systems. The use of this data model enables the suitable processing and transformation of access data for further use within the data warehouse. Therefore this model is the prerequisite for a wide range of access analysis.

This paves the way for several access rights reports and activities e.g.:
- ready-to-use and pre-configured standard reports which will be distributed either via scheduler/email notification or on demand. Moreover, the on-demand reports can also be adapted manually by filtering, sorting and sizing.
- ad-hoc reports: self-service Business Intelligence that allows the easy, efficient creation of your own individual reports according to your specific needs, based on a business-understandable data model.

Activities may include attestation, for example, access request and approval, re-certification or other activities that can be combined with an integrated business process workflow in the near future.

For this reason, it is justifiable to say that only the full integration of BI and Access Intelligence can provide the huge analytical capabilities that will enable us to gain an in-depth insight into access rights. It is this insight that will enable the right decisions to be taken as the basis for access governance activities.

Therefore this opens up completely new possibilities for Access Governance, possibilities that can be used immediately for the analysis and preparation of data from authorization systems.
The advantage of established BI platforms

When choosing a BI platform, organizations are faced with the question of developing something themselves, or using an established BI environment. Experience has shown that home-made implementations involve more disadvantages than advantages, often leading to silo applications. Furthermore, their scalability and expansion capabilities are usually limited. Using a formal platform seems to be the better proposition. The BI tool suppliers themselves make sure that their systems are powerful enough and sufficiently scalable. Moreover, as a rule these systems can be customized to meet specific customer needs. By adding other solution packages, organizations can set up their own enterprise-wide information platforms.

This use of an existing BI tool sheds an entirely new light on user data and the associated access rights. This can be illustrated by a simple data model:
Data preparation in a data warehouse primarily follows the star schema, which organizes data and meta data into star-shaped structures. The facts under analysis, e.g. a user’s assignment to groups, are the center point of the structure. In this case, the group assignments provide the nexus between the user and her authorization path. Peripheral to this is a descriptive dimension containing additional attributes such as the user’s function or location (her place of work). This star-shaped data model makes it possible to map authorization structures in such a way that they can be efficiently analyzed using the widest possible range of criteria.

This data model not only enables efficient analysis, but, with its use of business understandable meta data, also provides a kind of “business access semantics model”. Existing tools enable analyses and reports to be created more quickly and easily. This is also supported by the look and feel associated with Windows - for example, drag & drop, drilldown, and a wide range of visualization methods.
Better analyses and reports

Access intelligence answers the questions typically asked in authorization management. These include: “Who currently has what access rights?” and “What rights did this person have in the past?” Moreover, it is easier to obtain more in-depth analyses that give insight into such topics as risk ratings and certification procedures.

An access intelligence solution that is based on BI technologies opens up a multitude of other possibilities. It will be possible to create tailored reports that are specific to the needs of a customer’s organization. With its powerful drill-down and drill-through functionality it will enable organizations to give immediate, well-founded answers to ad hoc questions.

For instance, key performance indicators (KPI) can be easily derived from various authorization management criteria. This not only applies to the analysis of individual objects such as users or roles, but also to the relationships between these objects. Moreover, it enables the monitoring of threshold values, making it very easy to identify high-risk users, for example. Last but not least, BI tools enable complex analyses that provide a wealth of information on factors such as trends and patterns.

Provision of relevant content for a BI infrastructure

Drawing upon various sources, our solution extracts all kinds of access data relating to Identity Access Management and transfers it to a single data warehouse. This content includes both the historical and live data that will be stored in multi-dimensional layers of an access data cube. Our Access Intelligence solution enables customers to work with standardized ready-to-use reports. Furthermore, they can create specific reports that can be easily customized to meet individual needs. This means that this is not a rigid model providing standard reports only, but opens the way to customization by configuration - without any need for programming - to create specific reports.

The reporting and analysis tools include well-designed cover pages that enable a quick and simple leap forward to subordinate pages. They offer a wide range of reports based on different dimensions such as role, sub role, user, accounts and the relationships between these dimensions. A multitude of easy to use and clearly laid out cross-tables can be created, enabling the direct comparison of different groups, e.g. users grouped by job functions and the access rights assigned to them.

The resulting reports can be integrated into almost any customer portal where they can be viewed as required. This provides customers with a high degree of flexibility in creating the reports they need for their specific purposes.
Summary

Access Governance and Intelligence is a focal point of interest for Beta Systems. It plays a major role in the company’s strategic alignment. Our solutions provide a workflow-based request and approval procedure, and will be geared to offering an Access Intelligence infrastructure for business-oriented evaluations in the form of analyses, reports and dashboards. All of this will ensure better control and more transparency in the GRC environment. We are building on our many years of experience and skill in automated provisioning (deployment of access rights), and on our ability to support a wide range of target systems by means of our powerful standard connectors.

By using an Access Intelligence module, we are paving the way for access management to expand into the innovative realms of Access Governance. With the integration of an established BI suite, we are offering an IAG solution that is based on a full-featured, highly scalable and stable and mature BI environment.
Bringing together
Access and Governance