Role Management in Access Governance & Intelligence

# Table of Contents

Role Management in Access Governance – a technical relic or really relevant for business? ................................................................. 3

The shift to Collaborative IdM 2.0 .................................................................................................................................................. 4

The role as a business-understandable view of permissions ................................................................. 5

RBAC – Role based Access Control: a milestone in IdM ......................................................................................... 5

Best practice in role management ....................................................................................................................... 6

Excursion: Access Governance & Intelligence as the two pillars of IdM ................................................. 6

Request and approval procedure: business responsibility for the assignment of rights ......................................................... 8

Other role attributes needed by Access Governance .................................................................................. 9

Role management as the link between IdM 1.0 and IdM 2.0 ................................................................................. 10
Role Management in Access Governance – a technical relic or really relevant for business?

In the past, the main purpose of traditional identity management systems (IdM) was to take care of the more IT-biased administration tasks. Here, the main focus was on the »Single Point of Administration« approach, and the administration of identities and permissions was generally controlled by data from the personnel department. This was known as HR-driven provisioning. At the same time, the concept of Role-Based Access Control (RBAC) emerged as an effective method of encapsulating permissions.

Under great pressure from the proliferation of regulatory requirements and demands for compliance, organizations are driven to shift emphasis away from the tactical IT-biased model in favor of a more strategic, business savvy and business inclusive approach to manage permissions. Involving the business units more closely in the provisioning process, and providing a wide range of business-intelligent information demands a different paradigm for IdM. This change of direction in Identity Management steps over the tactical approach and addresses the strategic approach which has been incorporated into the terms »Access Governance and Access Intelligence«.

Access Governance calls for IdM to involve business in the control, administration and certification of access rights, to provide self-service functions, and to be workflow controlled. Access Intelligence provides business with the information and knowledge that enable the right decisions to be made in terms of e.g. controlling existing permissions, making risk analyses, and handling privileged users.

As a result of this shifting IdM ecosystem, it is important to understand the strategic status that role management occupies. Are roles merely a tactical tool, or do they have a crucial capacity in answering the needs of business? The aim of this paper is to cast some light on this subject, and to reveal role management within the framework of Access Governance & Intelligence.

Roles have been around for a long time as a core component of Identity Management. However, within the framework of Access Governance & Intelligence, their purpose and significance have undergone a change. Traditional role management, as represented by the pure administrative bundling of access rights, no longer meets today’s requirements. Roles now need to support new business-oriented functions, and are subject to a request and approval procedure.
The shift to Collaborative IdM 2.0

But let’s examine the changes that have taken place in Identity Management. As with everything else in IT, IdM must respond to the fast-moving demands of its consumers. For example, a parallel can be drawn between the community collaboration approach that Web 2.0 uses to create content and the capabilities of IdM in an Access Governance and Access Intelligence aware IdM environment. So that’s why we think about IdM today as IdM 2.0.

IdM 1.0 was IT biased [yes biased], and administrator-oriented. It placed single-point of administration, HR driven provisioning and RBAC in the foreground. Instead of the main focus being on identities and their administration, more emphasis was placed on permissions and handling permissions.

IdM 2.0 addresses the shortcomings of IdM 1.0 with business-oriented functionality. Today’s IdM 2.0 systems are business collaboration platforms for access management. The way the consumer, the business user, perceives and uses these systems has changed. The business units are integral in the IdM decision-making process. The IdM 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, IdM 1.0 answered the reasons that drove IdM adoption. 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, provide the basis for risk management and still not ignore the cost reduction needs and efficient user management requirements that have never diminished.
The role as a business-understandable view of permissions

In any company or organization, users have specific jobs to do and various IT systems are available to enable them to do their jobs. Users also need the appropriate accounts and permissions for these IT systems, and this is where “authorization triangle” comes in: Who (user) receives What (permissions) and Why (job). This triangle serves as the basis for deriving a general role model, where the role takes the place of the job function and encapsulates all the permissions in abstract form. The semantics of the role must reflect the tasks involved in the job, and represent the technical permissions in a business-understandable way.

RBAC – Role based Access Control: a milestone in IdM

The way in which we see roles was greatly influenced by the RBAC model, the first model to encapsulate permissions so that they are easier for business to understand. Described by Ferraiolo und Kuhn at the US National Institute of Standards and Technology (NIST) in 1992, it was known as the NIST model and immediately recognized as a (semi) standard. In 2004 it was adopted as an ANSI standard (359-2004). Among other things, it includes the definition of role hierarchies for mapping complex structures. However, role hierarchies soon became too complicated in terms of
design, understandability and maintenance. Moreover, the RBAC standard did not include enough practise-relevant use cases. Experience showed that this theoretical approach to role models was not really suitable for practical implementation.

**Best practice in role management**

RBAC’s focus was mainly on access control in the target system. In contrast, today’s role models tend to reflect the enterprise view of IdM, and hide the underlying authorization structures of the target system. As an alternative to theoretical role hierarchies, the division of roles into business roles and IT roles has established itself in practice as an adequate solution. The aim is to avoid complex role hierarchies that turn out to be unmanageable in the long term. IT roles define the technical relationships of permissions; business roles define the functional aspects and/or the position of the user within the organization. In this way, role management builds a bridge between business and IT.

Because IT bears the main responsibility for the assignment of roles and the request procedure, it still tends to be the greatest influencing factor in the creation of role models. Unfortunately, this often gives the impression that in a modern, automated IdM system, roles are there to make life easier for IT rather than to help the business unit. It is important to find ways of involving business more closely in the role life cycle. Among other things, this would simplify approval procedures and achieve greater transparency. More responsibility for provisioning must be handed to the business unit, not only for the creation of roles, but also for their assignment, maintenance and certification. This comes under the heading »Identity and Access Governance« (IAG). IAG signifies a »new« IdM in which business management takes control of and responsibility for access management, and where »governance« really means »ownership« in the true sense of the word. This takes us back to IdM 2.0 as a business collaboration platform carried by several actors. Its aim is to translate IT-specific resources into business-understandable terms and contents, and to superimpose a business view on the underlying IT-centric IdM infrastructure.

In addition to Identity and Access Governance, Access Intelligence is currently another driving factor in the IdM market. It takes care of the business-relevant preparation and presentation of permission structures. Because the focus today is on permissions rather than identities, we do not really need to add the word »Identity« to the term, and so we simply refer to »Access Governance & Intelligence«.

**Excursion: Access Governance & Intelligence as the two pillars of IdM**

As mentioned previously, Access Governance calls for IdM to involve business in the control, administration and certification of access rights, to provide self-service functions, and to be workflow controlled. Whereas Access Intelligence provides business with the information and knowledge that enable the right decisions to be made in terms of e.g. controlling existing permissions, making risk analyses, and handling privileged users.
Both structured and unstructured data are generated from various sources and made available to business as easily accessible information modules. These include analyses, offline reports, and online dashboards with drill-down functionality. But how do you get from data to information to intelligence? What is »intelligence«? In IdM, »intelligence« means the acquisition and preparation of information and knowledge. This in turn forms the basis for deriving business-relevant decisions and actions. Data are aggregated and divided up into small portions that can easily be »digested« by business in intuitive information portals, without requiring any special training. Predefined required and threshold values ensure that business is automatically informed about critical situations.

Which basic principles do Access Governance & Intelligence provide for business orientation? Workflow-based request procedures and collaboration with IT mean that the business units are involved in the creation of roles. The business units themselves grant access rights and take responsibility for their own roles at department level. Moreover, business-friendly reports, dashboards and drill-down functionality ensure they have a completely transparent view of the permissions that are assigned. Risks are reduced by recertification, a process that ensures that permissions are regularly reviewed, and also prevents the unwanted accumulation of access rights.
Request and approval procedure: business responsibility for the assignment of rights

Typically, the request and approval procedure is a workflow-supported process. Therefore it is vital to install a powerful, flexible workflow system that can meet the specific demands of any enterprise. But how do you go about designing an access request and access approval workflow? And where is the focus of business responsibility?

Workflows consist of a number of process steps and the associated actors. Every activity gives rise to a large number of basic questions. For instance, the first thing a requestor must do is request the assignment of a role. Already the question arises as to whether this person is making the request for himself (self request), or for someone else (managed request). The next step of the procedure is to select one or more roles. Which roles is this person allowed to select? Can he select any of the roles at first, with permission first being granted at the approval step? Or can he only select his own role? Once a request has been submitted, it has to be checked by the approver. The question now is, of course, who is allowed to approve the request? And how many different approvers have to give their approval? Once the request has been approved, the role needs to be assigned. There are two basic ways of doing this; automatically, by the IdM system that drives the workflow, or manually, by an administrator who makes the settings. Finally, at the end of the workflow, everybody involved in this particular request and approval process needs to be notified.

The approval procedure is the pivotal issue in the entire process. As a rule, more than one person will need to approve a request, depending on the area of responsibility and on the risk management policy. This is where business actually assumes responsibility. For example, a request for role assignment involves the following actors and approval steps: the manager, who needs to know which tasks the employee needs to fulfill and what he is requesting; the role owner, who is responsible for the role, knows its semantics and needs to be aware of who is using the role; The scope approver, who monitors groups of particularly critical access rights; the application owner, who controls the assignment of rights from the application side, and who checks restricted licenses, for example, to see whether enough accounts are available.

The request and approval process clearly shows that the shift to business-orientation results in a multitude of questions that all demand answers. These answers need to be mapped as new data structures and relationships where the role is a pivotal entity.
Other role attributes needed by Access Governance

Within the scope business-oriented support for Access Governance, it has become clear that risk analysis, recertification and the segregation of duties (SoD) are other important factors that need to be taken into account by the new role attributes. For example, this means roles can be rated in terms of risks, with regard to the encapsulated permissions and the information and actions they protect. Moreover, a risk rating can be attached to the permissions within a role. A risk analysis serves as the basis for special handling and special reporting, for example.

Recertification is the regular reconfirmation of a role. It asks whether the role is still necessary, and by doing so, prevents individuals from accumulating more rights than they should have. This means that a role needs someone who is responsible for recertification, and that a recertification cycle is specified on the basis of the risk rating.

The Segregation of Duties is governed by an SoD matrix, an entity that specifies which roles cannot be held by the same person at the same time, based on internal and external security policies. This is very important for financial institutions, for example, where there must be a segregation of duties between Sales (the market) and the operative credit function in decisions to grant loans. In other words, the employee who offers the loan cannot be the same person who approves it.

Previously, the main purpose of roles was to encapsulate permissions and their authorization. By doing so, they promoted efficient user administration (RBAC approach). Within the framework of Access Governance, roles have taken on new tasks that enable them to serve diverse business-oriented functions. The result is a new governance layer which is characterized by multiple relationships to other data objects. In future, these business-oriented functions will also influence granularity and the ›tailoring‹ of roles.

Governance Layer

Attestation Request Approval Policies Risk Mgmt.

Org Units Owner Approver SoD Rules Risk Rating

User Administration

User Assignments

Business Role Technical Role Permission Encapsulation
Role management as the link between IdM 1.0 and IdM 2.0

At Beta Systems we have recognized the significance of Access Governance & Intelligence and made it the cornerstone of our strategic alignment. Our solutions provide a workflow-based request and approval procedure, and include a business intelligence infrastructure with business-oriented assessments in the form of analyses, reports and dashboards. All this contributes to greater control and transparency. Our solutions take our competence in automated provisioning a decisive step further, supported by powerful connectors to a multitude of target systems.

From our perspective, role management and complete role lifecycle support are important data structures that bridge the gap between IT-centric IdM 1.0 and business-oriented IdM 2.0.

We contend that far from being a Tactical Technical Relic, roles are enablers to Business Strategy achievement. IdM 2.0 meets today’s security requirements for business success: it clarifies IT and business roles, provides a business comprehensible viewpoint on IT-centric permissions, removes the technical clutter and opens conduits to business centric Access Management.
Bringing together
Access and Governance