An Enterprise Business Role Concept as a Foundation for SAP IDM and GRC

Applies to:

SAP NetWeaver Identity Management, SAP GRC Access control.

Summary

There is an increasing focus on Enterprise Business role concepts, but not on the process of structuring such a concept. This paper describes what an Enterprise Business role concept consist of and it presents a method to develop it.

AuthorS: Troels Lindgård, Bernhard Escherich

Company: KMD, SAP

Created on: February 6th. 2009

Author Bio

Troels Lindgård is a SAP security architect at KMD; the main provider of IT to the public sector in Denmark. He has 4 years experience in SAP security, with primary focus on method building and organizing the areas of SAP security. He also holds the position as chairman of SUPAN, which is the leading SAP security knowledge sharing network in Scandinavia.

Bernhard Escherich is a strategic solution architect from SAP for healthcare, defense and public security and has a higher education with more than ten years experience in the IT industry. His areas of expertise include GRC and Identity management as well. Prior to his current position he was responsible for eHR solutions (ESS/ MSS/ eRecruiting/ eLearning) in the international consulting team of SAP.

Table of Contents

An enterprise business role concept – How to create such a concept?

Identity management (IdM) is high on the IT departments list of projects, but many fail to get the full benefit from IdM. In many cases this is due to a missing Enterprise business role concept. This article describes a method on how to create an Enterprise Business role concept for roles in the SAP landscape.

The process of creating an Enterprise Business role concept requires commitment and resources from the different parts of the organization and should never be started by IT department resources only.

How to create an Enterprise Business Role concept

Enterprise business role concept is the foundation for an IDM implementation, and the first step to a proper implementation of GRC.

The primary purpose is to have an exact view of which roles are used in the SAP landscape and furthermore to get a clearly defined ownership of the roles.

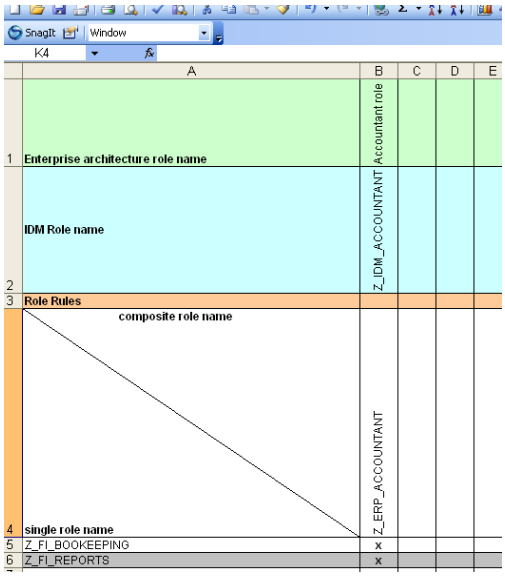
Secondly to get documented the rules to assigning the roles. These rules are often implicit and often understood differently by the user administrators and role developer. It is therefore important to consolidate these views. All these activities needs be performed and it will require some iterations to get the full picture.

The overall process consist of the following activities

A. Create an Enterprise business role concept
B. Define ownership of roles
C. Define enterprise business roles
D. Document rules
E. Refine Enterprise business role concept on the basis of ownership and rules
F. Clean up of the roles not in use
G. Define a maintenance process for the Enterprise business role concept

Create an Enterprise business role concept

The first step in creating the enterprise business role concept is to extract all the roles with user assignments from all the SAP systems. This can be an extensive list which is difficult to manage. It is therefore necessary to create a cover sheet with all the template roles/master roles which will give a better overview for the next steps. An example is shown below.



Define ownership of roles.

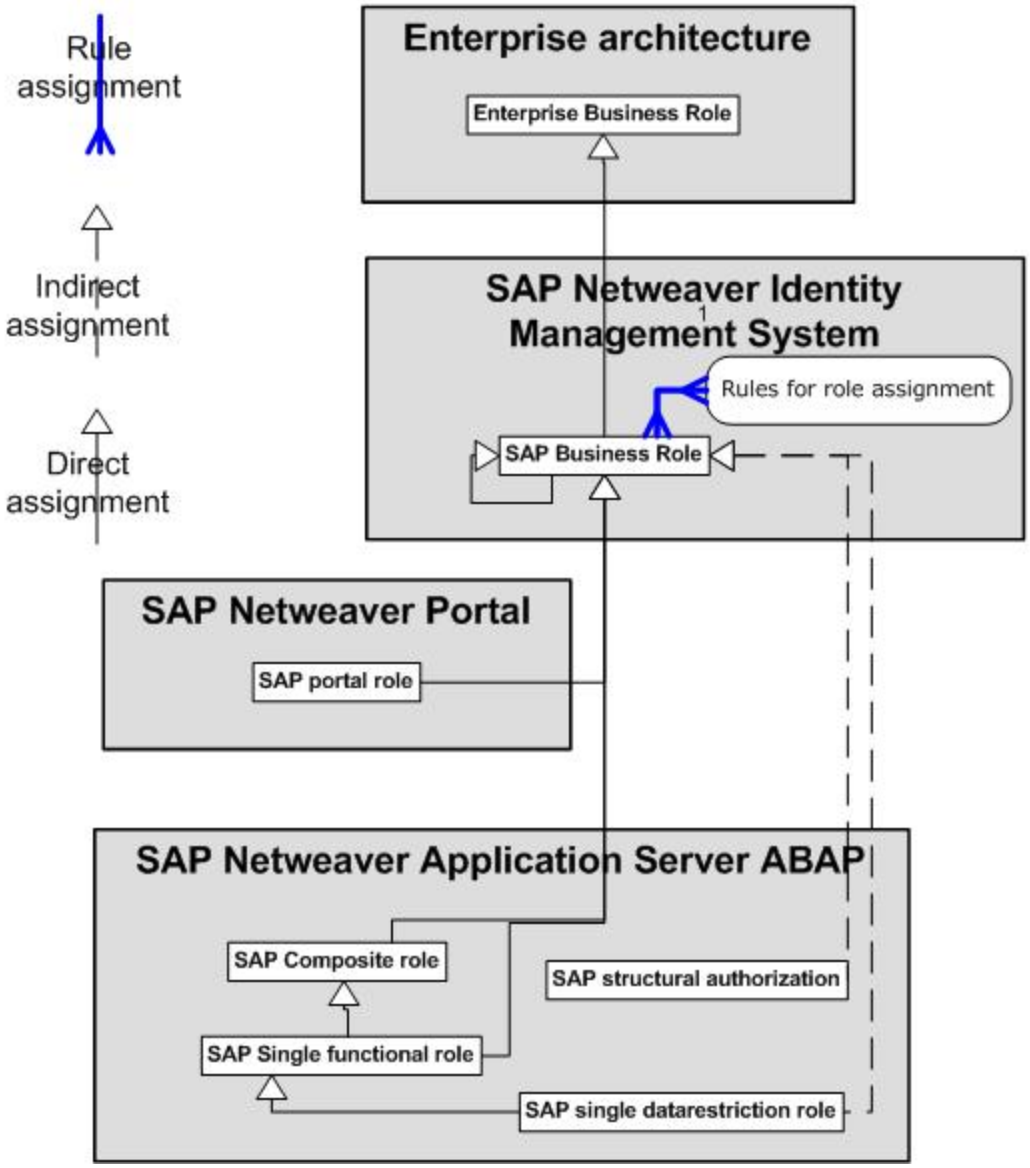
All the master roles need a clear defined owner. It could be that existing governance models can be used for this. But this will first be clear after an analysis of ownership has been made. This is done by setting up workshops with the presumed owners and get them commit to the ownership of both the master role and all the child roles. This may cause disturbance because some of the child roles can have been altered in order to comply with local regulations for daughter companies. In this case, it might be necessary to define a joint ownership.

Altered child roles should not be seen as a child role. Instead it should be a separate role, which is its own master role.

Define enterprise business roles

Having clearly defined ownership it is now the time to define the enterprise business roles on top of the roles. There are several approaches for this. One is to use the roles defined in the enterprise architecture as enterprise business roles. The enterprise business roles will be the SAP business roles, if SAP Netweaver identity management system is implemented. The illustration underneath explains the relationship.

Role model for Enterprise Business Role Concept



If an enterprise architecture isn't in place, job types or similar can be used. It is the role owner that will define relationship between the existing roles and the new enterprise business roles.

The enterprise business role helps the Enterprise to highlight issues where different roles give access to the same process. It can help to decrease the number of these conflicting roles and raise awareness among the role owners, because it will be difficult for them to administrate the ownership, if there is this kind of joint ownership.

Document rules on role assignments

The rules for assigning roles are often implicit and sometimes even unclear specified. In order to get a full understanding of the roles and their context, are the rules very important to get documented. This can be done in a structured way by using the methodology on Business rules from Zachmann and Ross. It is often difficult to get the business specialists to understand the methodology or even understand the purpose of documenting the rules. One approach can be to collect all the information you can get out of the business specialists and then afterwards analyze the results to get the information structured and aligned.

Different application areas can have the same rules on roles but define them totally different. It is therefore an important work to decipher the information, and it can take a considerable time to do this.

Refine Enterprise business role concept

The definition of ownership and the documentation of the rules on roles will have impact on the Enterprise business role concept. Roles might need to be split up in order to reflect the governance model or that additional roles needs to part the composite roles or roles can be merged.

Clean up roles which aren't in use

In order to ensure the Enterprise business role concept is complete. The deletion of obsolete roles should be handled as soon as possible. The obsolete roles are roles which don't have ownerships or are defined as not in use. These roles disturb the picture going forward, and deletions of these roles are necessary from development systems all the way up to the production systems.

Define maintenance process for Enterprise business role concept

Going forward a maintenance process is needed. The maintenance process should work on two levels.

One is on the role level, where new roles are added to the Enterprise business role concept and owners are documented.

The second level is the governance level which needs to be updated according to organizational changes such as the restructuring of departments or in case of a new manager is assigned to a position which has ownership of one or more roles. In this instance, education of the new manager is needed in order to understand the responsibility.

Besides the already mentioned points the benefit of this process will be higher productivity and job satisfaction for the consultants working with role development and user administration. This is due to the ownership of roles, which is spread out to the appropriate managers who understand and owns the business processes the roles are part of. In this way SAP consultants don't have to take on responsibility for business processes, which they don't own.

What about risks, tcodes, authorization objects and other access rights?

You may wonder why tcodes and authorization objects haven't been mentioned in this article.

The reason is, that an enterprise needs to be aligned on this higher level of business roles before it can begin the journey establishing a more secure use and implementation of tcodes and authorization objects. This will require a governance model for these elements and a technical translation of the risks. The risks are then translated to which tcodes, authorization objects and authorization object field values. This will hopefully be explained in a later article.

The reason this article doesn't describe how to align other types access rights is, that SAP authorization concepts usually are the most complex to align in an Enterprise role concept. But the model and method could be expanded to also cover other types of access rights, such as Active Directory, by relating these access rights to the Enterprise business roles.

Related Content

www.brcommunity.com/

SDN resource center to “Identity and access management”:
https://www.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/8039306e-cea4-2a10-15b9-8e96d40c51ef

SDN resource center to “Compliance”:

https://www.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/a04c8d47-1991-2a10-7696-e29422348813

Copyright