The business perspective on roles Including root causes of implementation problems and proven ways to overcome them

Marc Sel

PricewaterhouseCoopers
marc.sel@pwc.be

Abstract

We present a new way for addressing the business aspects of roles and provisioning. We will quickly outline what is meant by roles and provisioning. We will then discuss what is commonly understood by 'business aspects'. Subsequently root-causes for identity management project failures are analysed. A dual track/multi-layer approach to overcome the major hurdles is then introduced, and learning from a case study is discussed.

These six 'root causes' are: (1) language (different stakeholders speak different languages), (2) lack of distinction between accountability and responsibility, (3) mismatch between expectations of centralised top-down control models such as COSO and today's mainly distributed organisations, (4) technical incompatibilities of most of today's systems, (5) SOD is inherently hard to achieve with the current technical state-of-the-art, and (6) low visibility of access control issues makes it hard to obtain adequate funding,

The innovative aspects of our approach can be summed up as:

- three layers of activities (coordination, business and technical)
- adaptation of various software-based techniques from such as 'Use Cases' combined with distributed email campaigns to translate requirements into tangible solutions that can immediately be appreciated.

We illustrate how we addressed these six ‚root causes' during a project.

1 Roles and provisioning

1.1 Introduction

Most medium to large sized organisations today built up and manage what could be referred to as their 'authorisation space'. This space is essentially structured into three dimensions: the different user communities (subjects), the ICT services and applications (objects), and the processes allocating users authorisations onto these services. In the real-world, this space can be impressively large. For one particular company with 40.000 employees (and excluding the authorisations of customers on company systems) we estimated the total number of authorisations that were managed around 35 million. Since that organisation's authorisations were decided by a core team of 10 persons, this meant that on average, every authorisation manager was dealing with approximately 3,5 million authorisations. Most of these

authorisations have been built up over the years, often surviving multiple rounds of business reorganisation. Ensuring that authorisations are configured appropriately and stay that way is a challenge.

1.2 IdM initiatives often fall short of meeting expectations

Many vendors tout Identity Management (IdM) systems as the overarching solution to the management of user identification and authorisation. Such systems are aiming essentially at quicker turnaround time for user-id and authorisation provisioning. These systems typically address the aspects of authentication, directories, provisioning and access control. While the actual success rate of such Identity Management projects varies, their approach with regard to access control is typically incomplete. Furthermore there is a clear increase in regulation resulting in ever more complex compliance requirements. So most organisations find themselves confronted with both a complex authorisation space to manage and the requirement to do this in a sufficiently transparent and understandable way. The onus of demonstrating this is imposed on the organisation.

1.3 Roles and provisioning

1.3.1 Roles

With 'roles' we refer by default to roles as defined in the RBAC standard.

The word role as in ‚Role Based Access Control' means different things to different people. The RBAC movement picked up a big momentum, and much work has been done, both theoretical and practical. The original theoretical model has greatly been expanded, and the NIST (National Institute of Standards and Technology - US) published an ANSI standard. Vendors implemented role or RBAC functionality (at least this became common terminology) in relational databases, in operating system and application security, and even in Windows2003. The basic model is based on a 'User-Role-Permission' paradigm. Since users typically access a system via (multiple) sessions, this is also reflected.

1.3.2 Rules

A number of products claim they can provide RBAC functionality through their rule-based approach. A rule-based approach essentially allows to express a security policy in terms of groups and ACL's (access control lists). The minimal approach is to use regular groups ('static' groups) – this is what has been done by Unix for decades. These groups can be structured in hierarchical fashion, allowing inheritance. Furthermore dynamic groups are added, which are constructed 'on the fly' on the basis of filters working on attributes (e.g. LDAP-based), applied to users or groups. You can then express access as "allow (or deny)" for members of particular groups (static or dynamic). You can further add constraints on the basis of e.g. time, context or IP address. This approach has also been referred to as EDAC (Enterprise Dynamic Access Control).

1.3.3 Provisioning

Originally the term 'provisioning' was used restrictively to refer to the provisioning of users on platforms only. Key aspects were provisioning policy and rules engine, workflow, repository and connections to target systems. As provisioning systems extended their functionality, they added possibilities to relate provisioned users to groups on the target systems. In this way they evolved towards Identity and Access Management systems. However, creating hierarchical group-structures and relating groups to actual resources on the target system can also be considered as part of the provisioning challenge. Given the technical diversity of platforms and applications, this is significantly more difficult.

2 The business aspects

2.1 Business aspects of roles and provisioning

Business aspects are typically oriented towards business concepts such as 'Competitive Advantage', 'Compliance', 'Cash flow', 'Delegation and Empowerment' and 'Time to Market'. Alternatively, there is also a 'downside' where problems or negative consequences are categorized. We will first briefly touch upon the 'downside', before discussing the more positive business aspects in the 'upside'.

2.1.1 Downside – negative consequences

The following elements are often identified within larger scale organisations:

- Since it's very difficult to know which 'old' privileges are no longer needed when a person changes position, it is common for 'collectors' to appear in the organisation – people that collect privileges over their career without ever dropping any privilege
- It is common to copy privileges from an existing employee to a newly hired person, taking on the same or similar role. However, this will have dire consequences if the former employee is such a 'collector'.
- Unidentified or unresolved 'SOD' (segregation of duties) issues – leading to compliance violation;
- Access control problems at the level of Operating System or Database infrastructure, supporting financial applications (people with too many/too few authorisations, orphan (unused) definitions in the system etc) – leading to security exposures;
- Development staff can run business transactions in production – leading to security exposures or operational errors;
- Large number of users with access to all kinds of 'super user' transactions in production – leading to security exposures;
- Terminated employees or departed consultants still have access – leading to unacceptable accesses;
- Posting periods not restricted within GL application – leading to lack of financial integrity;
- Custom programs, tables & interfaces are not secured (since they cannot be covered via a standard access control solution) – leading to security exposures;
- Procedures for manual processes do not exist or are not followed – leading to a lack of mitigating controls.

2.1.2 Upside – roles and provisioning as a business enabler

Business aspects are typically expressed in terms of 'Competitive Advantage', 'Compliance', 'Cash flow', and 'Time to Market'. We are convinced that by identifying and addressing the right IAM challenges, the IAM solution allows an organisation be in tune with 'the business'. Let us briefly review each of the above aspects:

- 'Competitive Advantage' – differentiating products come from differentiated business processes – hence IAM should facilitate taking responsibility within the business processes to enable differentiation;
- 'Compliance' – hence IAM should help demonstrate that appropriate controls are in place and complied with, preferably in a repeatable and cost-effective way;

- 'Cash flow' – IAM automation should translate to cost reduction due to having more effective management;
- 'Time to market' – IAM internal process speed should facilitate having the right people with the right authorisations at the right time.

Furthermore, having appropriate roles and provisioning in place helps to combat the many possible 'leakage' scenarios where employees may see increased opportunities for "small theft" of goods and services.

2.2 The business case

The ‚Business Case' is a description that presents a comprehensive view of a project or programme and:

- Verifies the solution to a business problem that meets the needs of the organisation;
- Provides measures of success; and
- Provides a consistent message to communicate to many different audiences.

There is no single best way to describe a Business Case. We make use of the model illustrated below.

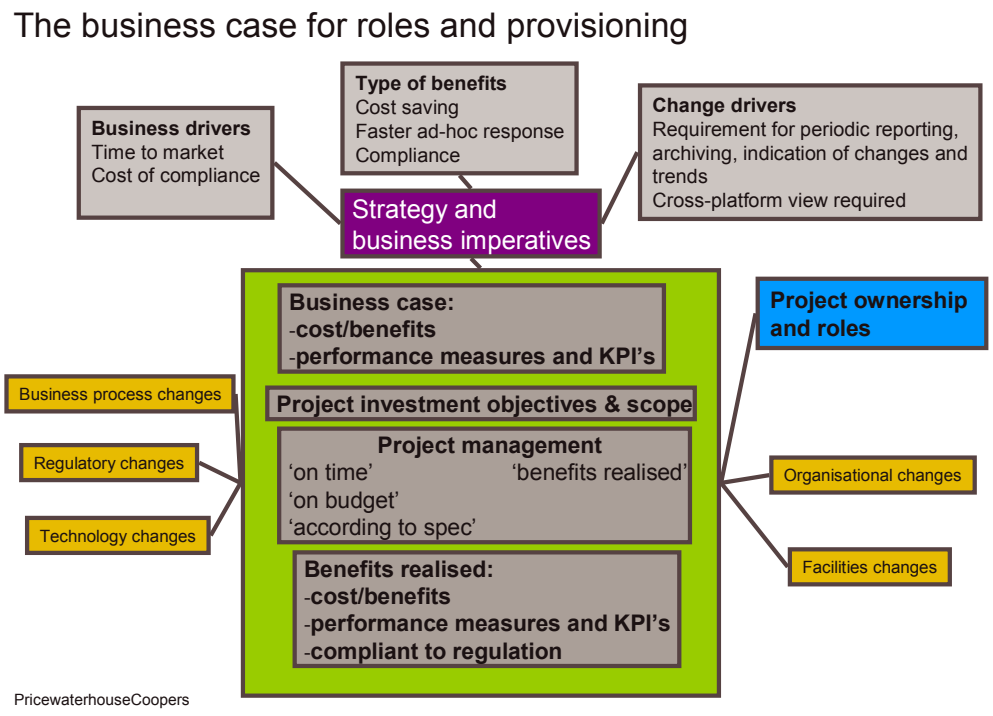

Figure 1: Structure of a possible 'Business Case' for roles and provisioning

3 Solution and case study

3.1 The challenge

The case study organisation is a European company that is subject to both national competition regulation and the US Sarbanes-Oxley act. They employ approximately 30.000 employees. They recognised the need to strictly manage authorisations, and initiated a company-wide identity and access management project to address the roles and provisioning issues.

3.2 The Business Case

This particular organisation was confronted with structural changes in its liberalised market. This led to significant organisational alignments both for business and IT. As a consequence of reorganisations and outsourcing, their identity and access control landscape had been somewhat neglected. This led to the situation that there was no longer clear accountability over identities and access control, and there was no clear ownership of the corresponding processes. However, under regulatory pressure, this had to be addressed or the company faced potential removal from the US stock exchange and fines from the national regulator.

This situation was rectified in two phases. In a first phase, measures were taken to demonstrate regulatory compliance via cleaning of data and authorisations, and reporting/resolving any SOD issues. In a second phase, a structural approach was followed to bring the IAM (Identity and Access Management) processes under control of the business departments.

The strategic intent was to enable the business departments to structure authorisations to their needs, under their responsibility. Furthermore, compliance requirements should be met. And there was the additional goal to increase productivity by shortening the cycle to get staff and contractors fully up-and-running in the client's processes.

The consequences of doing nothing were considered as undesirable, since both the operational and regulatory pressure would only increase. Hence a business sponsor who is accountable for the delivery of the project objectives was identified, as well as a project manager. Subsequently the key internal and external stakeholders were identified, and a technical solution was selected in line with the IT strategy.

3.3 Root-cause analysis

We witnessed on various occasions the outcome of unsuccessful or only partially successful IAM projects. On this basis, we performed a root-cause analysis.

We identified the following six 'root causes'

1. Language: different stakeholders speak different languages. While the final accountability over access and segregations of duty should reside with the business owners, IAM implementation is a very technical issue, across different systems and technologies. Business owners speak in terms of 'Order-to-Cash', 'Procure-to-Pay', 'Acquisition', 'Year-end Closing' etc. The implementation of these processes resides finally with people making use of programs, transaction codes and tables. IT people speak in terms of transaction codes, program names, database tables, or application objects. Despites their name, Service Oriented Architectures or Web Services are not going to bridge this language gap.

2. Lack of distinction between accountability and responsibility. In an organisation, the CFO typically assumes final accountability for the integrity of the financial statements. Business-line executes assume final accountability for the profitability of their line-of-service. When it comes to IAM, the final accountability for authorisations will reside with the various executives. However, they cannot be bothered with the technicalities of the IAM solution, or intervene in the low-level workflows.
3. Mismatch between expectations of centralised top-down control models such as COSO and today's mainly distributed organisations. While COSO is probably the most influential internal control model, it is inherently assuming that control is centralised. Today's organisations are often very networked and distributed, making it hard to achieve such a control model.
4. Technical incompatibilities of most of today's systems. Many systems have been built to perform business processes. Unfortunately, their identity and access control components are widely incompatible. The simple notion of 'group' for example is widely different in implementation between Unix, RACF and Windows. The applicative authorisation concept of mySAP is different from that of the Oracle E-Business Suite. One level down, the authorisation concepts of a database are different from those at the Application Server (e.g. J2EE) or Operating System level.
5. SOD (segregation of duty) is inherently hard to achieve with the current technical state-of-the-art. Original access control models implemented in the typical commercial products did not allow this. While it is possible to restrict authorisations via e.g. platform groups, application tables or SAP profiles, it is typically not technically feasible (or at least not trivial) to implement SOD. For this reason many company resorted to procedural controls.
6. Low visibility of access control issues makes it hard to obtain adequate funding. As access control is inherently technical and sometimes even rather complex, it can be labour intensive. This makes it often quite expensive, and investments are harder to justify unless you're a major player in e.g. the Financial Services industry.

We subsequently identified mitigating measures that address these various causes.

3.4 The solution

The innovative aspects of our approach can be summed up as:

- three layers of activities (coordination, business and technical); and
- adaptation of software techniques such as 'Use Cases' combined with distributed email campaigns to translate requirements into tangible solutions that can immediately be appreciated.

In each layer many different activities take place. We highlight those that we believe add most value.

3.4.1 Three layers of activities

Coordination - addressing root cause 1: the language issue
The language spoken by the various stakeholders is different which leads to misconceptions and inappropriate assumptions. As solutions, we used workshops, and documents that contain a clearly defined vocabulary, linking the business language to the IT security language.

We found it important to make the distinction between 'business roles' that are allocated by the 'business application owner' to users, and the 'technical roles', which are descendant roles of those 'business roles'. These 'technical roles' contain the technical resources required for business process execution.

Coordination - addressing root cause 2: the lack of RACI
With regard to responsibility for identity and access control, the distinction is often not made between being accountable and being operationally in charge - for this reason business departments are often reluctant to take up their real responsibilities

A clear segregation between final accountability and responsibility is required. We prefer to align on the well-known RACI-model (**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed). We use the term 'accountability' to refer to the single party that assumes final responsibility. We use the term 'responsibility' to refer to the more day-to-day exercising of the related activities. The party that is responsible reports to the party that is accountable. Both accountability and responsibility can be delegated. However, a clear hierarchical structure is required, including reporting.

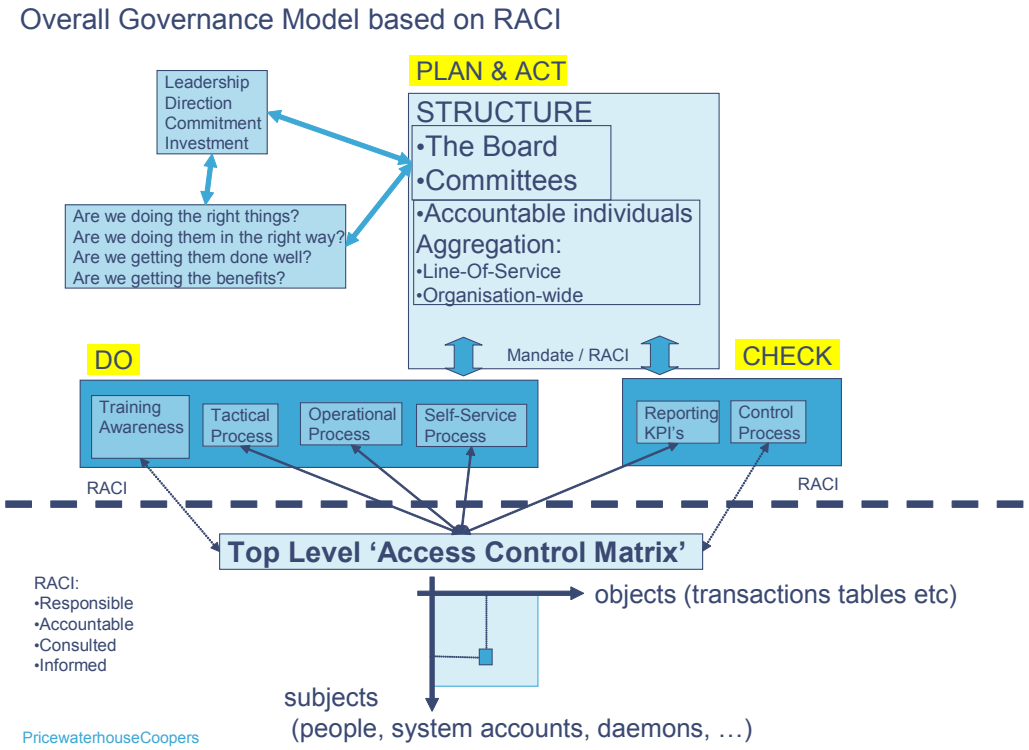

Figure 2: Use of governance model with RACI.

The overall model is divided into two halves. Above the 'dotted line' the managing domain defines structures and processes for the 'Plan, Do, Check, Act'. Below the 'dotted line', the managed domain contains the actual identity and access repositories. We tied the RACI attributes to the IAM data model, and used them to govern the workflow. Owners receive the mandate to be 'accountable', but they can delegate 'responsibility' to lower levels. However, they remain finally accountable. Resource or privilege owners are accountable for granting access to their resources. This means they are accountable for establishing an appropriate role structure, and assigning users to those roles. Obviously, for a large scale public or private organisation, a sound delegation model is required.

Business - addressing root cause 6: the lack of funding
Low visibility of access control issues makes it hard to obtain adequate funding, while addressing e.g. SOD is inherently difficult and hence expensive. Hence we used a business case approach structured as per figure 1 to obtain attention and secure adequate funding.

3.4.2 Software-based techniques

Addressing root cause 3: balancing centralised/decentralised aspects
We observed a certain degree of mismatch between the expectations of centralised top-down control models such as COSO and today's mainly distributed organisations.

Hence we use automated email campaigns to efficiently confirm the RACI assumptions. We used different types of campaigns. User-based campaigns invite the owners of organisational units (or cost centres) to approve the identity of actors in the authorisation model. Role-based campaigns invite the owners of the roles (i.e. the responsible parties) to first accept their ownership over the roles, and subsequently to validate the access of users onto those roles. This can be achieved e.g. by using automatically generated emails to provide access to workflow on a central authorisation portal. In a later phase, also Segregations-of-Duty can be defined, can receive an owner, and their violations can be accounted for via (signed) emails. Violations can be 'accepted' if e.g. sufficient mitigating controls can be demonstrated, or can be 'resolved', i.e. their causes removed. We found email to be a great facilitator for reaching out into today's distributed organisations.

Addressing root cause 4: technical incompatibilities
Technical incompatibilities of most of today's systems make it hard to build up a view on the complete authorisation landscape. For this purpose we introduce what we refer to as 'unification'. We use a simple NIST RBAC 'user-role-permission' model to establish a minimal common denominator for all the different systems. We established a single role-repository, split between 'business roles' and 'technical roles'. Within these technical roles, the different authorisation modes of the various platforms are accounted for.

Addressing root cause 5 – hard to achieve SOD's
SOD (Segregation-Of-Duty) is inherently hard to achieve with the current technical state-of-the-art. Many legacy access control technologies such as ACL's, groups, SAP authorisation objects etc do not allow to express an SOD constraint. To mitigate this weakness, SOD has often been incorporated in subsequent complementary products. However, this meant additional implementation costs and more difficult of integration.

In the SAP world, VIRSA and similar products emerged as enablers for the solution. However, many companies are confronted with having to manage more SOD's that just in SAP. Proprietary legacy systems have particular needs for managing their SOD's.

We decided to use a database as the major repository for the role model of the IAM solution, but store SOD constraints in a dedicated engine from Eurekify. We let the IAM solution validate its actions with regard to SOD in the dedicated engine via Web Services.

Overall architectural model
We used the following overall architectural model.

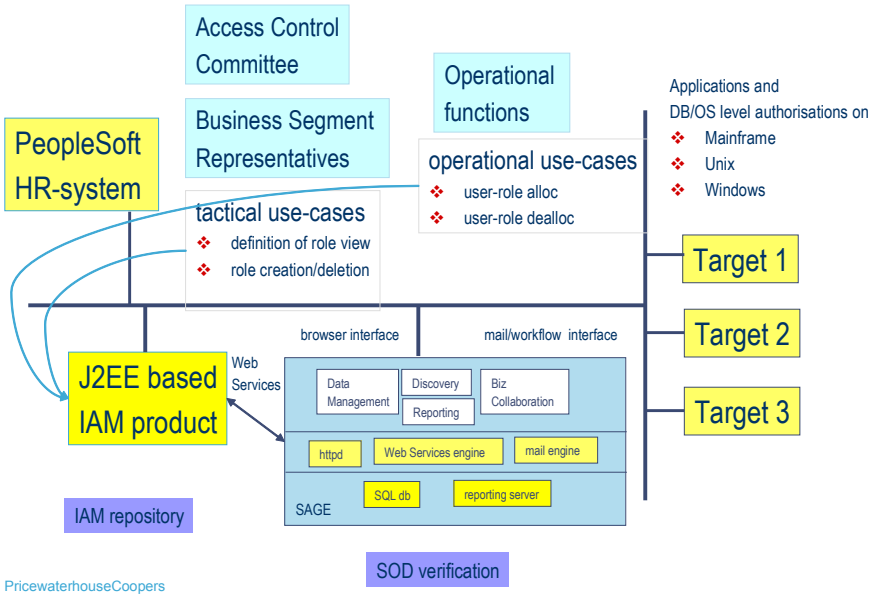

Figure 3: Architectural model

Role creation and allocation is implemented in workflow. By making use of the RACI-attributes of the users, roles and resources in the various use-cases implemented in the workflows, we made sure the final accountability of the authorisations was allocated to the right organisational function (representatives, committees, etc).

4 Conclusion

We presented a new way for addressing the business aspects of roles and provisioning. We identified six 'root causes' for failures of large scale IAM projects: (1) language (different stakeholders speak different languages), (2) lack of distinction between accountability and responsibility, (3) mismatch between expectations of centralised top-down control models such as COSO and today's mainly distributed organisations, (4) technical incompatibilities of most of today's systems, (5) SOD is inherently hard to achieve with the current technical state-of-the-art, and (6) low visibility of access control issues makes it hard to obtain adequate funding,

During the Case Study project, we overcame these 'root causes' by introducing three layers of activities (coordination, business and technical), and by making use of various software-based techniques from such as 'Use Cases' and workflow, combined with distributed email campaigns. Furthermore the use of RACI-attributes enabled us to allocate final responsibility within the business community through the workflow.

We are now looking into ways to further formalise, automate and improve our way of working.

References

[NIST2001] ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, pages 224-274.