

SecurIT RoleManager™ Return on Investment



The challenge of user privileges

One of the challenges organizations are currently facing is to grasp control over user privileges of ICT applications.

The major issue is that over the past years, the number of user privileges is growing very fast, and maintaining user privileges is a challenging task. Indeed, limited ICT staff cannot cope efficiently with manual administration of these user privileges.

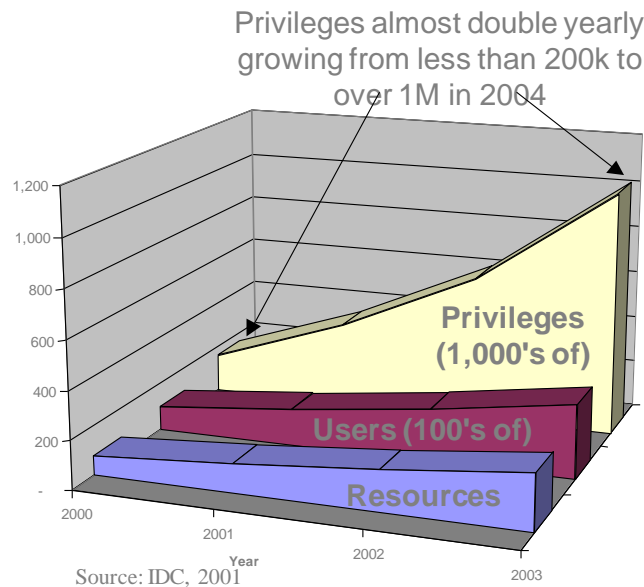


Figure 1 : Estimated Privilege distribution Activity in typical companies

When ICT organizations run out of controls, this eventually leads to situations where:

- Unused accounts proliferate
- Turn-on time rises for user privilege creation
- Privilege review is impractical
- Security audits fail
- User down-time increases

- Security admin requests staff increases
- Help desk requests staff increases

Role Based Access Control

In the 1990s, Role Based Access Control (RBAC) concepts and standards were introduced and standardized. RBAC has now matured to the point where it is being consistently prescribed as a generalized approach to access control.

Essentially, users are not assigned permissions directly, but only acquire them through their role (or roles). Management of individual user rights becomes a matter of simply assigning the user to the appropriate roles, rather than to low level data objects.

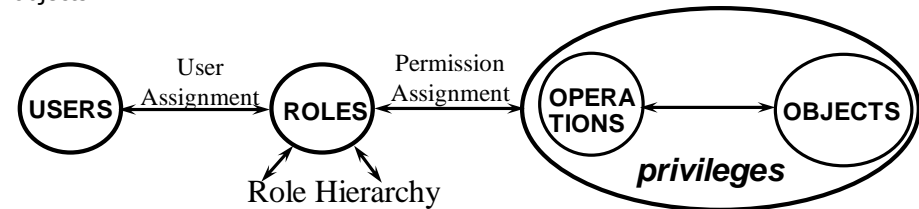


Figure 2 : RBAC model

By further developing the role concept to include a role hierarchy, one can even further reduce the number of possible user assignment actions, as well as reducing the number of low-level privileges to be assigned to a role, using user and privilege inheritance across the hierarchy, as illustrated to the right:

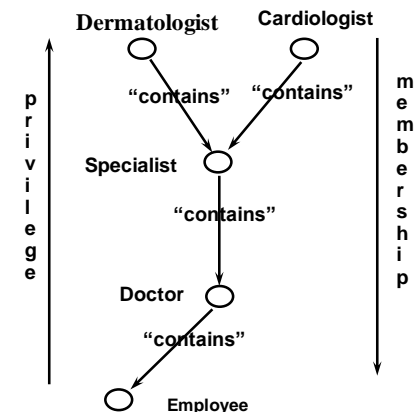


Figure 3 : Sample Role Hierarchy

SecurIT RoleManager™ Return on Investment



Economical aspects

While the RBAC model is often described to be advantageous from a security and administration perspective, cost estimations for real organization are difficult to find. This document illustrates how any organization can easily estimate such economic aspects. The case study section gives sample cost estimation for a mid-size organization.

A Comparison standpoint: which alternative ?

Usually, if RBAC is not implemented, when a user wishes to access an existing ICT application or resources(s), he requests this privilege from someone within the organization. Existing security controls mandate some approval each time a privilege is requested. Once the request is verified and approved, then ICT systems are modified to allow this new privilege. We further refer to this method of granting low-level privilege to users as *request-based provisioning*.

This method is ICT resource centric, as the organization has to process each request for every user and every ICT resource.

This is a key difference with the RBAC model, where privileges are inherited automatically once a user is assigned to a role. Therefore the number of administrative actions essentially scales with the number of high-level roles for RBAC, whereas for request-based provisioning, it scales with the number of low-level resources or privileges.

Assumptions

In order to gain most of the benefits from RBAC or request-based provisioning, it is essential to have an automated user provisioning tools. Its responsibility is to ensure that user accounts and user privileges are configured in all the ICT platforms and applications, regardless of the provisioning model. These tools have been available on the market since early 2000 and are now very mature from a technological standpoint. We therefore assume that such system is in place, regardless of how the user privileges are currently administered (RBAC or Request based).

A simplified cost Model

The easiest way to compare the cost model of either RBAC or Request based provisioning is to consider the various use cases.

In both models, changes to the current model of users and privileges are required when:

1. People are hired or leave the organization
2. ICT Privileges (either operations or objects) are added
3. People assignments changes as part of their professional career

By estimating the number of these changes on a yearly basis, and by assigning a mean administration time for each case, it is relatively easy to compute an estimation of the recurring operational cost for any organization.

It is important to note for cost comparison purposes, one has only to take into account administrative labor cost, associated with time to perform the follow actions:

- Making request (for new privileges or role)
- Having it checked and approved

Other secondary costs elements have been ignored to simplify the model. The ICT provisioning part is assumed to be fully automated.

The total cost varies with the following factors:

- Number of users
- Average number of privileges per user
- Average number of high-level business roles per user
- Hire/turnover rate
- Number of new privileges added to the ICT systems every year
- Role turnover rate
- The % of RBAC exceptions (old applications, exception handling,...)

Acme Case study

Based on the cost model previously developed, we have modeled the sample mid-size ACME organization with the following keys figures¹:

- Mean time to perform each specific administrative action is 10 minutes, and an average hourly cost of 28,3 \$.
- Number of users : 1000
- Average number of privileges per user : 20
- *Average cost to assign or change one privilege to a user : 8,02 \$*
- Average number of high-level business roles per user : 3
- *Average cost to assign a high level business role to a user : 9 \$*
- *Average cost to create/Adapt a high level business role: 120,5 \$*
- Hire/turnover rate : 10%
- Number of new privileges added to the ICT systems every year : 100

¹ Figures in italic are calculated from others (provided here for comparison purposes)

SecurIT RoleManager™ Return on Investment

- Role turnover rate : 15%
- A maximum of 75% of RBAC-enabled requests achievable, 25% being still served on a per request basis

The yearly recurring operational labor cost for handling request based provisioning 802.542 \$. When RBAC is deployed, this yearly recurring operational labor cost is reduced to 260.118 \$, as a consequence of the reduction of the number of individual administrative transactions to be performed.

The following chart illustrates the cost evolution of the Acme organization, when progressively² introducing RBAC processes and by further taking into account additional project and software costs:

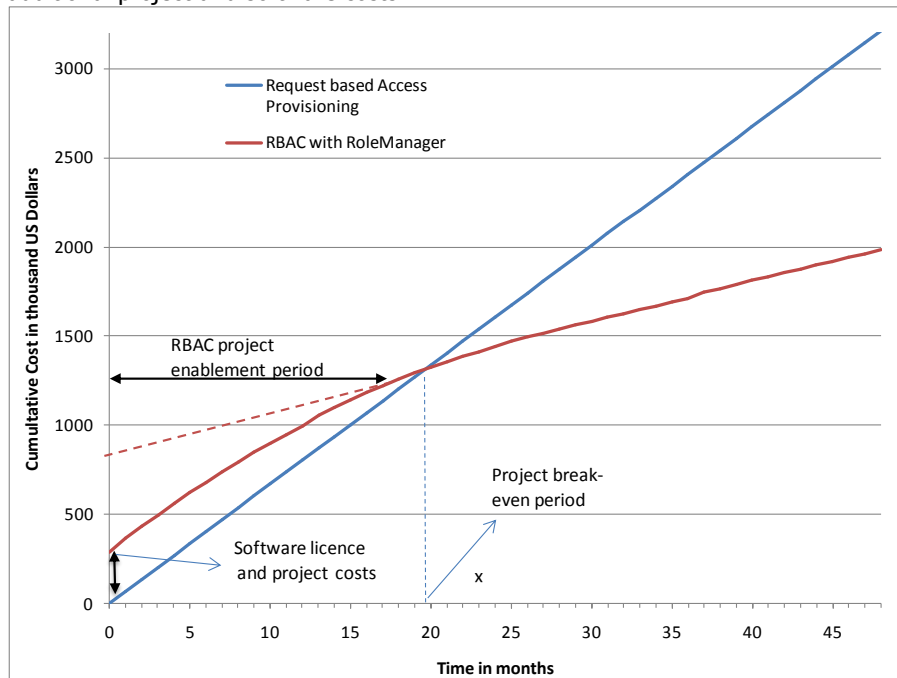


Figure 4 : ACME Cost evolution for RBAC versus request-based provisioning

² The pace of RBAC-enablement is primary driven by an organization will and capacity to drive changes. In this example we took a progressing linear enablement of RBAC from 0 to 75% over a 24 month period.



This further illustrates that, to fully benefit from the RBAC savings, it is essential to include RBAC enablement as quickly as possible into existing Identity & Access Management process and tools. By introducing RoleManager, ICT Operations can easily make an initial role model, based on existing privileges from the target ICT platforms and applications, usually in a matter of days. The model can then be quickly enhanced by introducing a role hierarchy. Then, the sooner the organization can revise and adapt its approval processes, the quicker the project break-even point is reached, therefore delivering full RBAC recurring savings.

This cost model is available as a Microsoft Excel spreadsheet and is available to SecurIT partners for helping their customers evaluating RBAC enablement project savings.

RoleManager benefits

RoleManager is an IBM Tivoli Identity Manager (ITIM) plug in for organizations that deploy an RBAC role model. The RBAC model simplifies and rationalizes ICT permission management, ensuring efficiency, security and reducing related recurring operational cost. Ultimately, RoleManager allows business people to manage security by letting them assign users to meaningful business roles.

For further information, please contact SecurIT:

SecurIT Belgium

Park Office
Franklin Rooseveltlaan 349d
9000 Gent, Belgium

Tel. +32-9-265 02 70
Fax +32-9-265 02 50

E-mail: Info@securit.biz

SecurIT Netherlands

Overschiestraat 184 K
1062 XK Amsterdam
Netherlands

Tel. +31-20-408 44 27
Fax +31-20-408 44 25

Web: <http://www.securit.biz>