A best practice case implementing Role Based Access Control at ABN AMRO

A long and winding road
1. Introduction
2. Reasons for the RBAC project
3. Background
4. Concept
5. A slow start
6. Soll versus Ist
7. A slow start
8. Strategic Choice
9. Off shoring the production
10. The project
11. Current state and lessons learned so far
12. Potential benefits for the future
13. Summary
14. Future

Questions ? Please interrupt !
Introduction

Who is Martin Kruit?

40 Yr

Officer Royal Dutch Navy
Fokker Aircraft

At ABN AMRO since 1994, working in several positions:

programmer (COBOL, Easytrieve Telon etc.)
Business analyst
Manager business support Operations Derivatives markets
Manager Reference data Operations Netherlands
European Head Reference data Wholesale clients
Manager Information security desk Wholesale clients NL
Manager Information security desk Services OPS NL
Manager Finance Data Management – Expertise centre
Reasons for the RBAC project

- DNB audit of our “Chinese Walls” – Proof of compliancy had to be given
- Internal audit in which “need to know” had to be proven
- Costs for ID`s that were never used
- Stricter regulations
Background

- The project had four main objectives:

1. To bring the access security process at a professional level by centralising the operations and increase the transparency of the process towards line management

2. To optimise the Access security service and to create cross-BU en cross-country synergy

3. To create enough critical mass in order to automate the process and gain efficiency and comply to BASEL II and SOXA regulations

4. Execution on an “low cost basis”
Background

Observations

• Current in-efficient setup of security maintenance function and several years of non-focus caused:

  – Lack of control and reporting on System access
  – Lack of control and reporting on System Authorization
  – No clear insight in roles and responsibilities
  – Duplication of effort across WCS Netherlands

• Scattered and redundant efforts throughout the whole organisation

• High operational risk preventing a lower risk indicator
Concept

1. “Clean up the house”
   - Redefinition of the access process with EDS (outsourced IT partner)
   - Create a Single point of Contact for our (internal) customers
   - Creation of (R)ole (B)ased (A)ccess (C)ontrol templates
   - Removal of all surplus rights, build up in the years

2. “Right sourcing, right sizing & Tooling”
   - Rationalise all User security access for Applications of WCS EMEA
   - Install a Workflow-tool
   - Setup function & competence profiles
   - Setup RBAC-control administration & maintenance
   - Periodic System Access & User Authorisation reporting
   - SLA Reporting
   - Strive towards a centralised Security administration production with a
decentralised RBAC administration
   - Explicit separation of IT-security and Application security
• “Clean up the house”
Concept - High level business model

Business

Dep X  Dep Y

Organization

Operational role input from mgt.

RBAC

Business-control unit

BC-input and control on roles

Regulations
Compliance
Audit

Current model flow

Reconciliation
RBAC / Actual (clean up)

IT

TOOL

IT

KCP 1st European Identity Management Conference
Munich, May 7-10
Concept- Right sourcing, right sizing & Tooling

Regional user and profile (RBAC) maintenance
- RBAC NL Maintenance
- RBAC EU Maintenance
- RBAC APAC Maintenance
- RBAC ..... Maintenance

Automated profile checking

Access Request Tool (workflow)

- End users
- Authoriser

HR

Appl +systems

Central Sec Admin production (ISD Mumbai)

Third party

Target Model
A slow start

- And in the beginning ........Excel

- We started with a limited scope (IB operations) and with our own developed RBAC model

- Functional view

- Per department

- Administration of the Soll (To Be) situation (See next slide)

- No automatic links to systems

- The project was run from the line organisation due to the “low costs” objective
• We already knew that our current situation was a mess, then why put energy in role mining and investigating the current chaos?

• By focussing on the SOLL situation we knew where we had to go

• We just had to “simply” reconcile the SOLL with the IST no matter what the current situation was
# Excel model

## RBAC Jobtitles - EXAMPLE

**Department:** 123456 - EXAMPLE - NETHERLANDS

### Mandatory

<table>
<thead>
<tr>
<th>Applications</th>
<th>Jobtitles</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS IS</td>
<td>ASSISTANT</td>
</tr>
<tr>
<td>G4/011</td>
<td>GROUP MANAGER</td>
</tr>
<tr>
<td>Request</td>
<td>ADM</td>
</tr>
<tr>
<td>BH1; INF</td>
<td>ADM</td>
</tr>
</tbody>
</table>

### Non Mandatory

<table>
<thead>
<tr>
<th>Applications</th>
<th>Jobtitles</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>ALL</td>
</tr>
<tr>
<td>CIR</td>
<td>GROUP MANAGER;</td>
</tr>
<tr>
<td>MANAGE PICK LIST</td>
<td>MANAGE PICK LIST</td>
</tr>
<tr>
<td>G4/011</td>
<td>Group Request</td>
</tr>
<tr>
<td>ADM</td>
<td>ADM; Request</td>
</tr>
<tr>
<td>BH1;INF</td>
<td>ADM; BH1; INF</td>
</tr>
<tr>
<td>BH2; INF</td>
<td>ADM; BH2; INF</td>
</tr>
</tbody>
</table>

**RBAC Approval**

**Authoriser 1:** BURGHARDT, ARJEN AJ VAN  
**Authoriser 2:**

**Head of Dept:** KEEN, ALBERT ACJ DE  
**Date signed:**

**Signature:**

**Senior Manager:** KRUIDT, MARTIJN MJ VAN  
**Date signed:**

**Signature:**

**ISD:** KRUIT, MARTIN  
**Date signed:**

**Signature:**

---

KCP 1st European Identity Management Conference  
Munich, May 7-10
A slow start

- Enthusiastic start supported by the management
- Decreasing support when it became clear that the departments (and management) had to put time and effort in RBAC creation
- Decreasing support by senior management after closing of the high risk audit issues
- Increased data volume became a bottleneck when working with Excel
- Tactical solution by designing and building our own RBAC application in MS-access
- Strategic solution had to be a proper project
Strategic Choice

Automated profile checking

RBAC NL Maintenance
RBAC EU Maintenance
RBAC APAC Maintenance
RBAC .... Maintenance

B HOLD

B HOLD or Other tool

End users

Access Request Tool (workflow)

Authoriser

Manual provisioning

Central Sec Admin production (ISD Mumbai)

Third party

Manual provisioning

Appl +systems

Automated provisioning

requests
We decided to Offshore the manual provisioning because:

- It offered an attractive cost base, convincing business to go ahead with us
- It offered high flexibility in volume changes and system changes during the project
- Legacy systems were too expensive (compared with manual entry in India) to build and maintain interfaces
- It bought us time to decide which systems would qualify for automatic provisioning
- We could start reconciling as soon as the team was operational without waiting for automated reconciliation tools
The Project

Issues were blocking the cause of the project

- Strategic solution became an “IT Party” with the main focus on London issues
- Cultural differences in security approach
- Time pressure SOX and DNB caused focus only on authorisation of requests in stead off controlling the total process
- Efforts to Financial justification put to much emphasis on auto-provisioning of applications

- Large reorganisation
  - RBAC templates were setup per department with their own roles, roles were redrawn and changed from 1 department to another,
  - The emphasis in the organisation became on geography, due to that, the project management was fully UK, the project clients and initiating business almost all in the Netherlands
The project

Splitup in 2 Projects 1 in unit Europa, 1 in Netherlands

Project in the Netherlands focussed on the functional side of info security

1. Control on the whole process
2. RBAC
3. Manual provisioning
4. MIS for the process

Project in Europe (London) focussed on

1. Technical linkage of applications (automated provisioning)
2. Authorisation of requests
3. Reporting the actual situation in the applications

In the end transformation to 1 global system
Project in Europe now stopped, waiting for the global approach
Desired state
1. Security administration project can not be justified by cost savings only
2. Without constant pressure of Senior management the attention will slip as soon as a department closed it`s audit issue
3. Discipline in following the agreed AO is key
4. In rapidly changing environments RBAC is very labour intensive
5. Business must stay in the lead, not IT
6. HR has a key role, but they have to be told and pulled on board
7. Management of expectations is key, RBAC is not the “Holy Grail” but a valuable tool if supported by the organisation, not only in words but also with action
8. It will only work if everyone is on board. A little secure means NOT secure at all
9. It is wise to have all roles and responsibilities clear, specially towards IT before starting such a project. The delay of setting up a good governance and structure pays back.
10. Manual provisioning is the most flexible interface, assuming it is centrally organised and if it can be strictly controlled (reports and MIS). It is by far the cheapest (offshore).
Potential benefits and threats for the future

Benefits:

Having your RBAC drawn up, it can help you when converting to a SOA environment as it can form the basis of your security service in the SOA structure.

The effort of creating the RBAC should have updated your business control which helps in future reorganisations.

Implementing new systems will benefit heavily due to the clean up and clear overview on who needs what.

Threats:

Once setup, it must be maintained, otherwise all benefits will seize to exist and you are back at square 1.
Summary

- Consolidate
- Optimise
- Automate
The Future

- Still a long straight road, following the lines that have been drawn, but the end is still not in sight.