Identity and Access Control

Managing the authorization repositories to enforce compliance.

October 2006

marc.sel@pwc.be

PRICEWATERHOUSECOOPERS

Agenda/Contents

Section one

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

This presentation is about new ways for

- Managing the complexity of identity and access control in large-scale environments
- Creating cost-effective compliance
- Quick initial review and cleanup
- Automated periodical demonstration

Results in a large European Service Provider

- 48 applications reviewed and analyzed in 4 months
- Created and verified 80 policies with approximately 15 business process rules per policy

Section two

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Objectives of this presentation

- ✓ To explain how new techniques can be put to use, both in small and large scale environments
- ✓ To share experience with regard to the techniques deployed in the pilot project

Section three

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

The challenge

Client is a European-based provider of services, employing approximately 25.000 employees and some 70+ applications

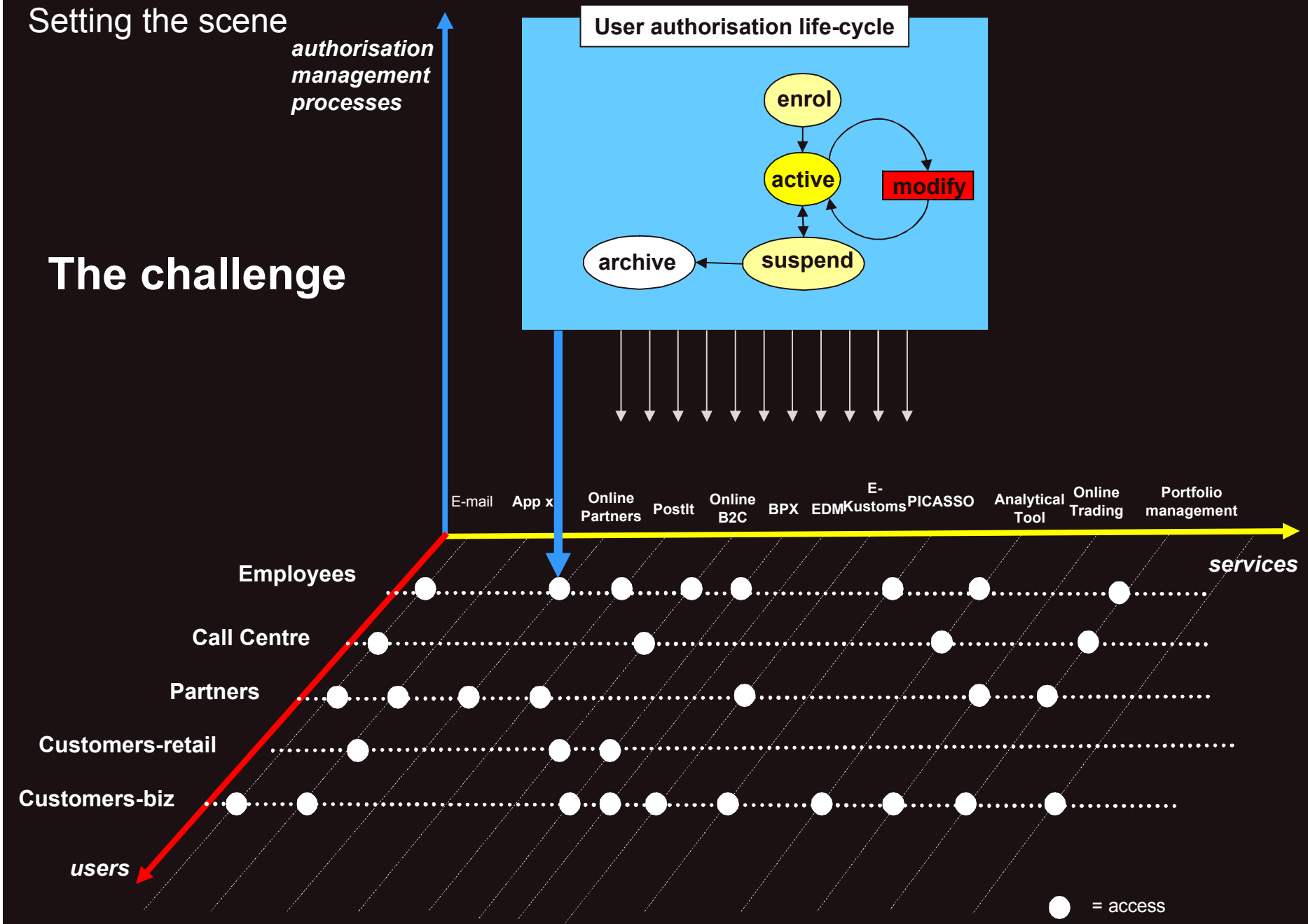
These applications are a mixture of in-house developments and customised packages including SAP and Baan ERP's.

For various reasons, the authorisation landscape could be significantly improved

The client is gearing up for compliance with various regulations including SOX and national legislation, and needs a mechanism to define compliance, and the periodically demonstrate it. The project shall first cover 48 applications.

Setting the scene

The challenge



Objectives of the pilot project

Evaluate the added value that explicit repository management can bring to customer:

by applying it to the two selected applications in two specific areas:

- **Role-based audit and analysis:** evaluating the quality and effectiveness of the current authorizations, and formulating recommendations where appropriate, particularly with regard to data cleaning

- **Compliance verification:** evaluating the compliance of the current authorizations with expectations from
  - SOX
  - SAS 70
  - Competition regulation

Objectives of the implementation project

Implement automated compliance reporting for all relevant regulations for all relevant applications

Regulation: Sarbanes-Oxley, National Competition Legislation, National Industry-segment Legislation

Cooperate with the on-going identity-management initiatives (datacleaning of users, gradual roll-out of new authorisation request system developed in-house)

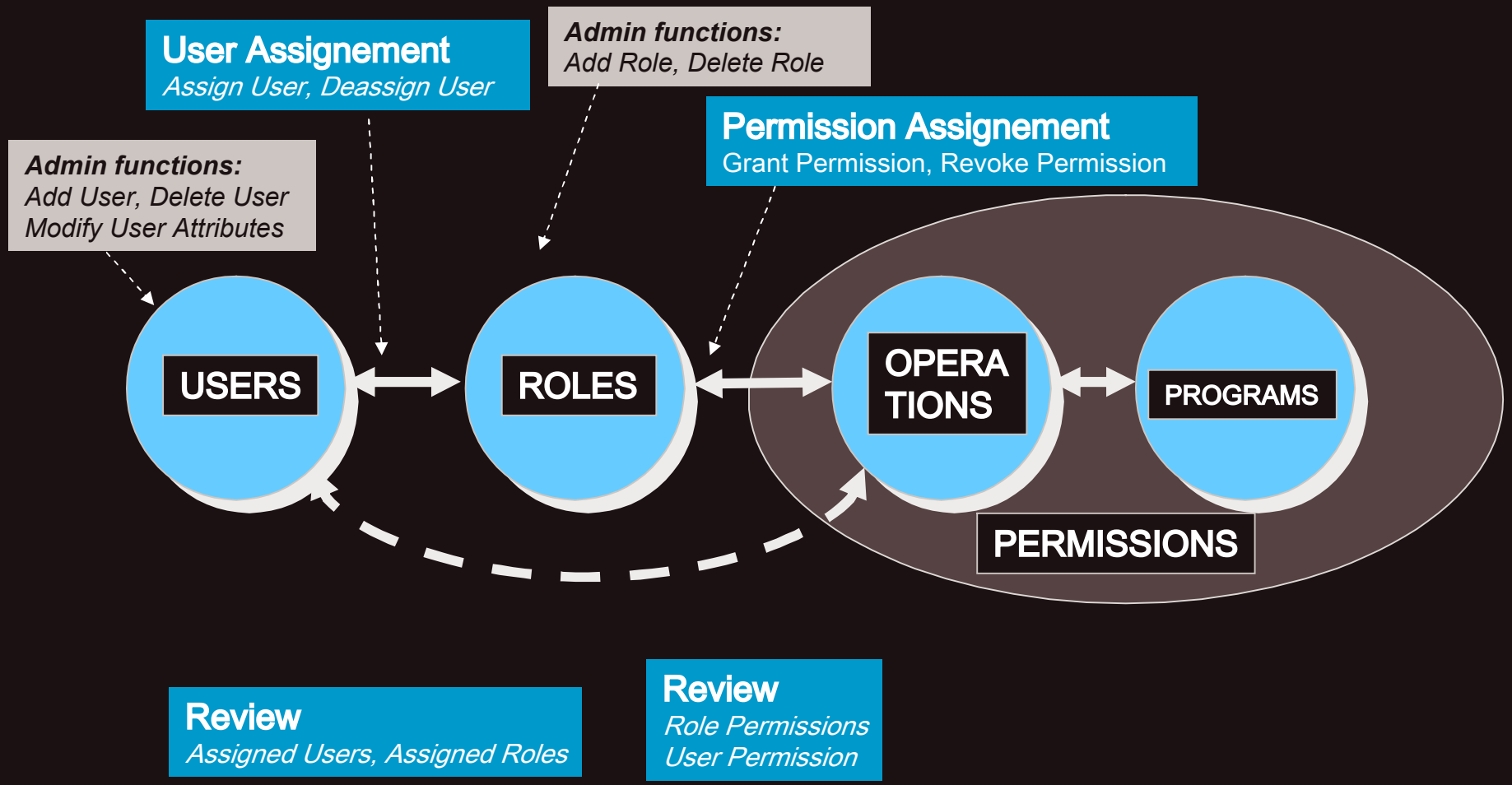
Number of applications: 48

Section four

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Unification
NIST Role-based Access Control model



Control libraries
Proposed structure

We propose a three-tier structure for a control library that is focused on identity and access management:

- Tier #1: the control baselines
- Tier #2: controls related to organisational structure and processes
- Tier #3: controls related to time

Control libraries
Tier #1 – commonly accepted principles

- Individual accountability – authorisations are granted to specific individual users. Use rids/accounts are not shared.
- Single user identification – a user should have a single identifier per platform.
- Authorisations should be allocated through roles (or a similar grouping mechanism). Direct links between users and resources should be avoided.
- No single user should have all authorisations.
- No users should accumulate so many authorisations that there can be reasonable suspicion that the risk for (un)intentional misbehaviour increases.
- There should be no “orphans” in the identity and access management system.
- Obviously the organisation may keep expired users and authorisations for historical reasons, these should however be separated from the active set.

Control libraries
Tier #2 – controls related to organisational structure and processes

- Authorisations should be limited to the appropriate functional organisational scope and processes. Where required this may lead to ‘Chinese Walls’ (ref the well-known Brewer-Nash model)
- Authorisations should reflect a high-level segregation between production, acceptance/test and development environments.
- Authorisations should reflect the required segregation-of-duties (combinations of certain authorisations are to be forbidden).
- Specific functions within the organisation require specific authorisations. For example, auditors will have read authorisations only.

Control libraries
Tier #3 – controls related to time

- Users that are no longer employed or servicing the organisation need to be blocked.
- Users that have not accessed the systems for the last 90 days need to be blocked.

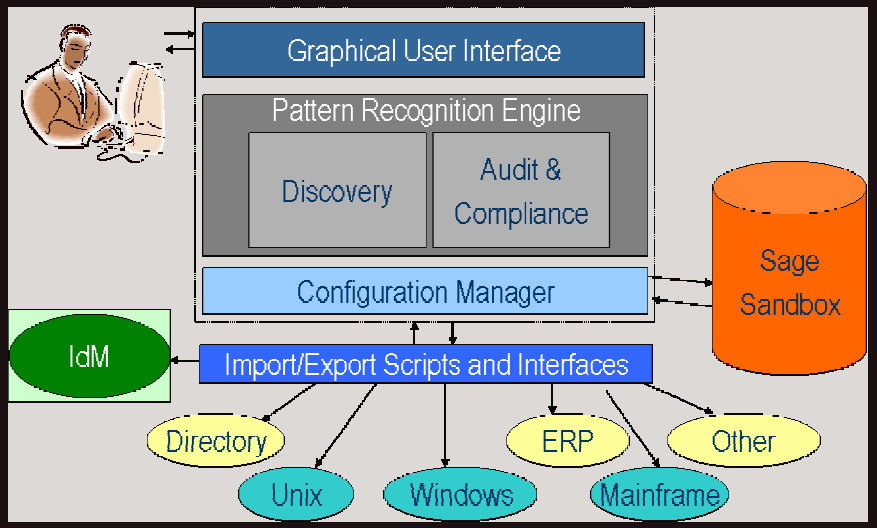
Furthermore, application-specific controls may be required.

Selected technology

- We selected Eurekify Sage DNA (www.eurekify.com)
- Tool combines
  - Role engineering and role mining
  - Automated recognition of out-of-pattern privileges for cleanup
  - Compliance verification based on specified business process rules
- Utilizes advanced pattern recognition technology
- Data model is

  'user-role-resource',

  NIST RBAC-compliant

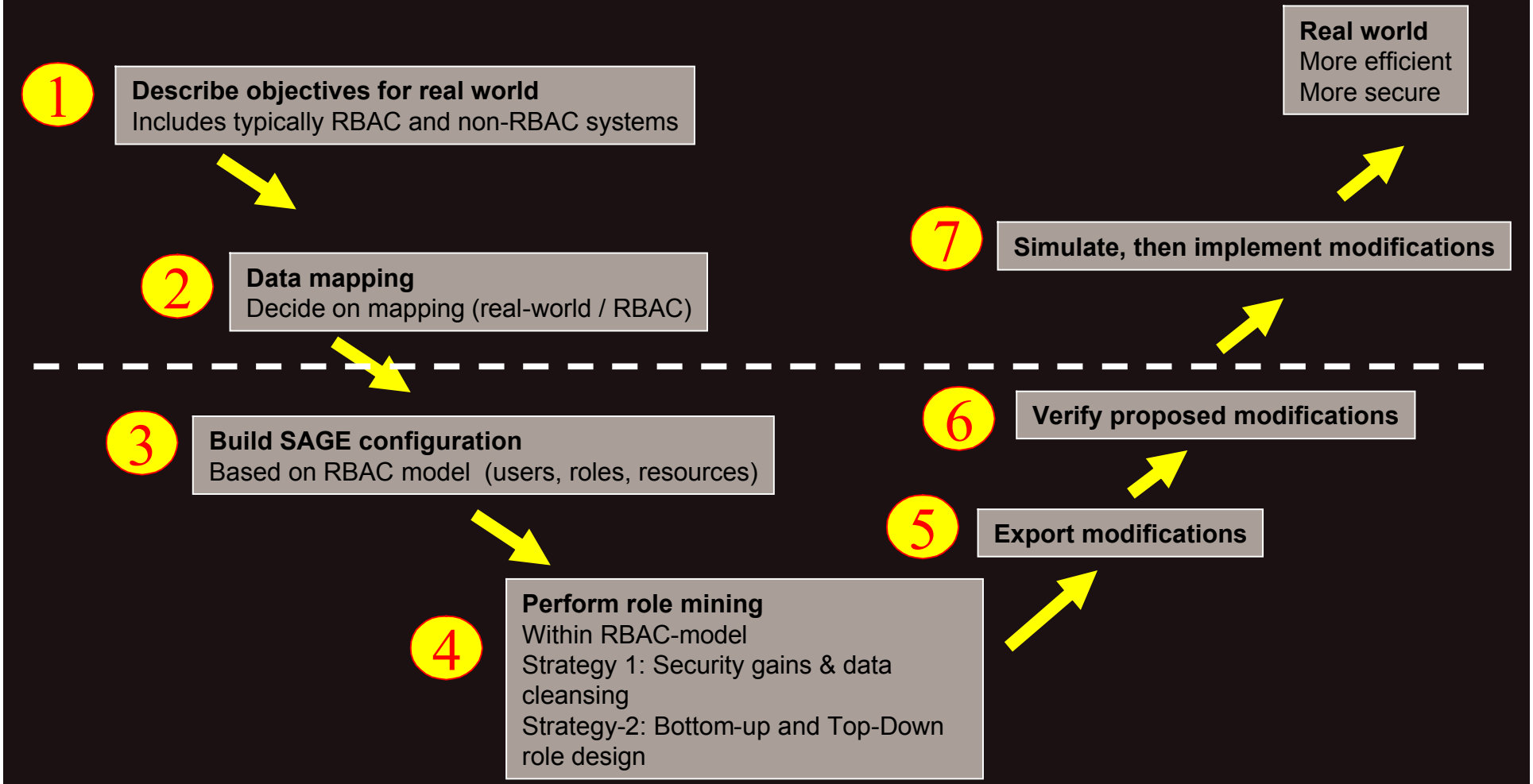


Section five

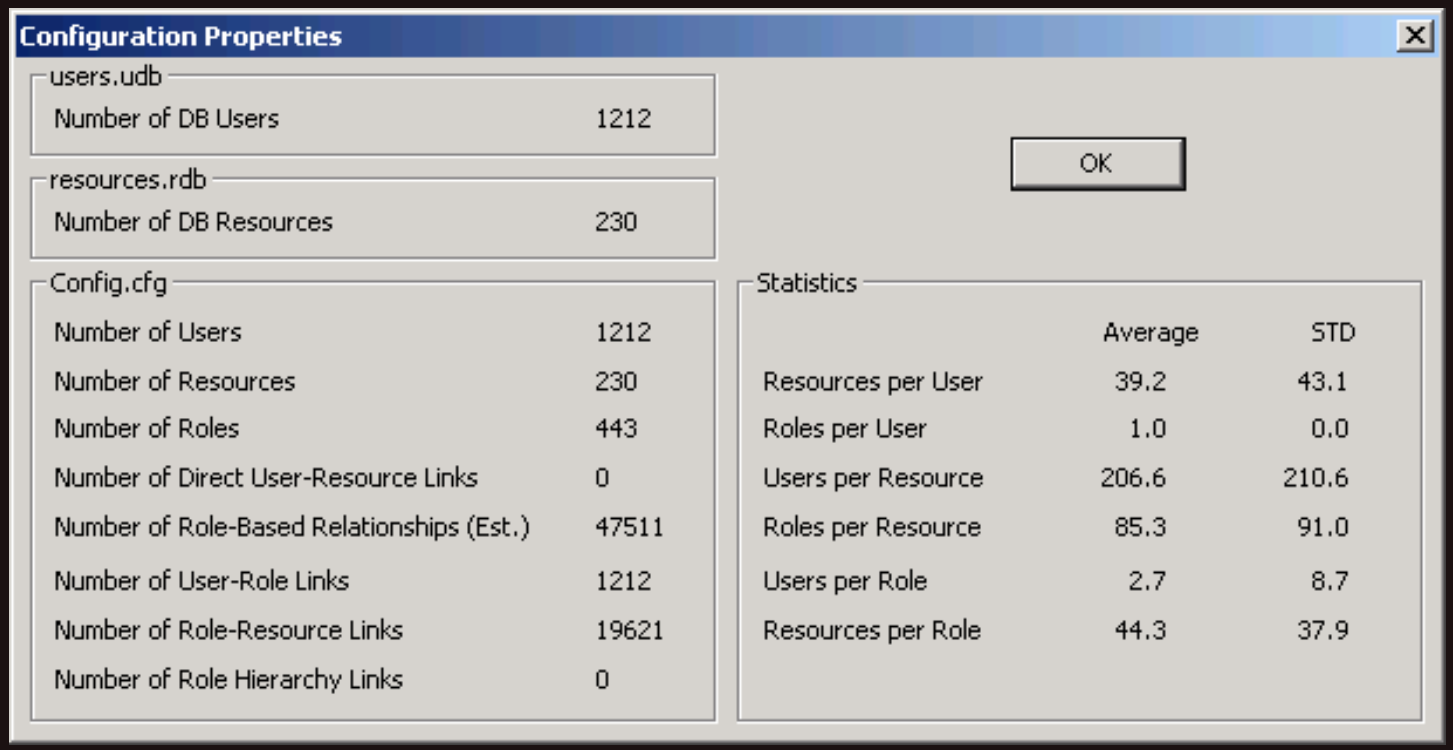
Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Role - mining process



A view on the loaded authorisation data in one application PICASSO (imaginary name)



PICASSO configuration

Analysing PICASSO

As one can easily see, this configuration handled the authorisations of 1212 users, via 443 roles onto 230 resources

There were no direct links from users to resources (as dictated by ‘best-practice’).

Furthermore:

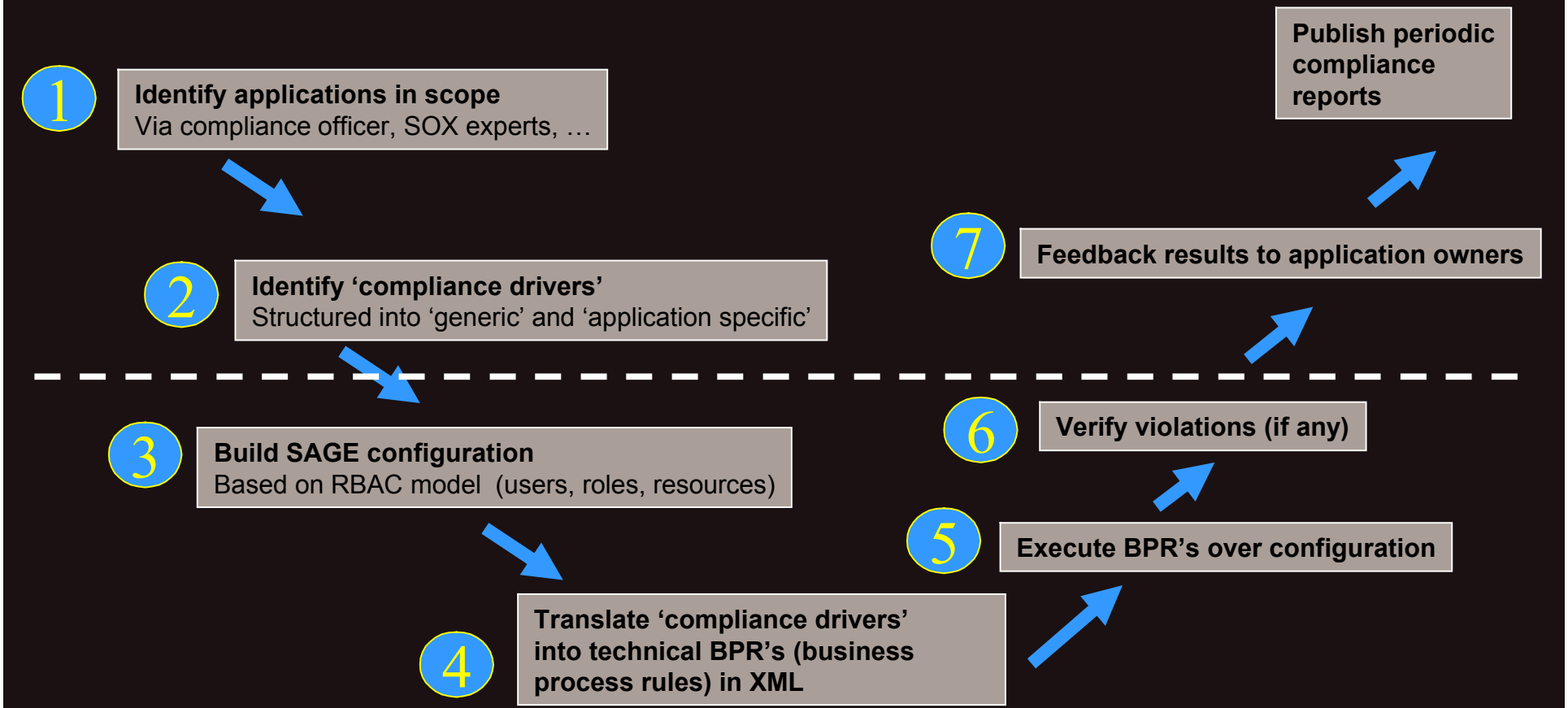
- 5 roles (32 users) have all resources – this is not in line with good practice.
- 22 users had no access to any resources at all – they were only present for historical reasons.
- 251 of 443 roles have no users at all (due to reorganizations – should be cleaned on a short term).
- 74 roles have only 1 user.
- Many sets of roles exist with the same (or almost the same) resources.
- Furthermore, a significant number of users could not be related to the official HR database.

Section six

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Compliance process



Introducing the Sage 'Business Process Rules'

Sage Policy BPR Rule Types

Business Constraints – SOD - License

Type 1 - Business Constraints Types

- Role-Role – a restriction on the users in two sets of roles
- Role-Resource – a restriction between the users in a set of roles and a set of resources
- Resource-Resource – a restriction on the users in two sets of resources
- User Attribute – Role – a restriction between users with a certain attribute value and a set of roles
- User Attribute – Resource – a restriction between users with a certain attribute value and a set of resources

Restrictions

- Forbidden – Users in left side are not allowed to be on right side
- Must be – Users in left side must also be on right side
- Only allowed – Users in left side are only allowed to roles/resources on right side
- May be – Only users in left side (and not others) are allowed to roles/resources on right side

Compliance

Sage 'Business Process Rules'

Sage Policy BPR Rule Types

Business Constraints – SOD - License

Type 2 - Segregation of Duty Types

- Segregation of Duty Roles – Users are restricted in how many of the roles on the left they can have
- Segregation of Duty Resources – Users are restricted in many of the resources on the left they can have
- In each of these, you must have a NUMBER on the right side

Restrictions

- No more than – Users cannot have more than NUMBER of roles/resources on the left
- No less than – Users cannot have less than NUMBER of roles/resources on the left
- Exactly – Users must have exactly the NUMBER of roles/resources on the left

More types exist…

Identifying the PICASSO compliance drivers

We identified:

1. The existing authorisations matrix, manually maintained in Excel;
2. Restriction of a particular resource (PICASSO function) to specific employee classes - access to function F5909 restricted to billing employees (role R-HSE-BLL) and TNU analysts (role R-BPX089);
3. Restriction of a particular function combination to a specific employee class - access to the combination of functions F5909-F5326 restricted to billing employees (role R-HSE-BLL);
4. Users belonging to the ‘retail’ organisational unit may only have ‘read’ access.

Illustration

The second compliance driver (access to function F5909 is restricted to billing employees (role R-HSE-BLL) and TNU analysts (role R-BPX089) is expressed as the following BPR-rule:

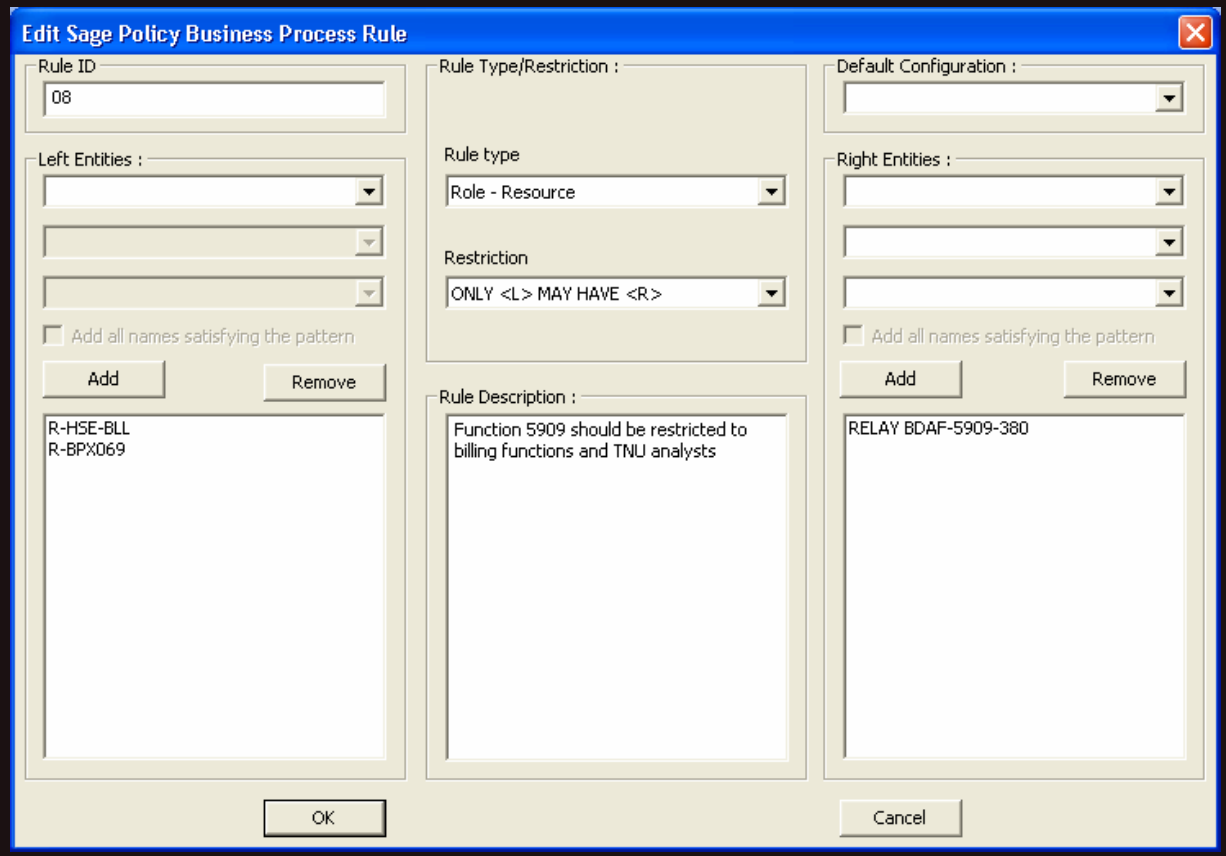
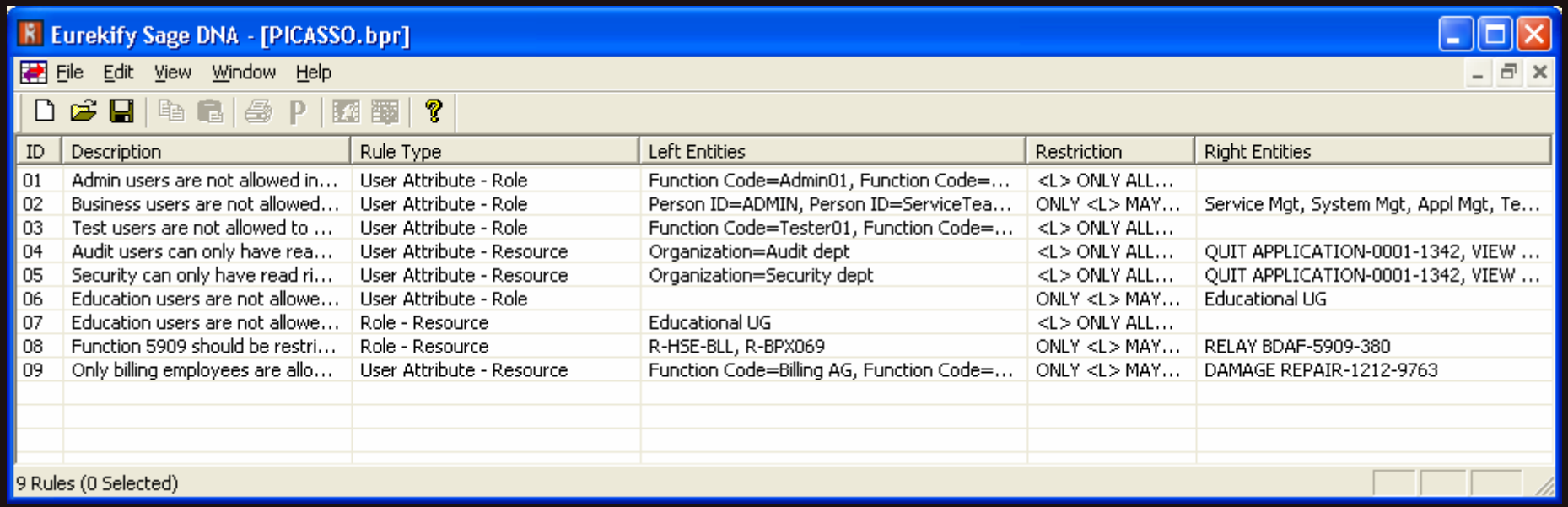


Illustration of a full policy

Here is an example of a full policy for application PICASSO



ID	Description	Rule Type	Left Entities	Restriction	Right Entities
01	Admin users are not allowed in...	User Attribute - Role	Function Code=Admin01, Function Code=...	<L> ONLY ALL...	
02	Business users are not allowed...	User Attribute - Role	Person ID=ADMIN, Person ID=ServiceTea...	ONLY <L> MAY...	Service Mgt, System Mgt, Appl Mgt, Te...
03	Test users are not allowed to ...	User Attribute - Role	Function Code=Tester01, Function Code=...	<L> ONLY ALL...	
04	Audit users can only have rea...	User Attribute - Resource	Organization=Audit dept	<L> ONLY ALL...	QUIT APPLICATION-0001-1342, VIEW ...
05	Security can only have read ri...	User Attribute - Resource	Organization=Security dept	<L> ONLY ALL...	QUIT APPLICATION-0001-1342, VIEW ...
06	Education users are not allowe...	User Attribute - Role		ONLY <L> MAY...	Educational UG
07	Education users are not allowe...	Role - Resource	Educational UG	<L> ONLY ALL...	
08	Function 5909 should be restri...	Role - Resource	R-HSE-BLL, R-BPX069	ONLY <L> MAY...	RELAY BDAF-5909-380
09	Only billing employees are allo...	User Attribute - Resource	Function Code=Billing AG, Function Code=...	ONLY <L> MAY...	DAMAGE REPAIR-1212-9763

Outcome

Completed 48 applications in 4 months

- Created 80 policies with 10-15 business process rules per policy
- Client is currently cleaning violations and mismatches
- Client will automate periodical re-verification

Base report:

- ‘Sage Configuration Preparation’ – the technical details
- interfacing
- data mapping
- translation of CD’s into BPR’s
- actual configuration creation and safeguarding

Periodic reports:

- ‘Sage Configuration and Compliance’
- containing overview tables on number of BPR’s executed, resulting violations, classified according to regulation

Policy Verification Report

10/17/2006 12:06:47 PM

Config: PICASSO1	AuditCard: PICASSO1Audit1
Policy: PICASSO-BPR	

Rule Name	12_4_30
Description	No user is allowed to have more authorisations than his function or task needs. (Mdw KLIC)
Rule Type	BPR Role-Resource <L> Only Allowed to Have <R>

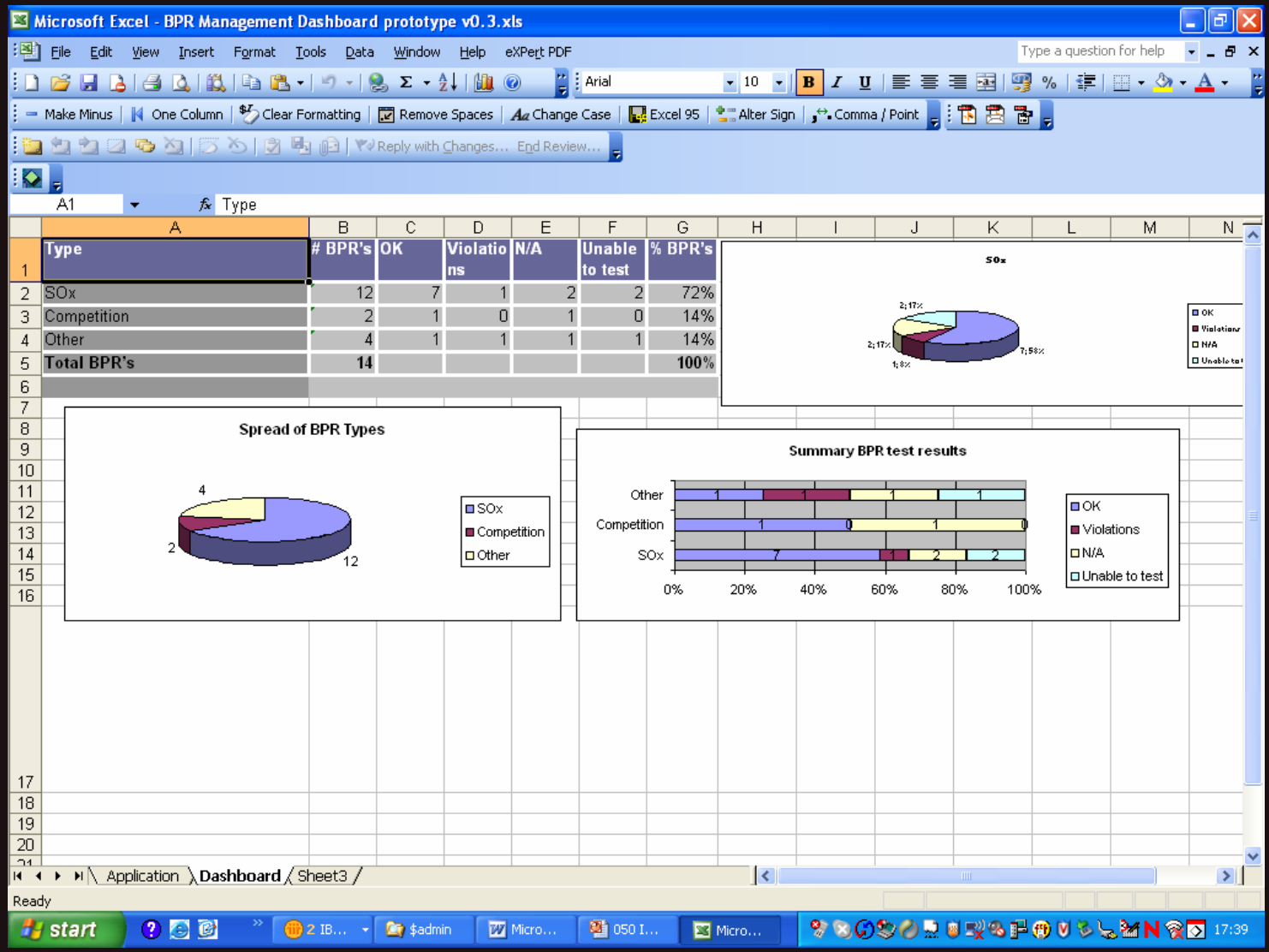
Left Entities		
L-FTTI01		

Right Entities		
5807	OVERZICHT LIGGINGSGEG. PER IK-KABEL	0170
5808	OVERZICHT ADRESGEGEVENS	0171
6999	VERLATEN SYSTEEM	0038

Violations

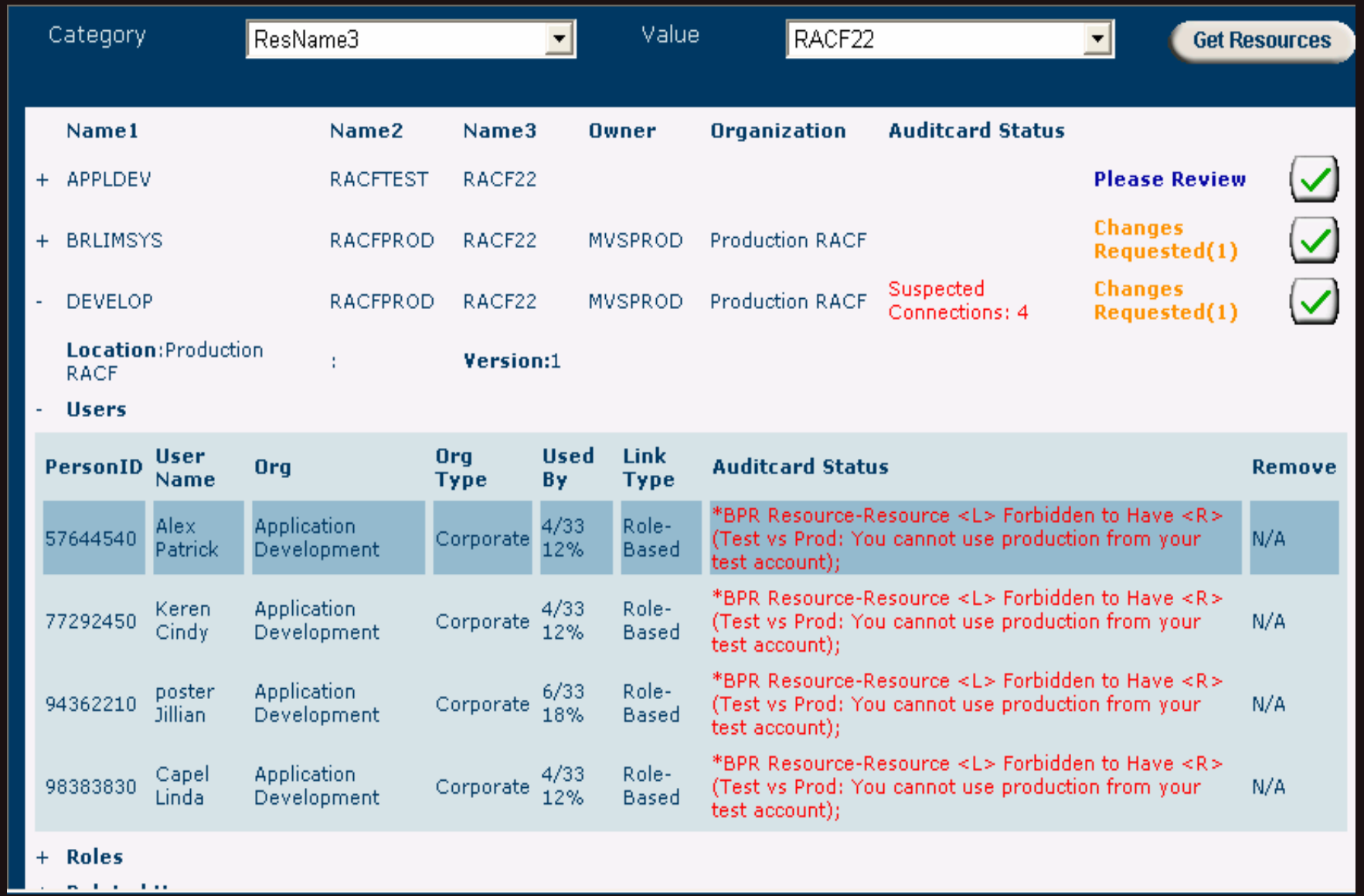
First Entity	Second Entity	Third Entity	Scr.	Status	Date
James T Borg (FRANK016)	L-ALA888-C	4801,SCHAKELEN ENKELVOUDIG,0249	0	Suspected	10/17/2006
Abigail U Maximilian (JONG007)	L-ALA888-C	4801,SCHAKELEN ENKELVOUDIG,0249	0	Suspected	10/17/2006
Ed Q Black (TIJSS009)	L-ALA888-C	4801,SCHAKELEN ENKELVOUDIG,0249	0	Suspected	10/17/2006

Dashboard



Type	# BPR's	OK	Violations	N/A	Unable to test	% BPR's
SOx	12	7	1	2	2	72%
Competition	2	1	0	1	0	14%
Other	4	1	1	1	1	14%
Total BPR's	**14**					**100%**

Compliance
Next: Periodical Review of Violations and Recertification of Privileges



Section seven

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Conclusion

- Technology
- Pilot
- Implementation project
- Lessons learnt
- Way forward

Section eight

Introduction
Objectives of this presentation
Setting the scene
Unification and control libraries
Role-mining
Compliance
Conclusion

Further references

Further references

- www.pwc.com/security
- www.eurekify.com
- users.skynet.be/marc.sel

PRICEWATERHOUSECOOPERS