



IT ADVISORY

Access Governance

A cost effective and integrated approach

17 November 2010 – ISACA Roundtable

ADVISORY



AUDIT ■ TAX ■ ADVISORY

Today's Agenda

- A. Setting the scene
 - Relationship with Identity & Access Management
 - Key controls

- B. Access Governance defined
 - Definition / Concept
 - Heterogeneous approach

- C. Use in financial audits
 - Background
 - Main steps & results

- D. Access Governance case study

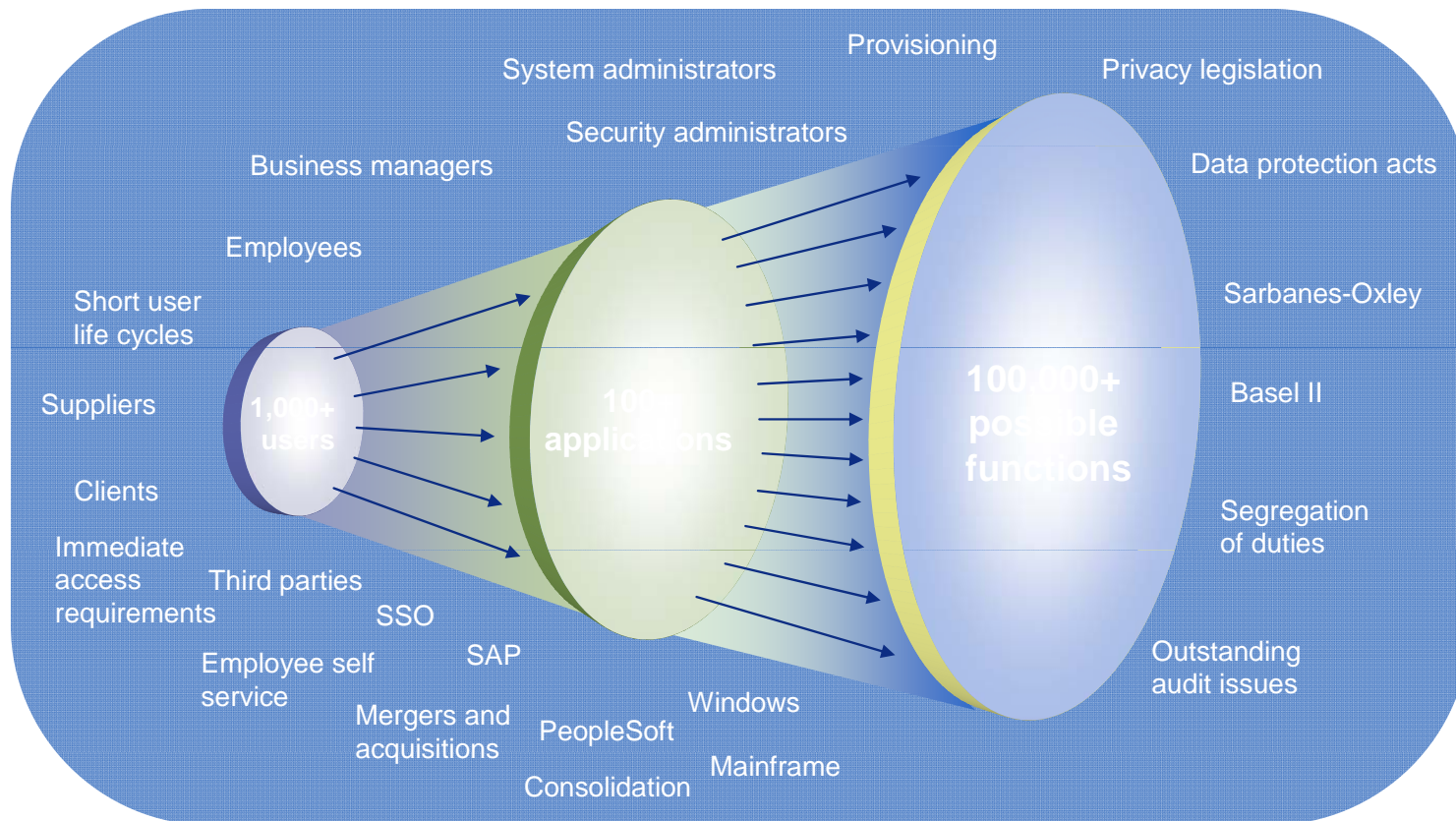
- E. Conclusion & Questions



Part A: Setting the scene



A Typical Business Access Management Environment Today...



How do you manage and control who has access to what in an efficient and effective way?

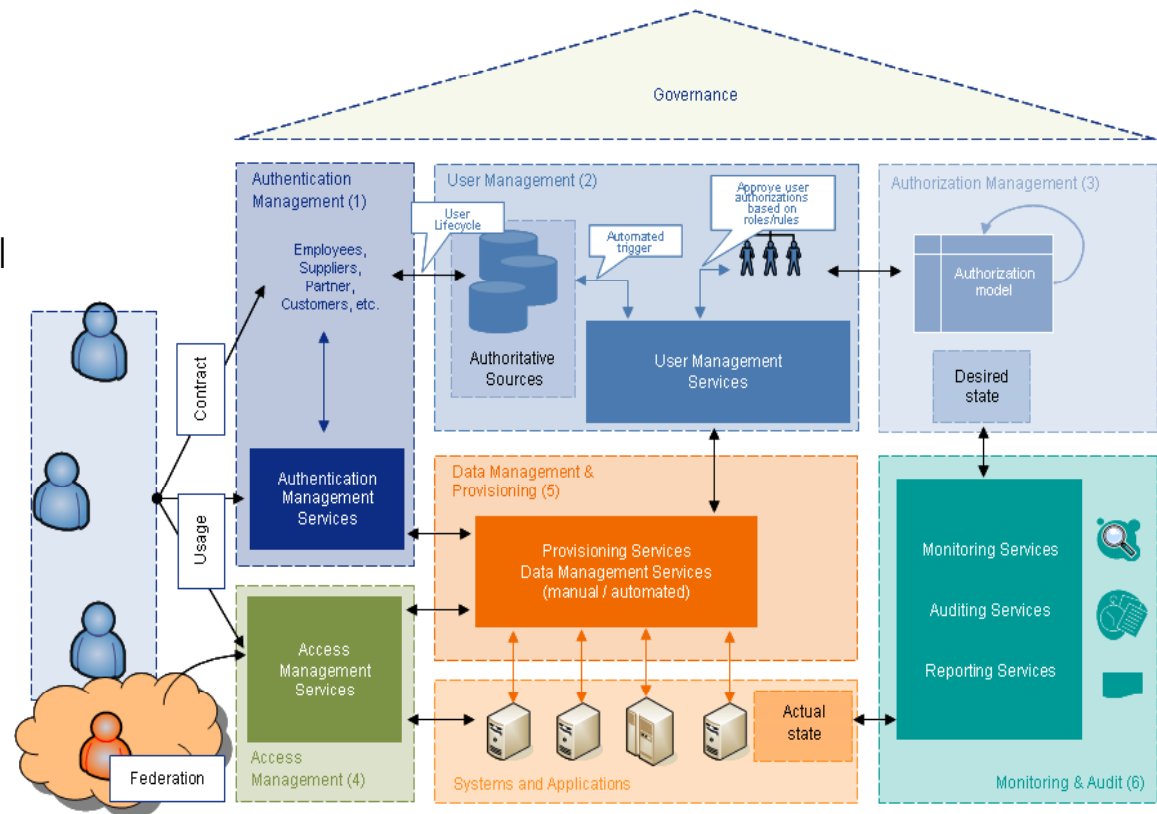
Identity & Access Management – the answer to this problem ?

Identity & Access Management:

“The **policies, processes and systems** for **efficiently** and **effectively** governing and managing who has access to which resources within an organisation”

Optimised processes for:

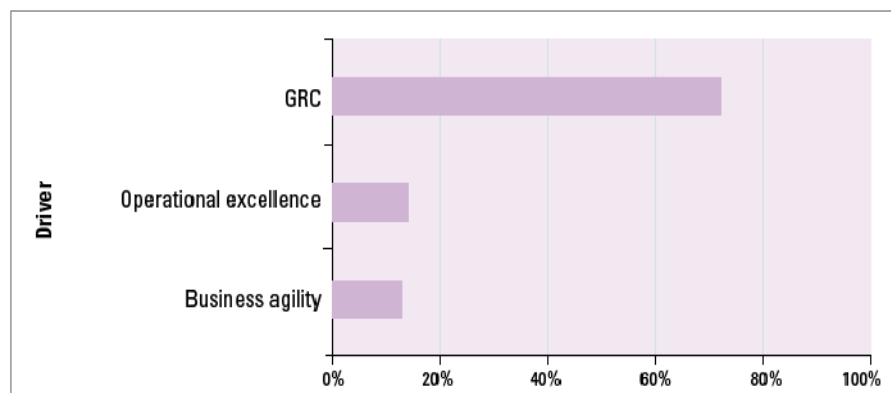
- Managing identities
- Managing access requests
- Managing authorisation model (such as role based access)
- Improving IT-fulfilment by automatic provisioning
- Improving monitoring & reporting capabilities



Identity & Access Management – the answer to this problem?

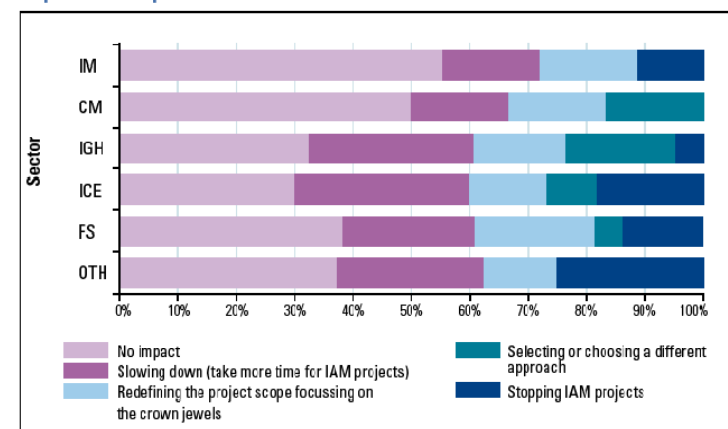
- full blown IAM can be too complex in current economic climate

- Identity & Access Management (IAM) as a whole is still the envisioned end-state to improve IAM on the following aspects:
 - Governance, Risk and Compliance (GRC)
 - Operational excellence
 - Business agility
- However, full blown IAM is still complex and realising the benefits requires significant investments, including a long term program with various projects
- Due to the current economic climate organisations are more focussed on Governance, Risk and Compliance (72% according to our recent European IAM Survey) and put less emphasize on operational excellence and business agility



Source: KPMG/Everett IAM survey, October 2009

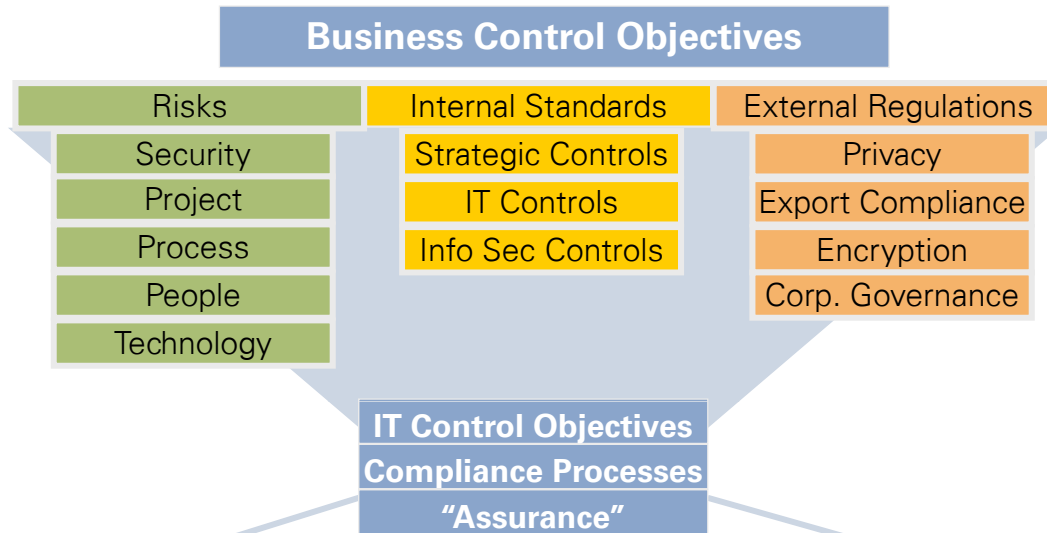
Impact on scope



Source: KPMG/Everett IAM survey, October 2009

What is required ?

- Identity and Access Management Key Controls



Identity & Access Management Key Controls

logical and physical access to IT computing resources is appropriately restricted to reduce the risk of unauthorized / inappropriate access to the organization's relevant applications or data

procedures are established so that user accounts are managed in a timely manner to reduce the risk of unauthorized / inappropriate access to the organization's relevant applications or data

controls are in place to ensure that authorizations or access rights are assigned in accordance with the responsibilities of the various roles or profiles to help reduce the risk of unauthorized/inappropriate access to the relevant applications or data

controls are in place to ensure that appropriate segregation of duties within key processes exist and are followed

an effective control process is in place to periodically review the appropriateness of access rights, including appropriate segregation of duties in order to reduce the risk of unauthorized / inappropriate access to the organization's relevant applications or data

controls are in place to restrict super user access to an appropriate group of individuals and to monitor the activities performed by those users to reduce the risk of unauthorized/inappropriate access to the relevant applications or data.

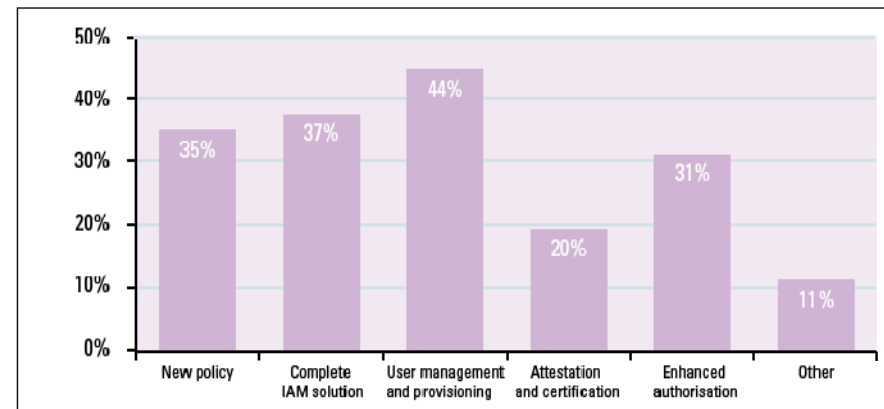
Change in dealing with the IAM problem

- moving from Provisioning projects to Access Governance projects

- In stead of improving efficiency of IAM before improving effectiveness, we see a change towards improving the effectiveness of IAM before improving efficiency
 - In stead of focus on provisioning, we see more focus on reporting, attestation and certification of access rights

(Access Governance)

Means to achieve project goals



Source: KPMG/Everett IAM survey, October 2009

- Observations
 - Provisioning projects did not deliver (timely) the expected results regarding being in control
 - Provisioning projects do not follow the priorities of being in control as set by the business (platform versus applications)



Part B: Access Governance defined



Access Governance

- defined

Access Governance is a **process to review user access** to and within applications on a frequent basis to achieve regulatory compliance and improved security.

Access Governance includes:

- attestation (verification / validation) of user access
- certification of user access

by appropriate stakeholders in a manual or (partly) automated manner

related to one or more applications -> review can go beyond platform and application domains

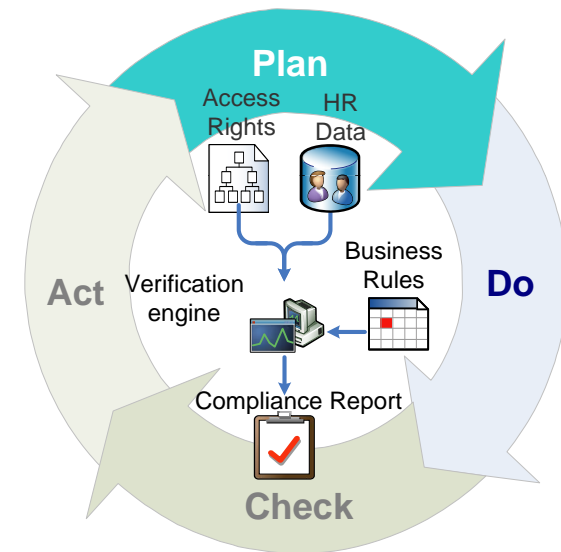


Access Governance

– the basic concept using analytics tools

Basic concept:

1. Determine key data, applications and systems that require attestation and certification based on risk assessment
2. Create or update business rules and authorisation matrix between HR attributes and authorisations of databases, applications and/or systems
3. Use analytics tools to import and enrich authorisations with HR data – create data warehouse
4. Use tools to analyse authorisation data and to generate a compliance report of authorisations violating the business rules
5. Discuss violations with business owners / certification by business
6. Remove excessive authorisations
7. Use tooling to determine application profiles to improve the access request process – preventive control



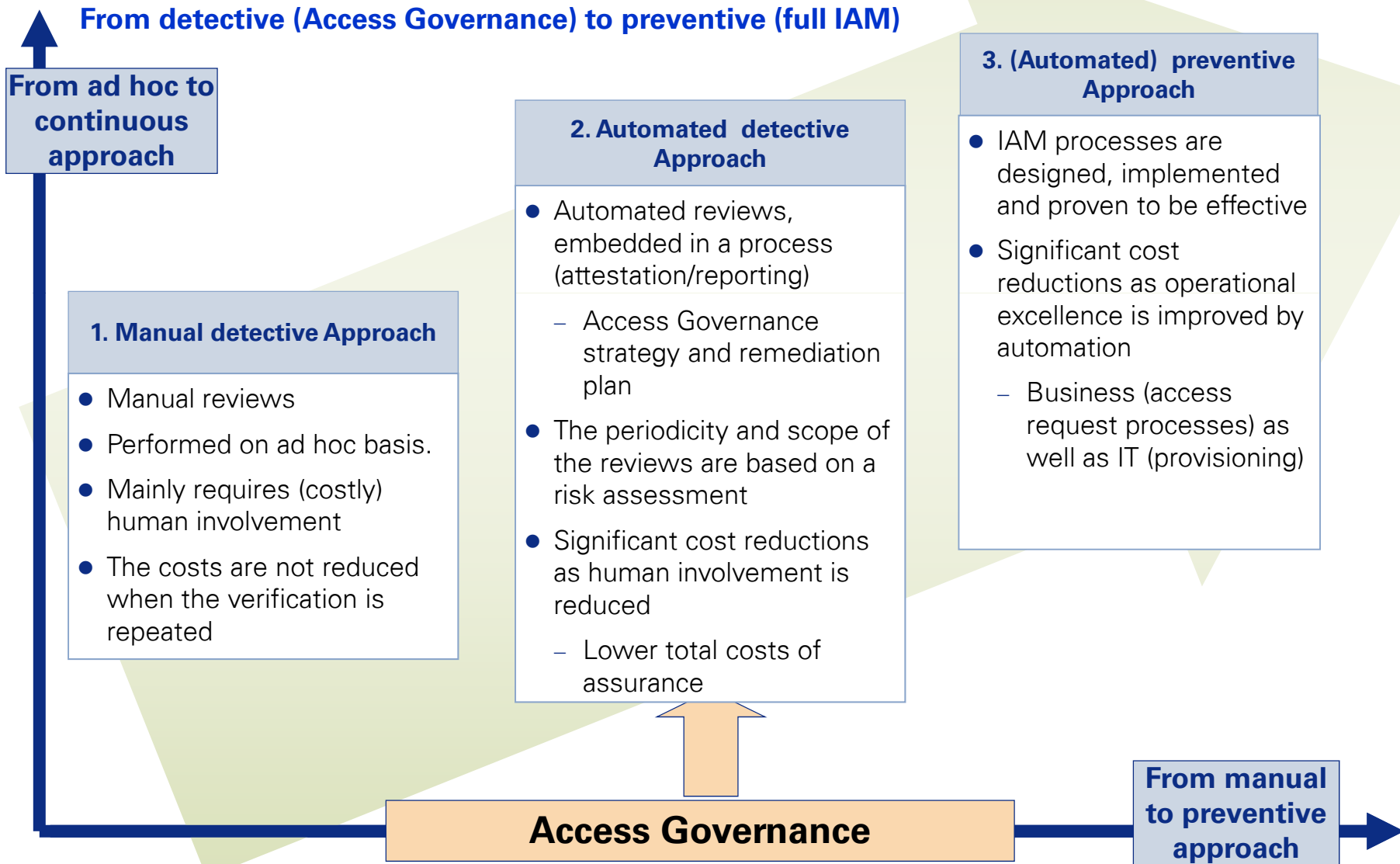
Access Governance

- heterogeneous approach

- Access Governance focuses on the heterogeneous application landscape of your organisation
 - For the common ERP platforms specific analysis tools are in place (such as Approva), using predefined rules
 - For all other platforms without specific tools the Access Governance approach can be used
 - SoD-checking can be done beyond the boundaries of platforms or application (cross-checking) and master/slave validation is also possible
- As Access Governance is focussing on heterogeneous applications there is not one set of applicable business rules
 - For every application new rules have to be defined, rule definition is thus more intensive
 - However, processes can be the same and thus also the basis for the rules – generic accounting rules can be translated to every organisation

Access Governance

- a necessary step towards full IAM





Part C: Use in financial audits



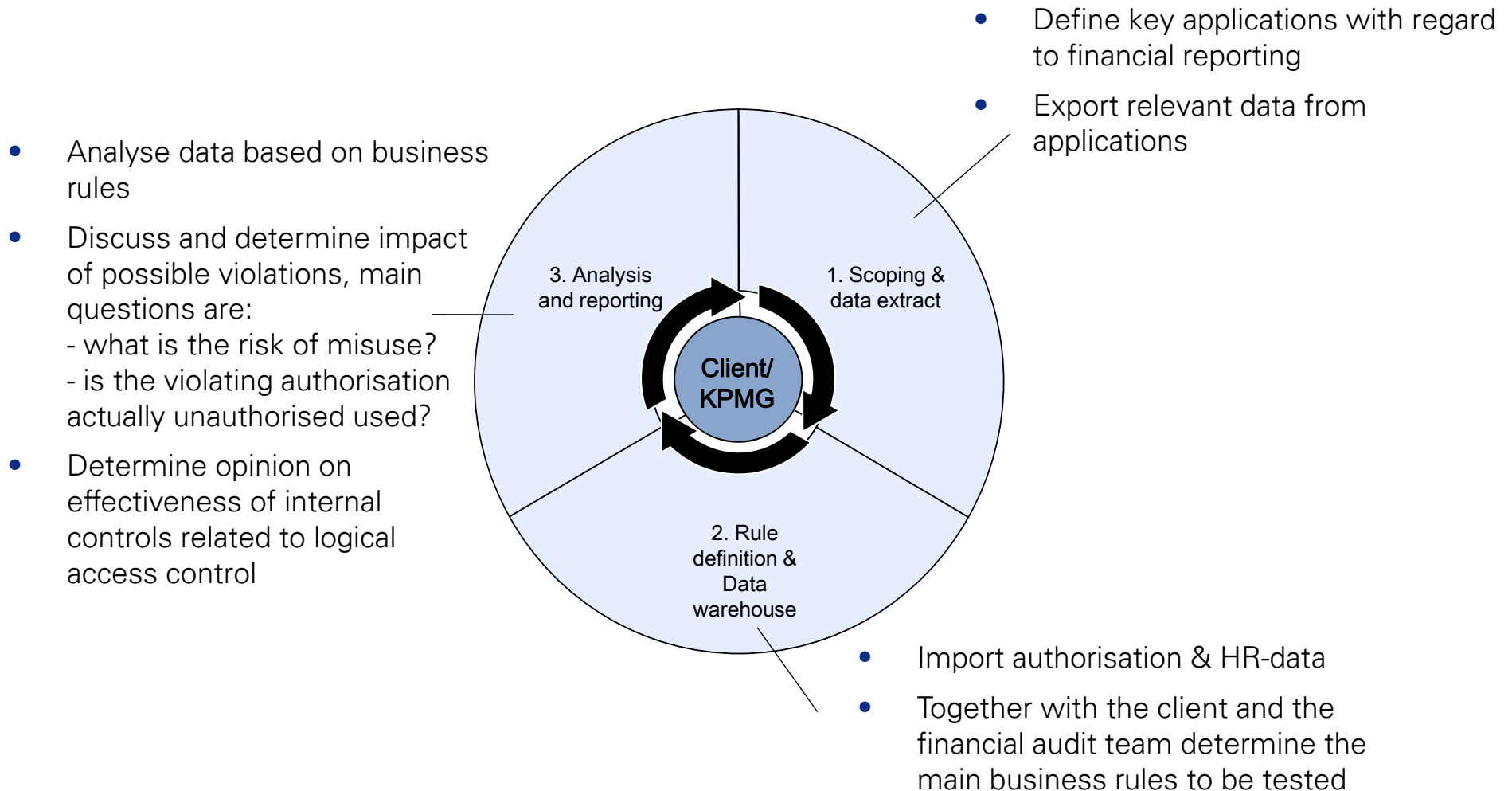
Access Governance in the financial audit

- background

- Access controls are one of the key control mechanisms in place to protect sensitive (financial) information
- Regulations around access governance are getting stricter and auditors need to obtain proof that access controls are operating effectively
- Traditionally, testing of the effectiveness of access controls (for example as part of financial and internal audits) was laborious and time consuming
- Access Governance can help the financial auditor in analysing the key access controls of the applications and systems with an impact on the financial reporting
 - Less time consuming
 - In-depth analysis in stead of sample testing
 - Input for the opinion if the internal control objectives are met with regard to logical access control

Access Governance

- main activities for use in the financial audit



Access Governance in the financial audit

– overview business rules

- ☑ All accounts must be traceable to an individual
- ☑ No user should have all authorizations
- ☑ Each active user must have at least a single authorization
- ☑ Each authorization must be linked to at least a single user
- ☑ Test accounts are not allowed in the production environment
- ☑ Only members of OU Accountancy are allowed to have access to the GL application
- ☑ Only members of OU Procurement are allowed to have access to the Purchasing application
- ☑ Only users of OU Accountancy are allowed to create a GL account
- ☑ Each role must have at least a single user and at least a single permission
- ☑ Each account must be linked to a natural person (with first and last name)

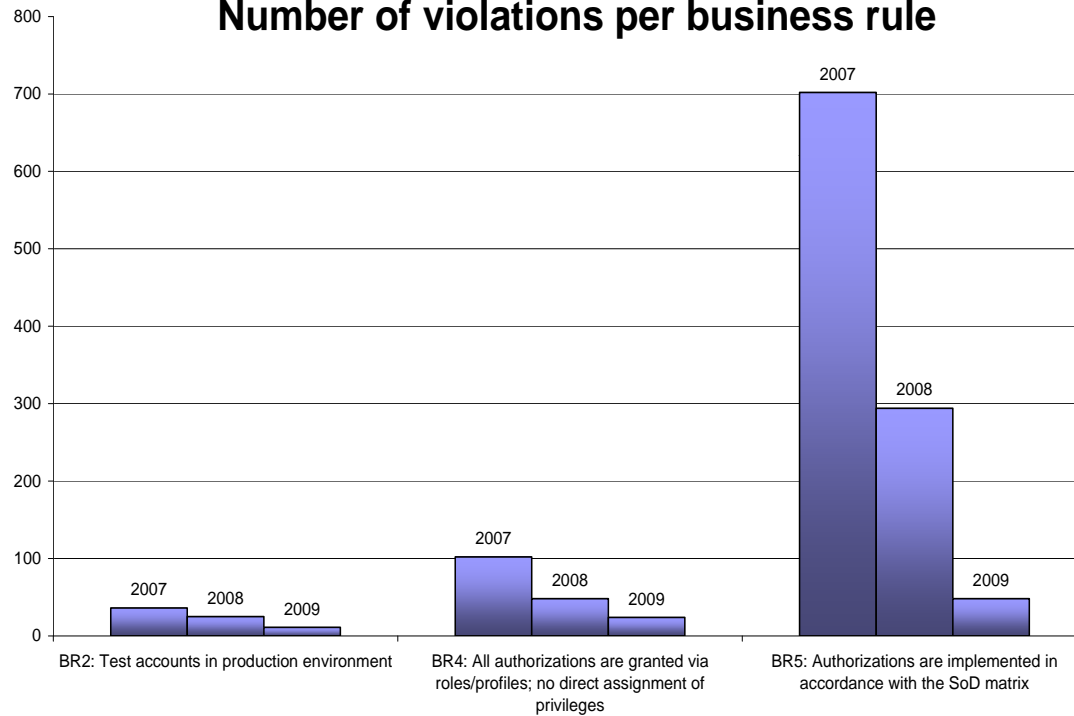


Rules can be categorized:

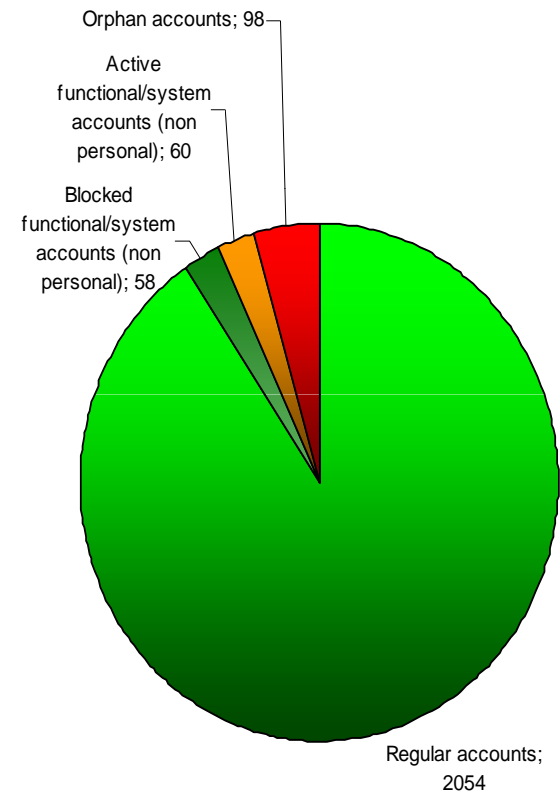
- ◆ Accounts
- ◆ Users
- ◆ Permissions
- ◆ Organisation Units
- ◆ Applications
- ◆ Roles

Some reporting screenshots

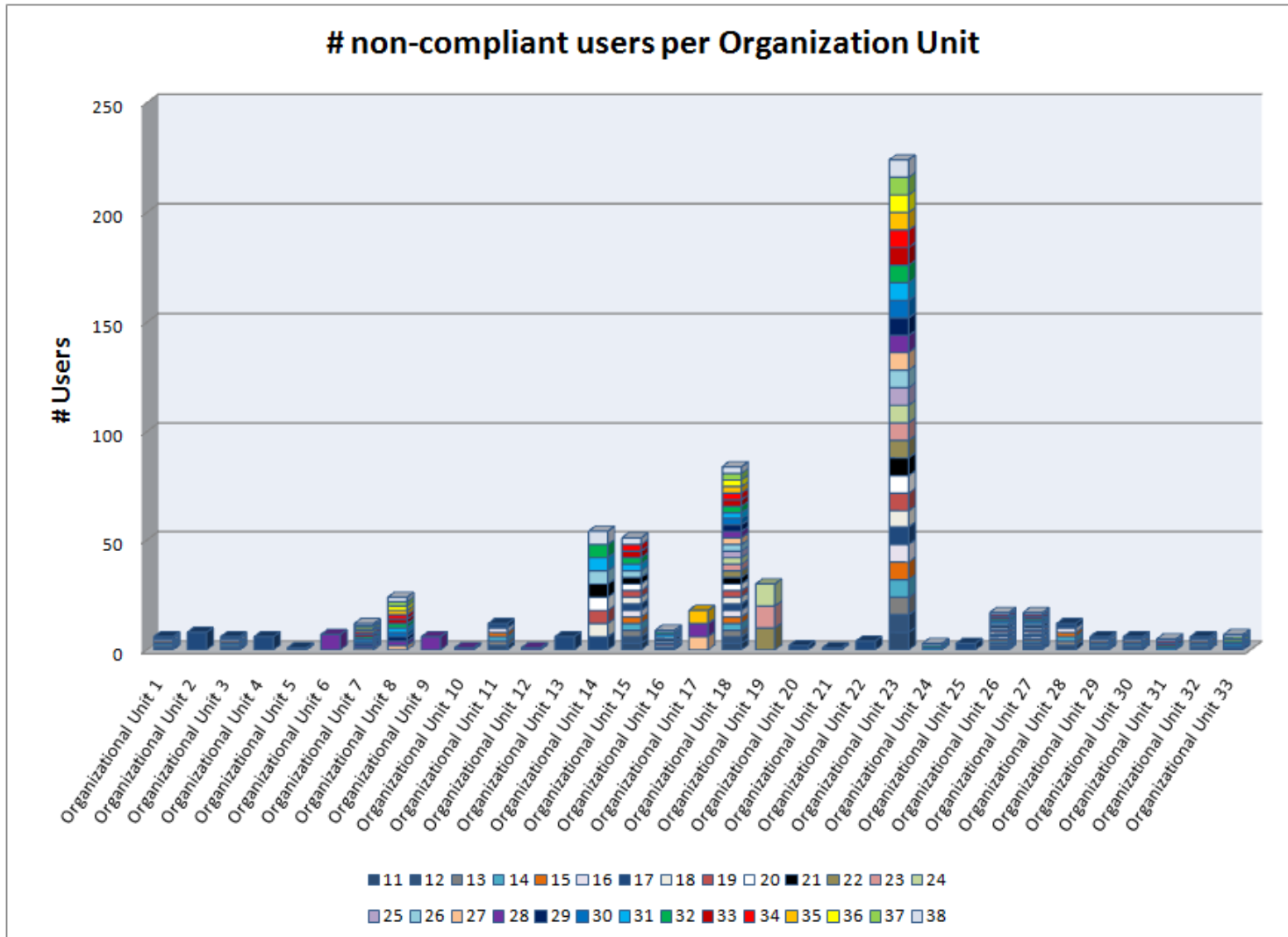
Number of violations per business rule




Overview of accounts 2009



Some reporting screenshots



Specific finding related to business rule

ABR_06	Users who have no access to the core banking system, are not allowed to have access to the share were input-files are stored
Additional used information	List of users who are explicitly allowed to access the input-share
<p data-bbox="163 529 296 561">Findings</p> <div data-bbox="176 651 617 794" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p data-bbox="180 659 569 786">Bank risk: unauthorised payments could have been injected</p> </div>	<p data-bbox="667 529 1885 594">50 accounts have access (read/write) to the input-share while not having access to the core banking system.</p> <p data-bbox="667 643 1163 675">Mitigation action is already initiated</p> <div data-bbox="674 737 1108 1019" style="background-color: #800000; color: white; padding: 10px; margin-top: 10px;"> <p data-bbox="678 748 1104 1008">Action: Analyse log-files which people have created or changed input-files while not having access to the banking system</p> </div> <div data-bbox="1766 1203 1913 1325" style="text-align: right; margin-top: 20px;">  <p data-bbox="1766 1276 1913 1325">Adobe Acrobat Document</p> </div> <p data-bbox="1457 1341 1856 1406" style="text-align: right; margin-top: 10px;">Link to pdf with overview of violating accounts</p>



Part D: Access Governance case study



Case study

- Project definition

Financial institution

- Around 3000 employees
- 30+ applications need to be analysed

Objectives:

1. Unequivocal and clear (non-technical) request methodology

- To minimize the space for errors in carrying out authorisation requests
- To accelerate and improve the efficiency of the way authorisation requests are carried out

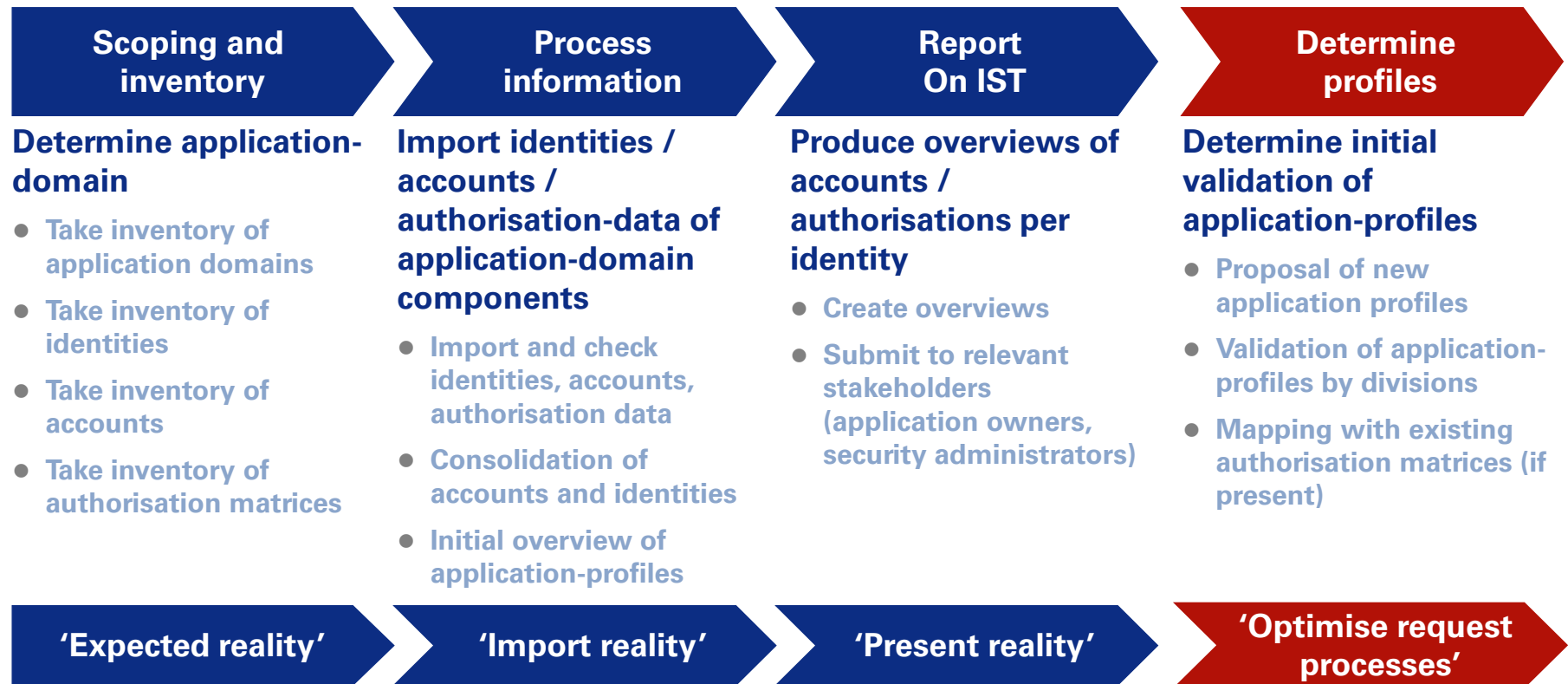
2. Comply with (increasing) laws and regulations (“In Control Statement” / SAS 70)

By means of:

- Creating a central entitlement administration
- Improving the authorisation management processes
- Enabling reporting on authorisation management for compliancy purposes

Case study

– Overall phasing



Case study

– End result

- 30 Applications were analysed in a time frame of 3 months, using automated analytics tools
- Reports were used for cleansing activities as well as attestation / certification purposes
- Key learning points:
 - It is not about the tool, but about the process
 - Tools will ease the data import / analysis of user access data
 - Get your foundation in place
 - Overview of stakeholders per application – who do you need to involved
 - How to get this concept operationally?
 - Flat files are cumbersome, so you need to have some mechanism in place (drop box / automation)
 - Communication is key !



Part E: Conclusion & Questions



Conclusion

- Access Governance facilitates a focused **detective approach** with relatively limited budget expense
 - After initiating the project the results are directly available; direct link between investment and results
- Access Governance can be **customised** for every organisation
 - The frequency and scope of access attestation and certification may vary, depending on the risk controls and regulatory requirements
 - Organisations should find a balance between delta certification and full certification cycles
- Access Governance tooling is more mature than a few years ago and can **speed up the process** and **reduce manual effort**
 - Tools encompasses also functionalities for preventive controls, e.g. use the access control rules for handling access requests
 - Clear advantage compared to home grown solutions

More information?



KPMG IT advisory

Benny Bogaerts
Senior Manager

Prins Boudewijnlaan 24-D
2550 Kontich, Belgium
Phone +32(0)3 821 18 93
E-mail: bbogaerts@kpmg.com
Internet: www.kpmg.be

The information contained in this document is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

