KPMG

How PAM projects evolve from regulatory requirements
II
How SoD is handled within SAP

Dominic Stommen

Agenda

1. Greeting
2. Introduction
3. View in the future
4. Conclusion
5. Discussion

Regulatory Requirements evolve from BAIT and VAIT

Bankaufsichtliche Anforderungen an die IT (BAIT)

The "Banking Supervision Requirements for IT" (BAIT), which primarily address the management of Credit institutions, states that the expectations of the supervisory authority with regard to IT security should be presented more transparently. The requirements of the MaRisk in the context of IAM are specified in Chapter 5 "User authorization management" of the BAIT.

Key Points Chapter 5 BAIT

- User access rights concepts define the scope and the conditions of use for access rights to IT systems in a manner that is consistently in line with the determined protection requirements and can be completely and comprehensibly deduced for all access rights for an IT system. User access rights concepts shall ensure that users are assigned access rights according to the need-to-know principle, that the segregation of duties is observed and that staff conflicts of interest are avoided. (BAIT part 5, number 24)
- It must be possible for non-personalised access rights to be unequivocally traced back to an active person at all times (wherever possible, automatically). Any departures from this in justifiable exceptional cases and the resultant risks shall be approved and documented. (BAIT part 5, number 25)
- The institution shall set up logging and monitoring processes consistent with the protection requirements and the target requirements that enable checks to be carried out to ensure that access rights are used only in the manner intended. (BAIT part 5, number 29)
- Accompanying technical and organisational measures shall be implemented to ensure that the requirements contained in the user access rights concepts cannot be circumvented.

What does a PAM project in a nutshell look like?

Example for a common PAM project

1 Design

—Design your IAM and PAM governance
—Design your PAM processes

2 Define

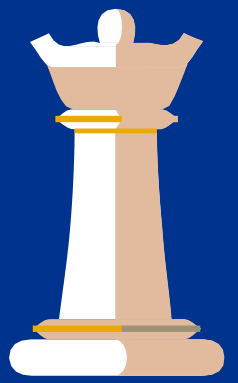
—Define requirements, your PAM-tool needs to fulfil

3 Execute

— Select a tool & implement PAM-tool and processes with a PAM project

PAM-tool requirements can vary depending on the sector in which a company operates. The main requirements that need to be defined are functional, non-functional, legal and regulatory specifications.

- Think first, buy a PAM-tool later



What are the key constraints?

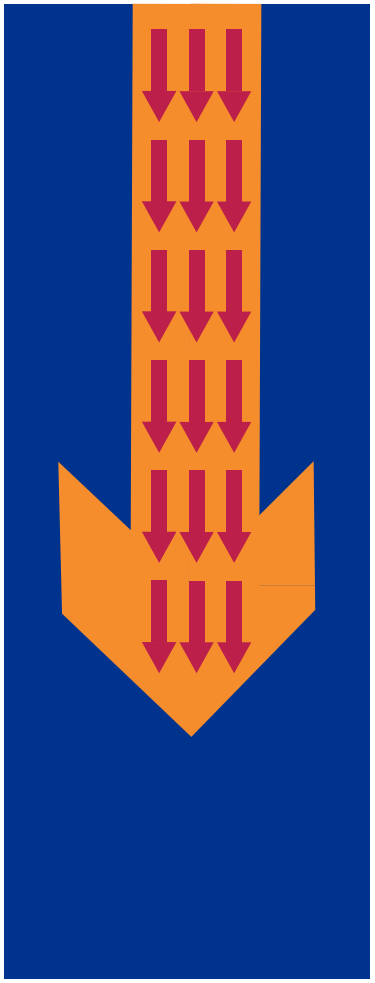
Common pitfalls in a PAM project

—Incomplete data basis
  — Usually due to lack of a CMDB

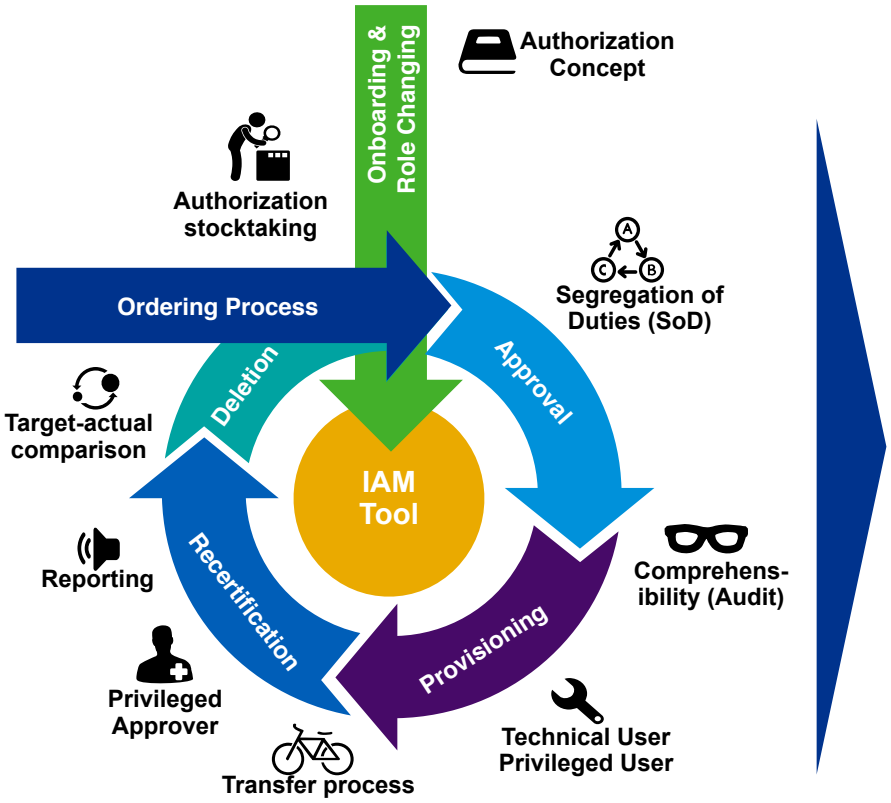
— Definitions not in place or unclear
  — What is a privileged account
  — What is a privileged user

— Complex or outdated IT architecture
  — Challenge for integration of PAM-tool

— Insufficient communication within the company
  — Relevant employees, e.g. admins, don’t receive sufficient information regarding change in log-in process



We’ve developed an IAM-Lifecycle to address client’s needs



Schematic representation of the work packages (AP)

1 Maturity Level Assessment
- Determination of the actual-situation
- Reflection against KPMG maturity model for IAM
- Result report and proposal of further steps for department

2 IAM Conception
- Definition of IAM governance guidelines
- Development of target-processes
- Definition of measures list
- Creation of a target architecture concept

3 Implementing IAM
- Determination of the actual-situation
- Reflection against KPMG maturity model for IAM
- Result report and proposal of further steps for department

4 Authorization Concepts
- Run a Gap-analysis of the authorization concepts
- Creation of a regulatory compliant template for authorization concepts
- Adjustment of existing authorization concepts

5 Authorization Refurbishment
- Analysis of the systems with clean up needs
- SAP systems clean up using our KPMG AIM tool
- If necessary, clean up of other systems

6 IAM Organization
- Creation of manuals and training documents
- Support during the filling of the developed positions according to the IAM conception

7 Authorization Concepts
- Planning the rollout of new requirements, processes and controls
- Development of IAM specifications including written, fixed regulations
- Knowledge transfer to the client

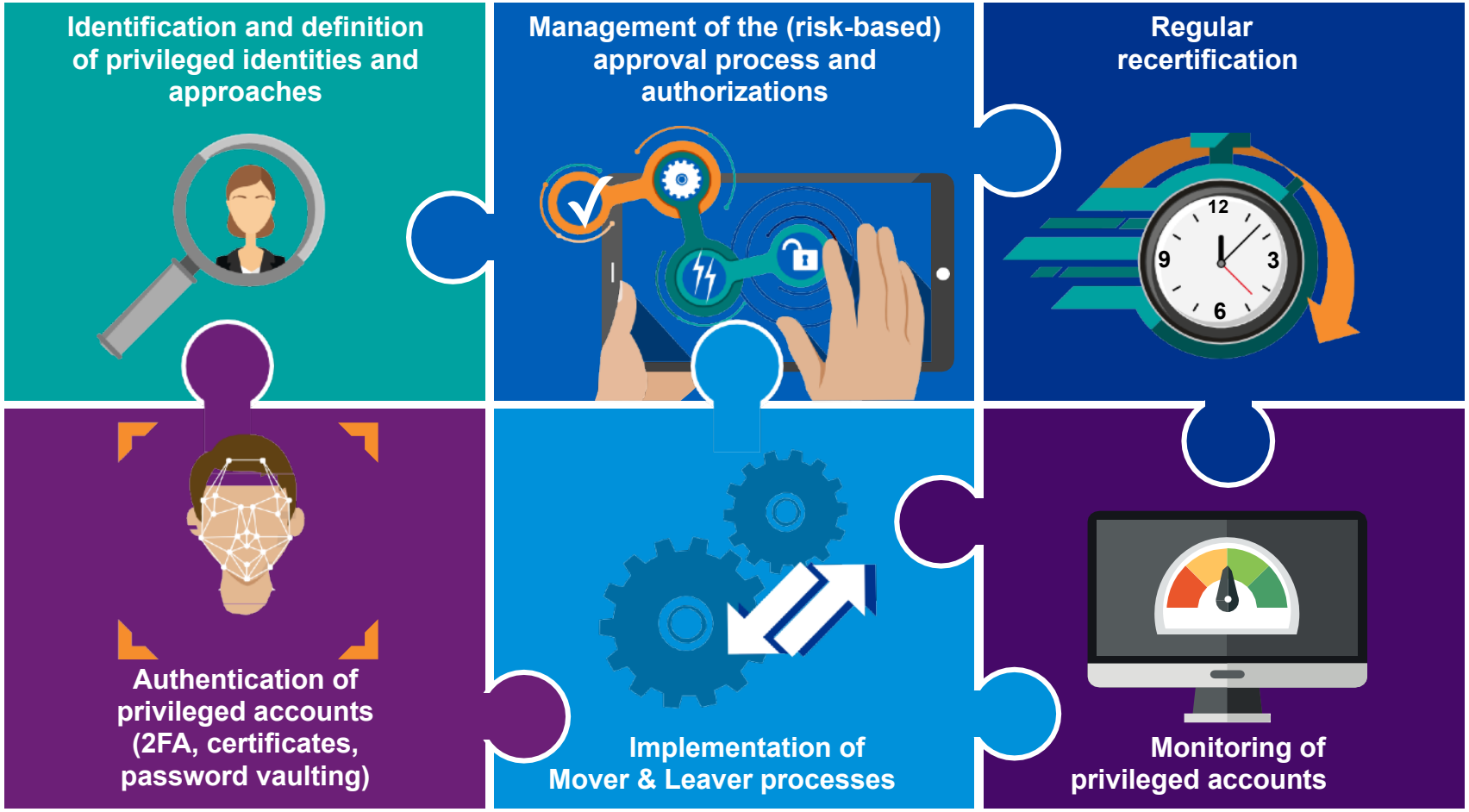
8 Authorization Refurbishment
- Risk oriented analysis of the actual-situation
- If necessary, analysis of the existing pam tools and basic requirements
- Risk oriented analysis of the affected systems

9 IAM Organization
- Recording the actual-situation of the system overview
- Support with construction of interfaces to the IAM tool

Our **KPMG IAM lifecycle** is based on many years of **project experience**. It takes regulatory requirements into account and reflects a **robust IAM overall process flow**.

Based on the **KPMG IAM lifecycle** and **better practice experience** from implementation projects in state banks and banks (national and international), **9 relevant work packages** have been created that represent the overall framework.

Best Practices – Features of a successful PAM framework



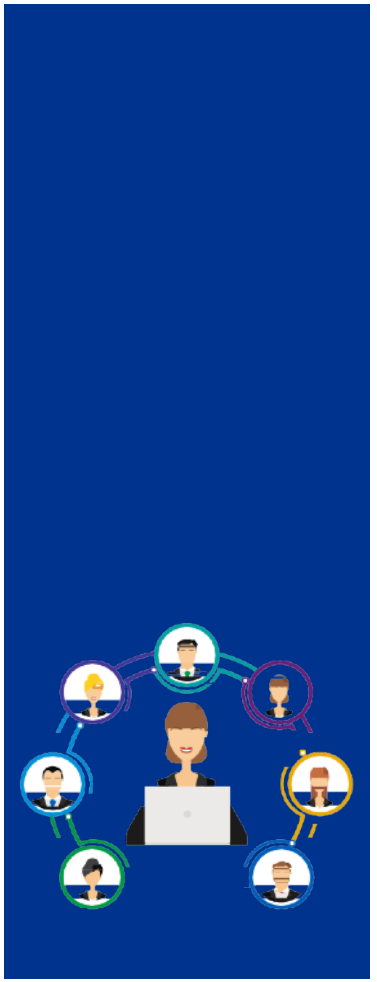
The Do’s and Dont’s

Do’s: ‘Communication is key’

- Communication is key – All stake holders (Departments, HR department, auditors) must be included and informed on time.
- Coordinate and tune guidelines and processes at first.
- Define and assign functions and responsibilities properly and train those affected.
- Create clear distinctions between 1st and 2nd Line of Defense.
- In the project, always pay attention to which elements the later line function will need.
- Introduce business before considering technological options.
- Organize IAM projects from top to bottom - Without management support, the project becomes incredibly difficult to impossible.

Dont’s: How to ruin a PAM project

- Buy a tool without proper planning and coordination.
- Declare IT-department responsible for authorizations management without an adequate knowledge transfer.
- Declare the departments responsible for their permissions without an adequate knowledge transfer.
- Require approvals where there is no transparency.
- Expect everyone affected to have time for the project (especially departments and human resources).
- Assume that delivered data is reliable (high quality).
- Expect intuitive understanding from the end user.



Segregation of Duties

Definition

Segregation of Duties (in short: SoD) describes the organizational and technical separation between functions (organizational units, positions, activities, etc.) in a business process to avoid possible conflicts of interest.

Requirements

— Assigning incompatible authorizations to the same identity is prohibited.

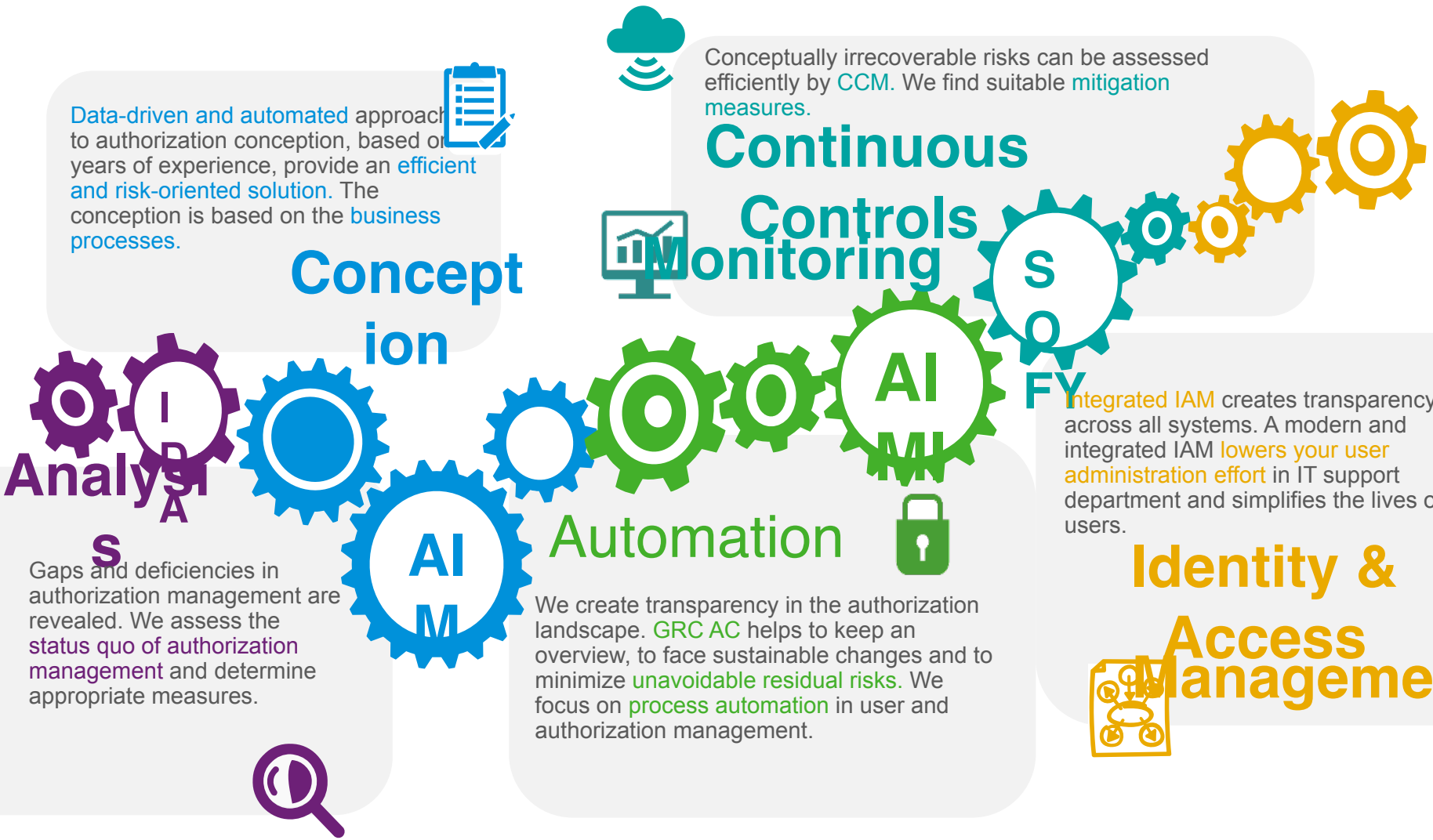
— Incompatible authorizations must not be grouped into one role.

— Users may only receive roles that contain incompatible authorizations with special permission from IT security or the security officer.

— SoD requirements can not only separate functions according to roles, but also according to people or entire organizational units. For example. the front office must be separated from the back office or the reviewer of a document must not be the creator.

— SoD requirements can be specified externally (e.g. MaRisk) or arise from internal specifications. If necessary, they have to be adapted to the specific branch.

Methodology of a SAP SoD Project



Ihre Ansprechpartner

Bastian Becelewski
Senior Manager, Lighthouse
T +49175667-3457
bbecelewski@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
The Squaire am Flughafen
60549 Frankfurt am Main

Linda Noack
Senior Manager, FS CIO Services
T +49 160 9850-4901
lindanoack@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Ludwig-Erhard Straße 11-17
20459 Hamburg

www.kpmg.de/socialmedia

www.kpmg.de