SAP
An Introduction

Agenda

What We Will Do…

- Provide a high level overview of what SAP is
- SAP Authorization Concept
- Provide an introduction to Auditing ITGC's in SAP
- Segregation of Duties in SAP

What is SAP?

What does SAP stand for?

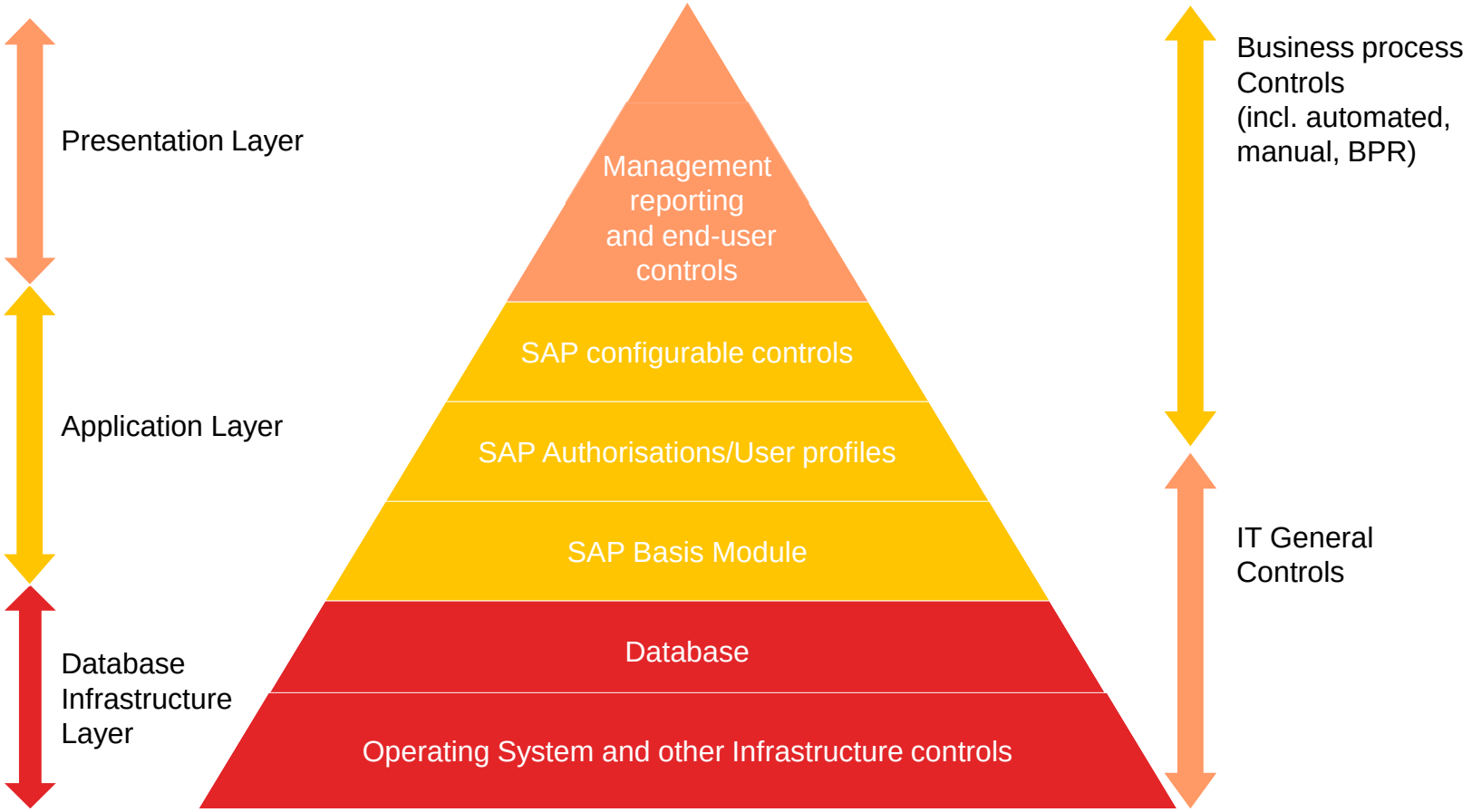
- Systeme, Anwendungen, Produkte in der Datenverarbeitung

Systems,
Applications and
Products in Data Processing

What is SAP?

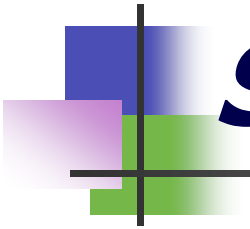
Integrated	SAP integrates all business processing through one application. Links operational results and the financial aspects of those results.
Multifunctional	SAP can track financial results, procurement, sales, manufacturing, human resources and payroll.
Modular	SAP comprises of 18-20 modules in finance, logistics and HR. One or more SAP modules can be implemented.
Enterprise Wide	SAP is typically accessible by the entire business organisation. Most company information and transactions originate from SAP.
“Real Time”	An order in SAP can automatically generate an inventory movement and a posting in the GL without any “human” intervention.

Overview of an SAP Environment



SAP Instances

PR1	SAP R/3 or ECC 6.0
PH1	SAP Human Resources
PC3	SAP Customer Relationship Management
PE1	SAP Procurement
PA1	APO Planning
PS1	Solution Manager
PB1	Business Warehouse



SAP Authorization Concept

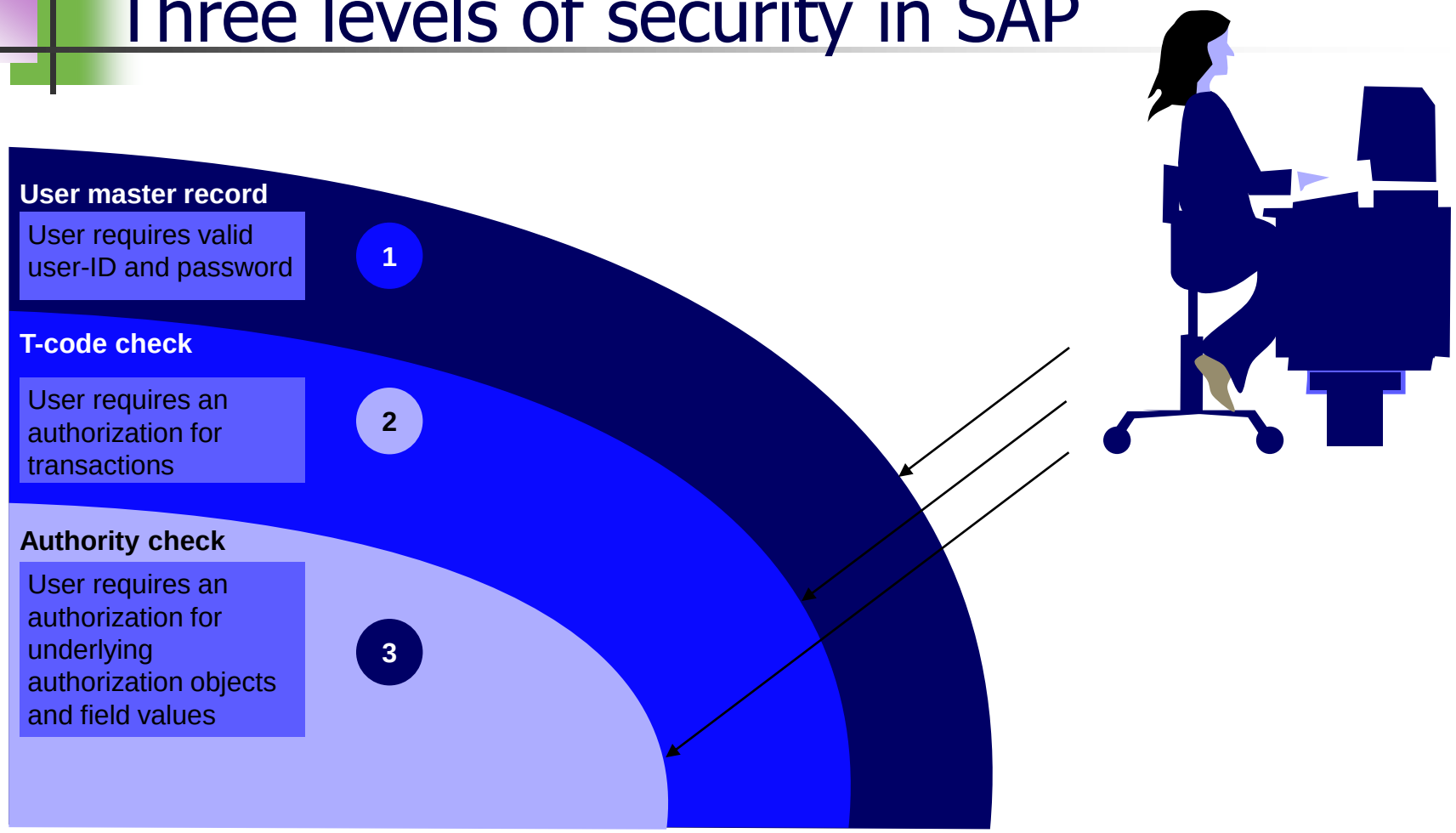
Overview
What is the SAP authorization concept?

Security within SAP is achieved through the authorization concept
The authorization is designed to ensure :

- Maximum security
- Sufficient privileges for end users to fulfil their job duties
- Powerful user maintenance

Overview

Three levels of security in SAP



SAP Authorization Concept

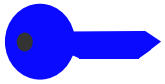
The components

SAP User Master Record (UMR)
Master data for SAP users

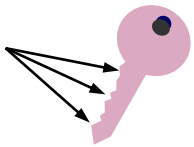
Transaction Code (t-code)
Provides access to specific functions within SAP

ME21 – Create Purchase Order

Authorization Object:
Template for security that contains fields with blank values (uncut key)



Authorization (Field Values):
Authorization object with completed fields (cut key)



SAP Authorization Concept

The components

Roles
Collection of transaction codes, authorizations and user assignments

Buyer

R: Display PO

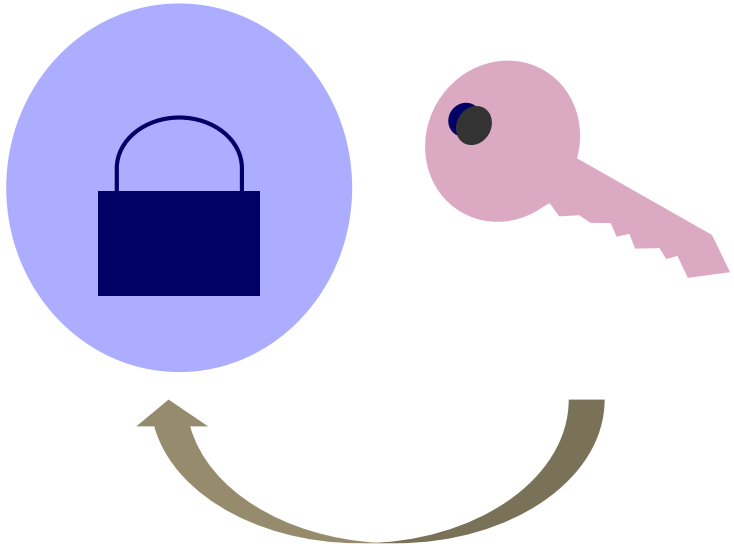
R: Create PO

Profiles
“Key ring” that contains authorizations (cut keys)

Authority Check
Performed by SAP to ensure that a user ID has the correct authorization object and field value combination (cut key) to execute a particular task

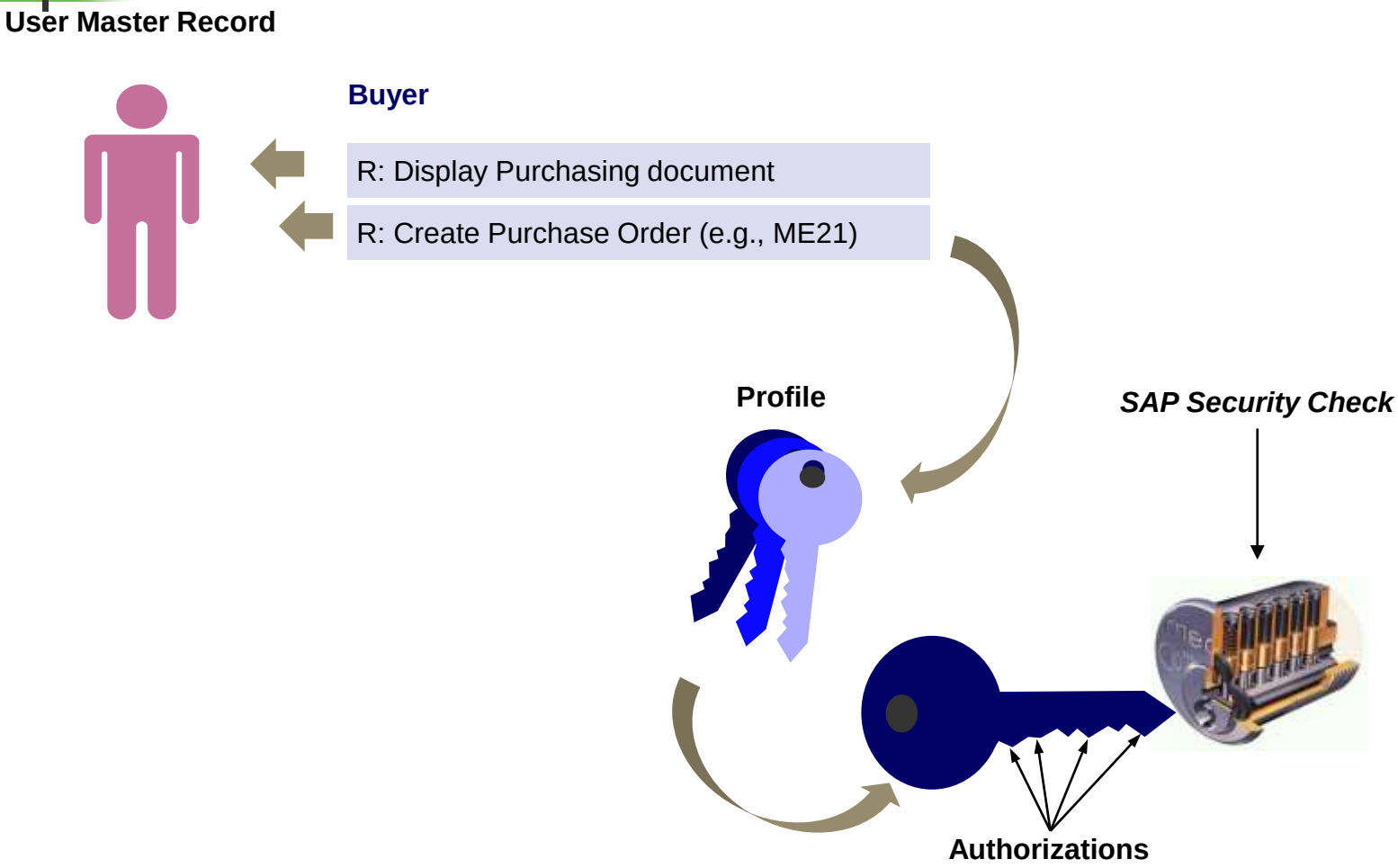
SAP Authorization Concept
Bringing it all together

- **Let's make an analogy…**
- **… the Lock and the Key**



To open the lock, you need the right key!

SAP Authorization Concept
Bringing it all together



Auditing ITGC's in SAP

Risk based approach in a SAP environment

SAP is not a typical application / environment split

Many traditional environment functions are provided within the application including:

- development environment
- change control
- system administration and job scheduling

These functions are collectively known as SAP Basis

Combined with SAP integration, this serves to complicate access security

Risk based approach in a SAP environment

SAP allows more comprehensive functionality and control, however, the following needs to be considered:

- Financial transactions are executed throughout the business making segregation of duties control key
- The SAP access mechanism is complex making security and segregation of duties a key risk
- Configuration has a large impact to the overall business process and controls

Key IT General Control Domains

- Consider tests for controls around:
  - Access to programs and data
  - Changes made to the system (Change management)
  - Computer operations

- Weaknesses identified within the IT general controls can potentially undermine confirmed and tested automated controls and access controls at the business process level

Key Areas within the SAP environment
Access to Programs and Data

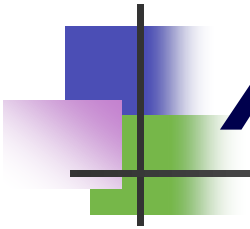
- Key areas to consider include:
  - SAP system settings including password parameters
  - Access to user administration functions including defining and assigning profiles to users (Profile Generator)
  - Access to run programs/ transaction codes
  - Assignment of SAP_ALL, SAP_NEW, other sensitive profiles
  - Default passwords of SAP supplied accounts (SAP*, DDIC, Earlywatch, SAPCPIC etc.)
  - Management and review of User IDs and generic User IDs
  - Use of audit logs (SAP Table Logging)

Key Areas within the SAP environment
Change Management

- Key areas to consider include:
    - Customised programs and tables should be assigned to appropriate authorisation groups.
    - Ability to unlock production environment to make direct changes to production is restricted and monitored
    - Segregation of duties within the change management process including developer, customizer and approver of the program change/transport
    - Changes to SAP tables and data dictionary in the production environment is minimized

Key Areas within the SAP environment
Computer Operations

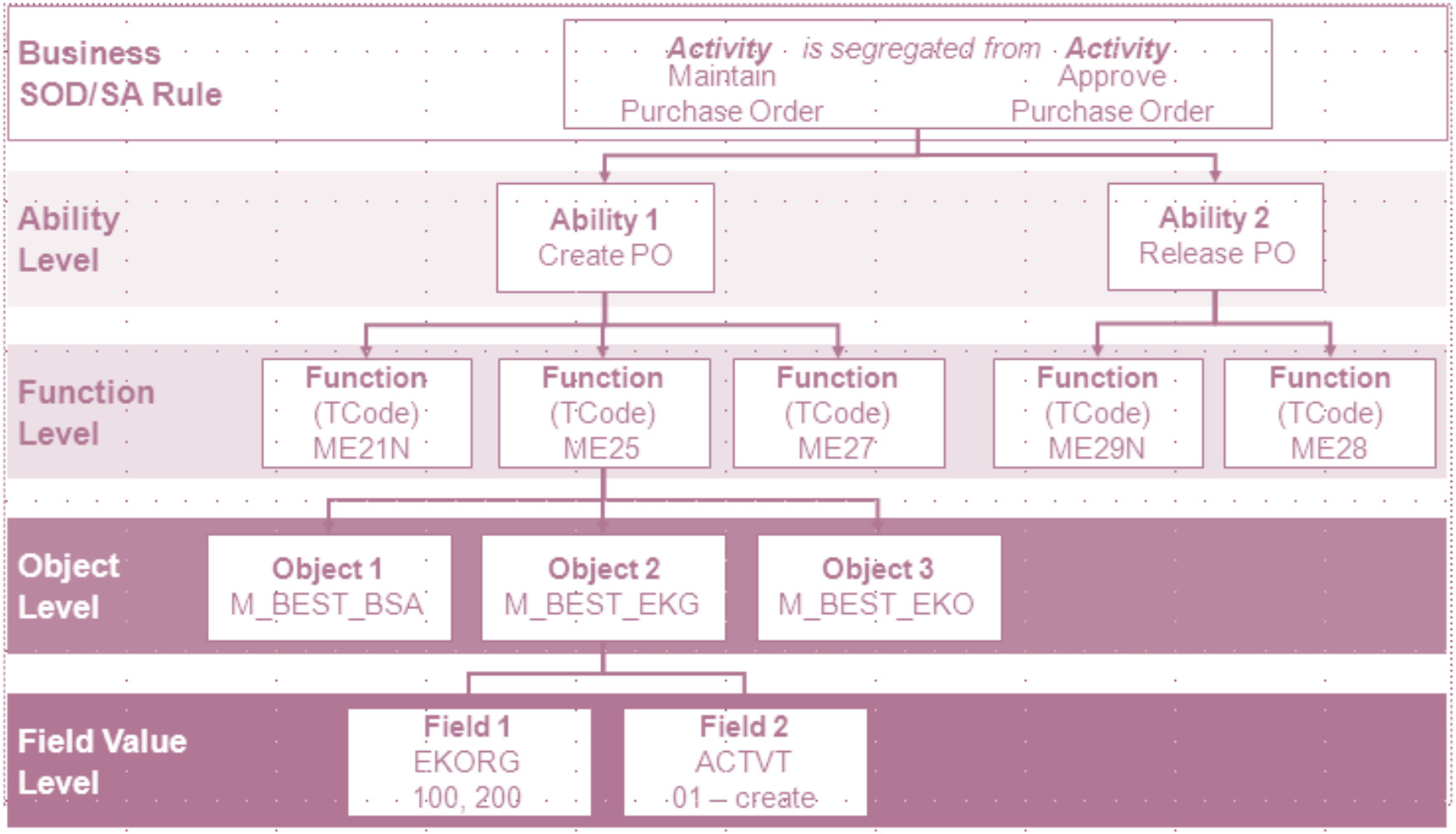
- Key areas to consider include:
  - Batch jobs and interface processing should be regularly monitored, with access to amend them restricted
  - Batch jobs run under ANOTHER user should be restricted to appropriate personnel
  - Batch jobs run under ANY user should be completely restricted
  - Operating and database system administrator access should be restricted



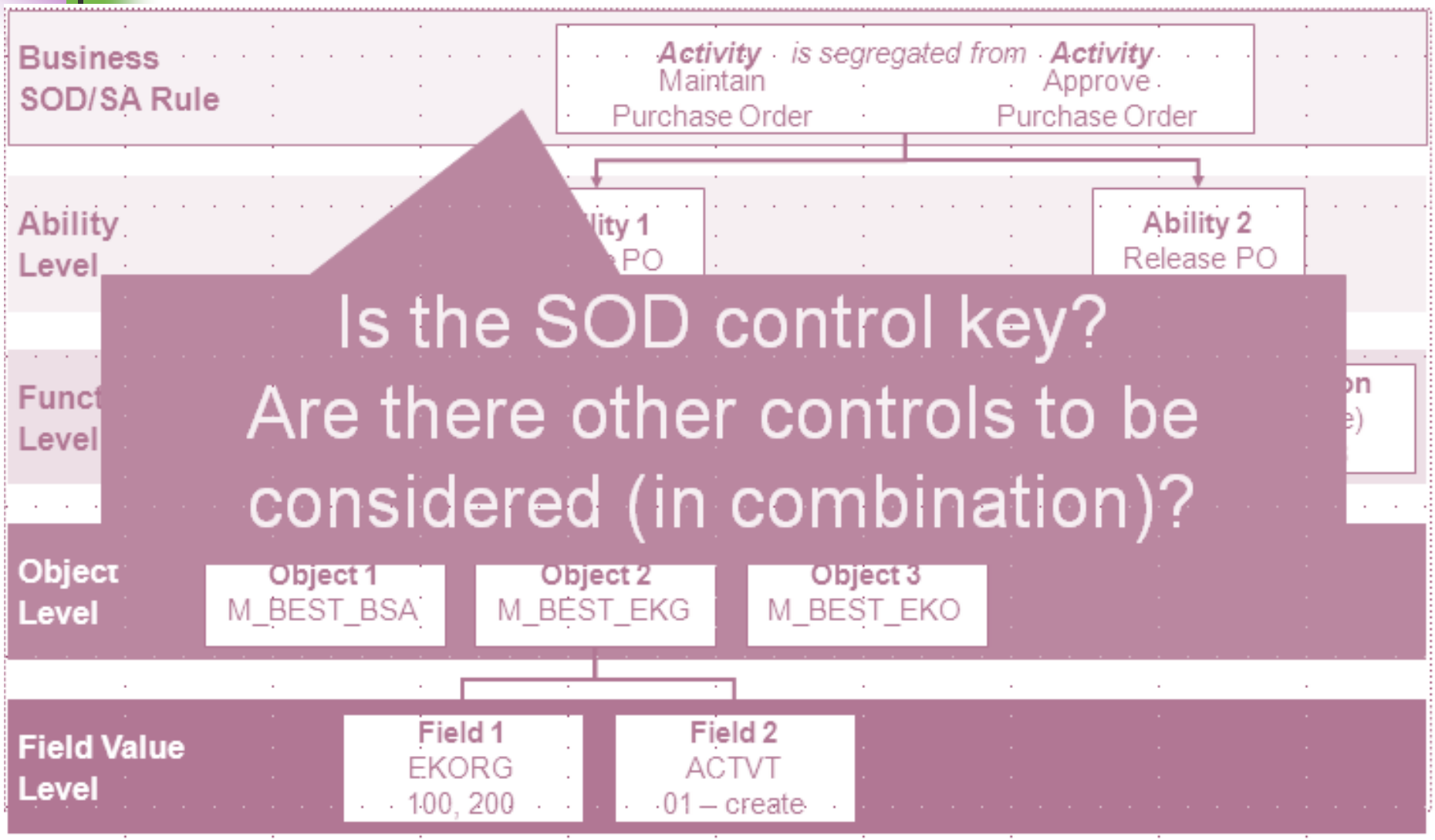
Auditing SAP

Segregation of Duties Example

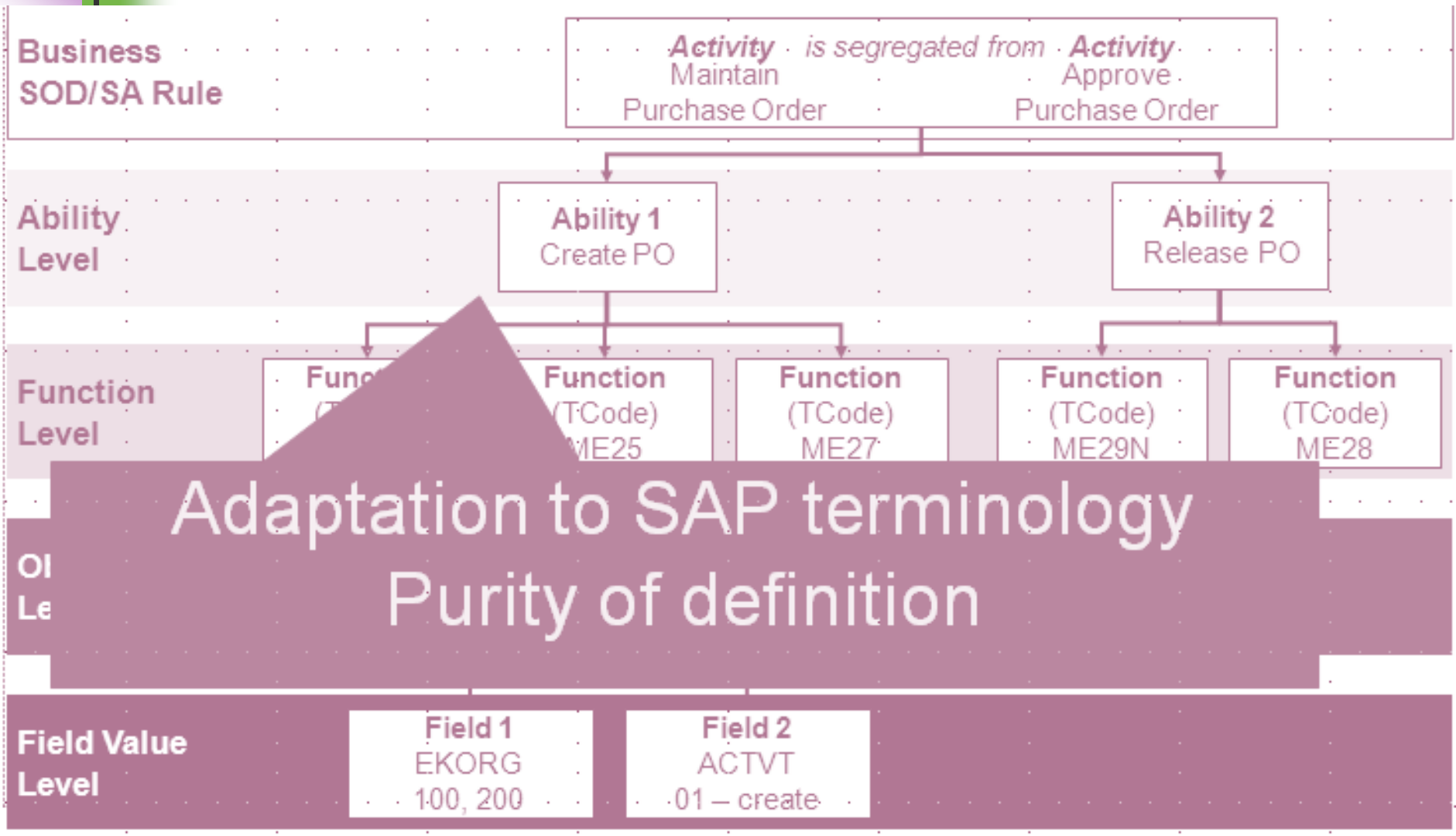
SOD – Framework – Overview



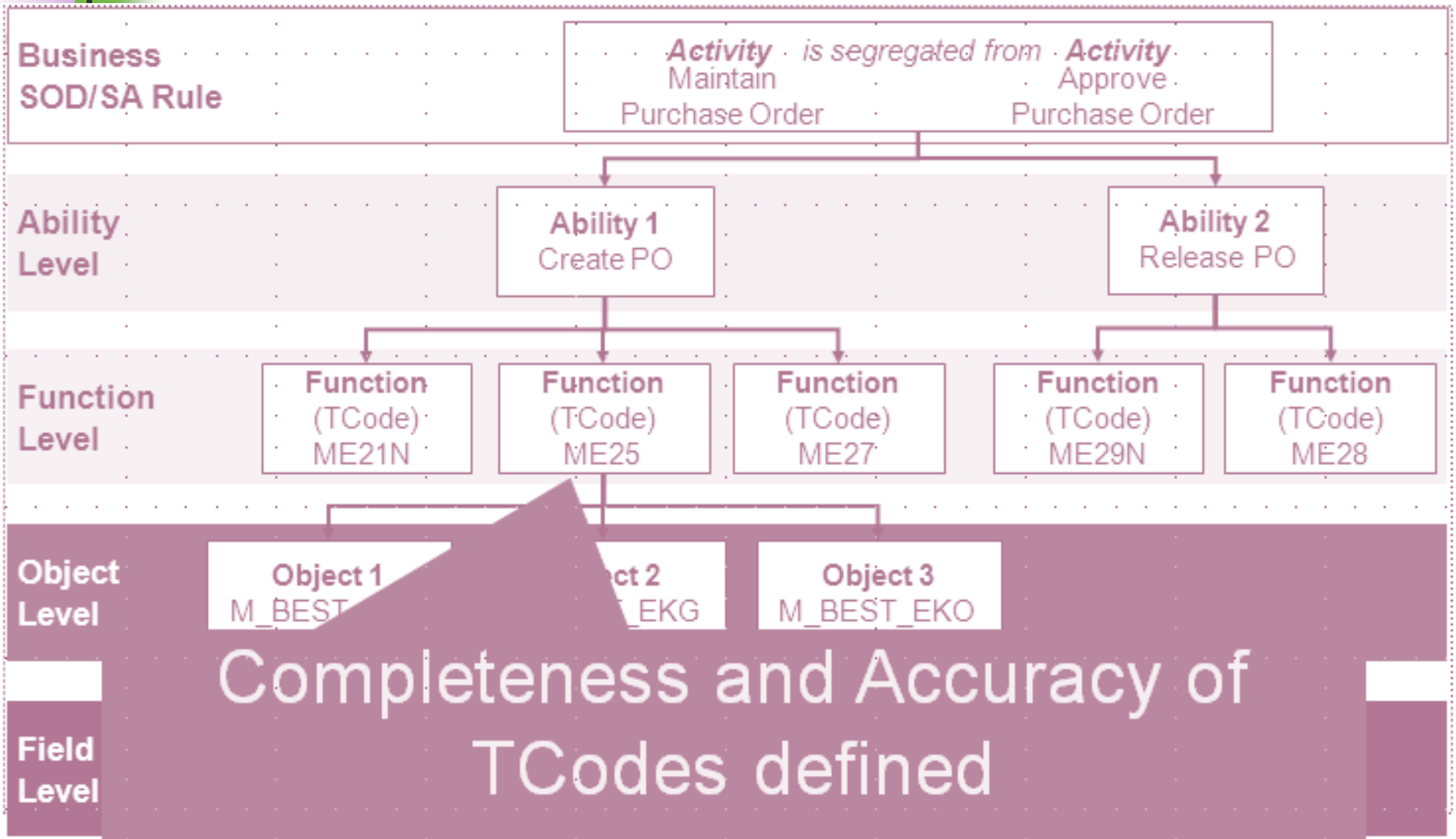
SOD – Framework – SOD/SA Rule



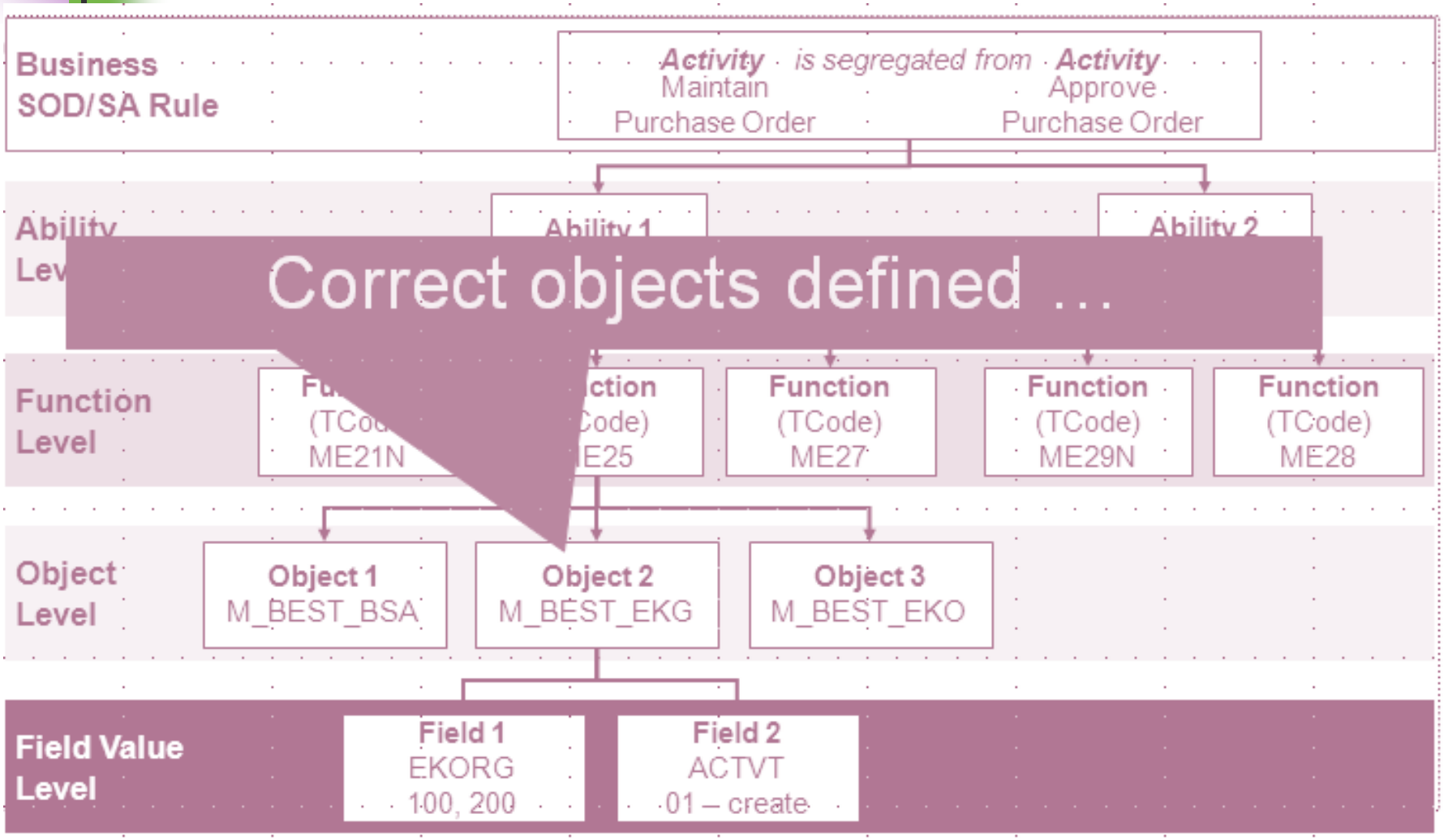
SOD – Framework – SOD Rule



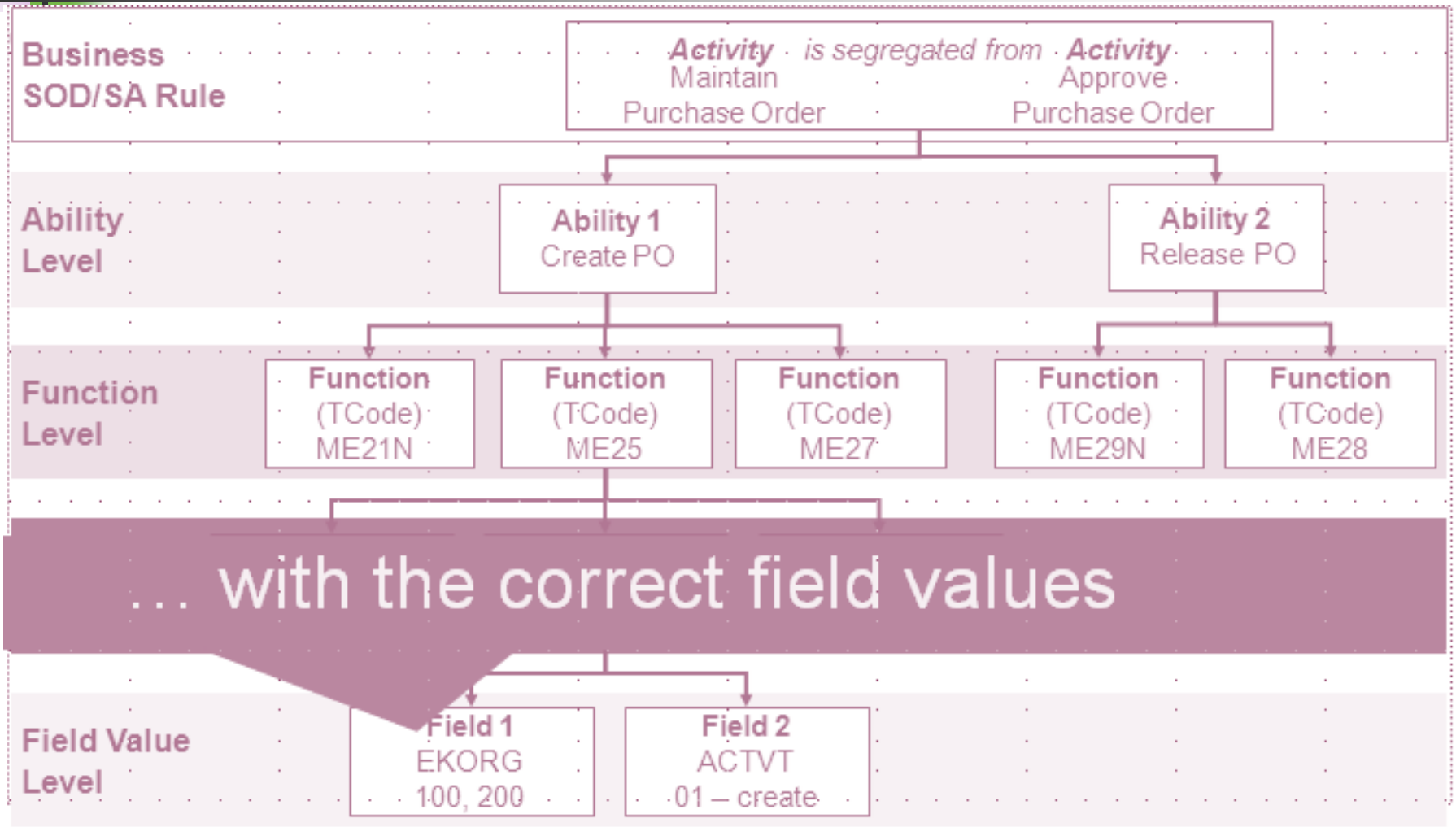
SOD – Framework – SOD Rule



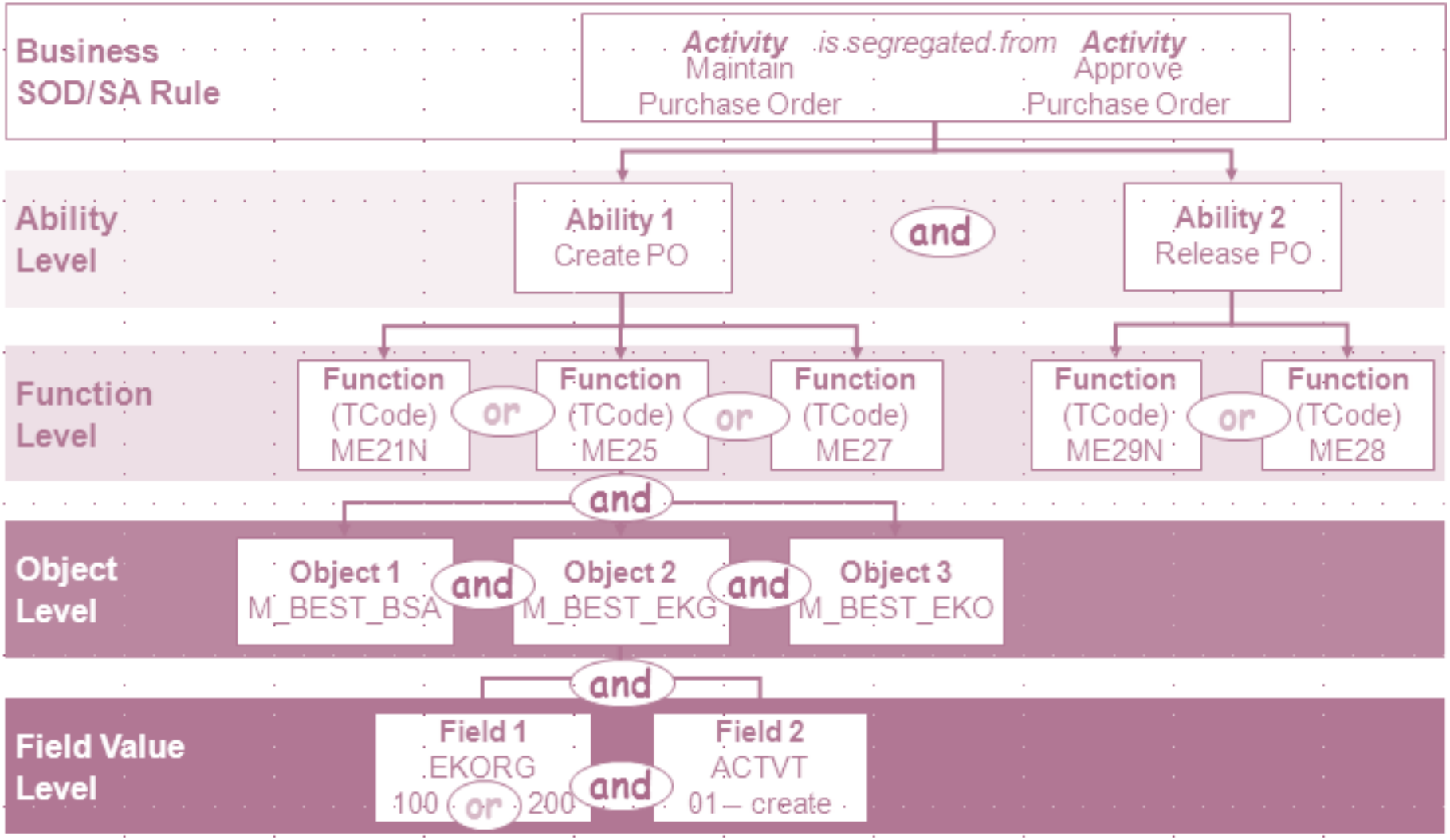
SOD – Framework – Object Level



SOD – Framework – Object Level



Relationships Between Layers



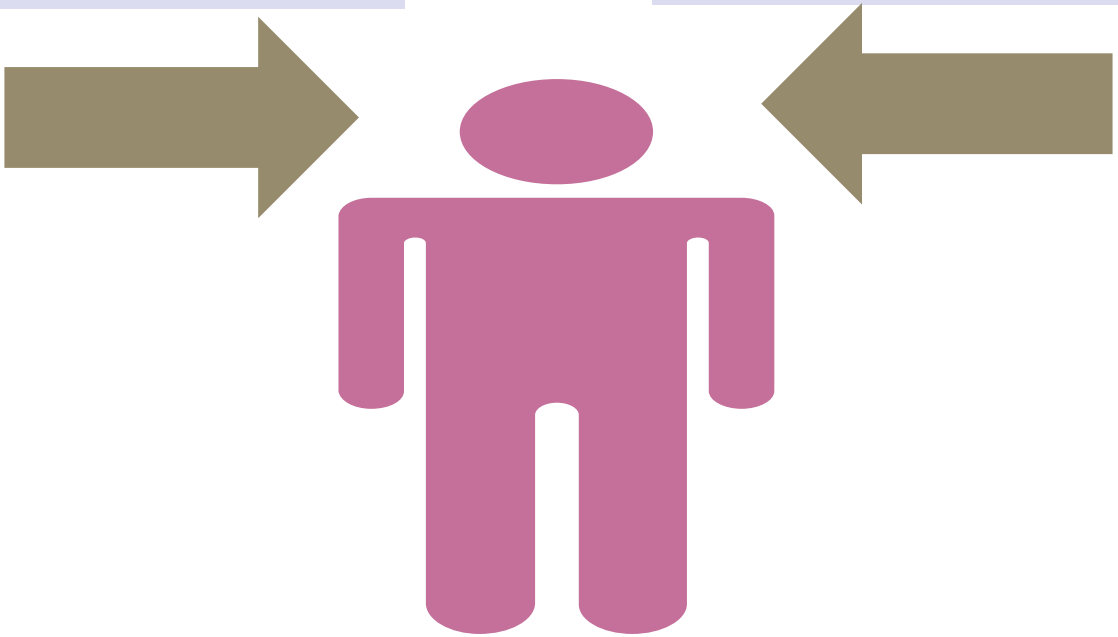
SAP SOD Example

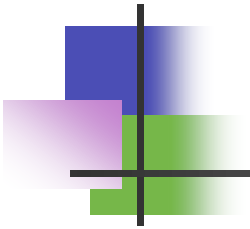
Ability A

Create Maintain Purchase Order
t-code: ME21
Auth Object: M_BEST_BSA
ACTVT: 01

Ability B

Create Maintain Vendor Master Records
t-code: FK01
Auth Object: F_LFA1_APP
ACTVT: 01





Questions?