KPMG

# SAP S/4HANA Security and authorizations

**Webinar**

**27/04/2021**

KPMG Advisory Belgium

# Contents

# Today's speakers

## Maarten Vercruyssen

Maarten is senior manager within KPMG Advisory focusing on SAP Security and Governance, Risk and Compliance.

With over 9 years of experience, Maarten worked at multiple clients and projects with regard the design and implementation of SAP authorizations, as well as in auditing and reviewing existing authorizations in both ECC and S/4HANA environments.

## Philip van Geenen

Philip is a Senior Expert Advisor at KPMG Advisory with more than 9 years of experience in the area of Governance, Risk and Compliance.

He has built up an expertise on User and Access Management in SAP during different SAP consulting projects. He is familiar with all the area's in the UAM roadmap. Designing roles, building role, testing, SoD analysis, Go live support, creating policies and procedure, authorization training.

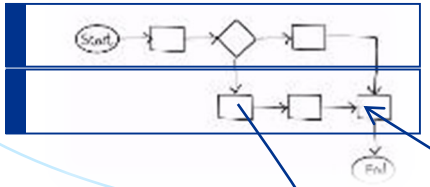
# Setting the Scene

# Setting the scene

*“Security and authorizations should be an integrated part of your S/4 Hana project approach and risk management approach”*

# Setting the scene

Business Processes



Lead to...

Risks

Controlled by...

Controls

- Configuation Controls
- Access controls
- Reports
- Procedures

Business roles are translated into composite roles

Composite role

Single role 1
Single role 2
Single role 3

Activities are translated to single roles

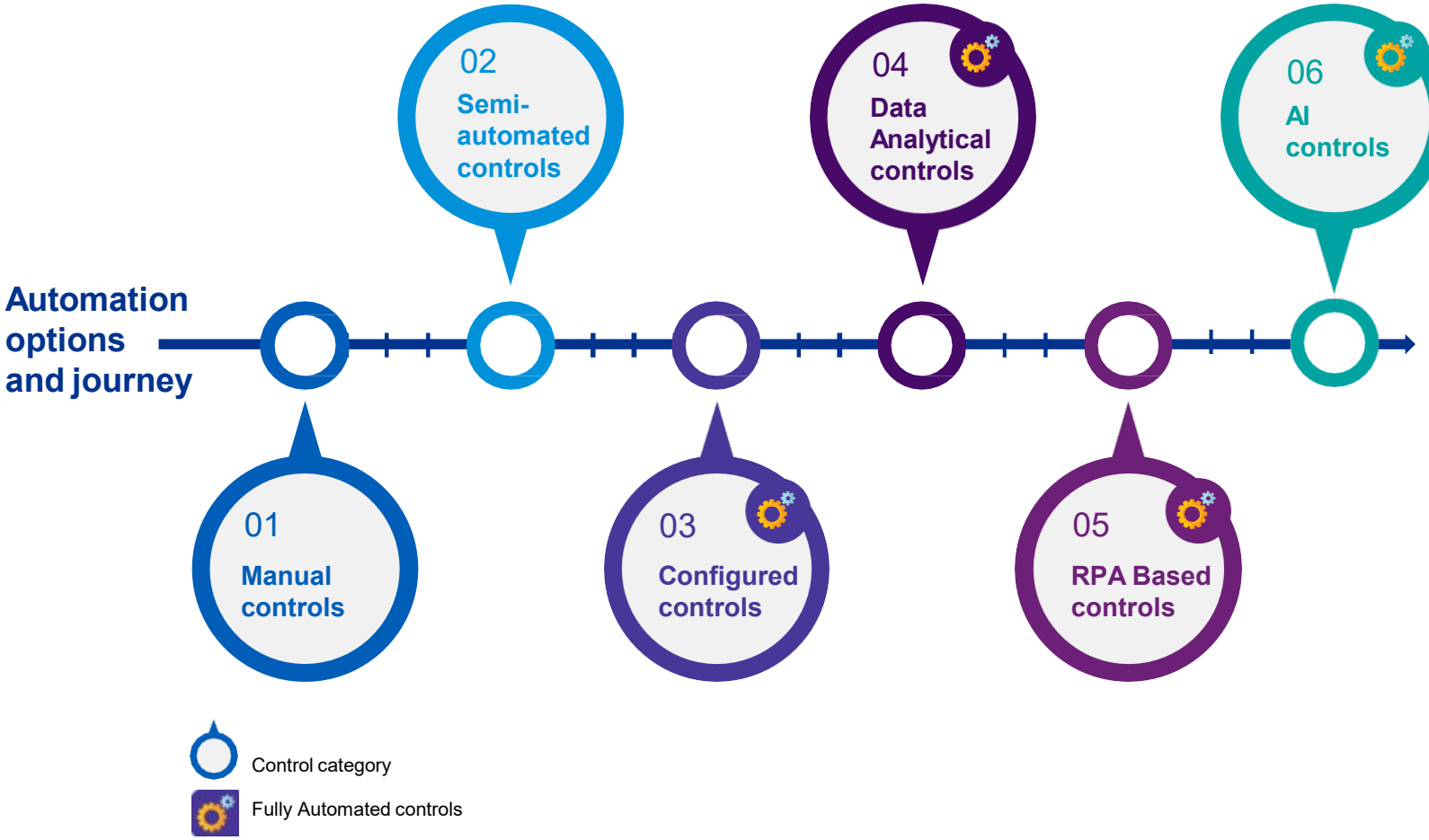
SoD Conflicts should be properly embedded in the design.

Technically translated in...

SoD Matrix

SoD Risk 1 = Activity 1 + Activity 2

# The evolution of control options to manage risk and regulation

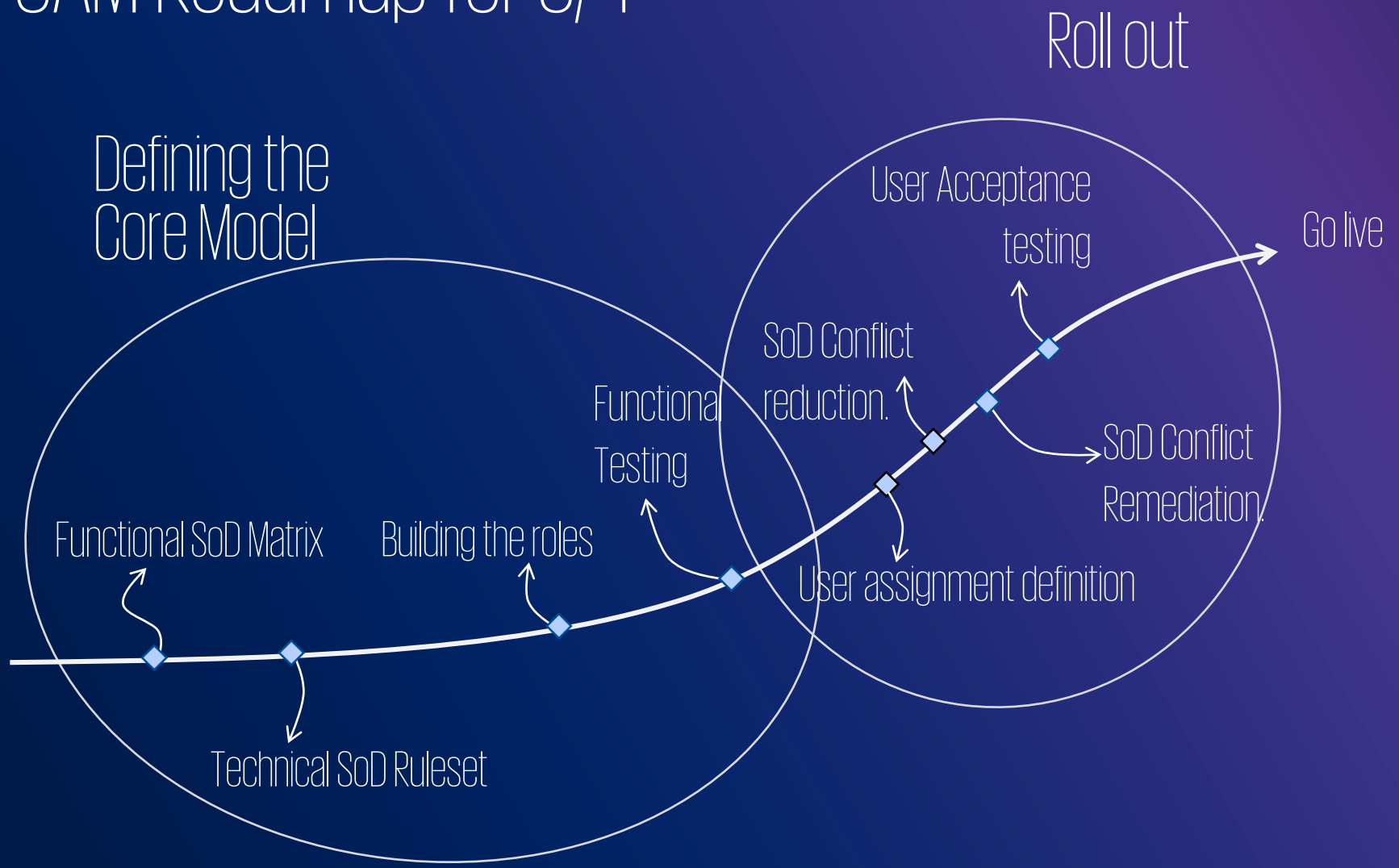



## We need to accelerate automation

- All functions within an organization need to operate controls to manage risk; this is a given however there is an increasing need to automate manual activities reducing reliance on key resources
- With the sheer scale and pace of technology there are more options than ever to automate controls where this is best suited to do so.

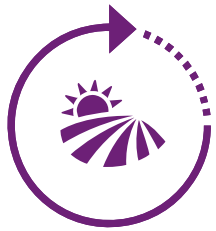
# S/4 Hana UAM Roadmap

# Typical UAM Roadmap for S/4



# Reviewing the functional SoD Matrix

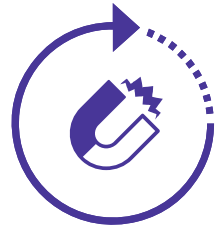
The SoD Matrix translates all Access Controls from the Risk & Control Matrix into a measurable set of system risks that should be monitored in your S/4 Hana environment.



## Greenfield implementation

Greenfield implementation will implement the S/4 Hana from scratch, potentially implementing new functionality or altering existing business processes.

Activities should therefore include a full revision of the risks with the SoD Matrix to ensure that they are covering all modules and processes.



## Brownfield implementation

Brownfield implementation will implement the processes ‘as is’ into the new S/4 Hana environment.

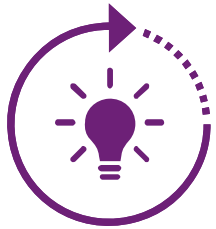
Activities are therefore focused on re-evaluating the risk level based upon potential changes in the overall control environment.



KPMG

# Reviewing the technical ruleset

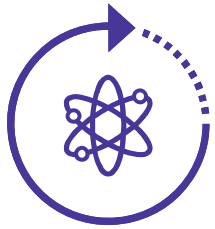
The SoD Ruleset translates the risks from the SoD matrix into technical ‘rules’: a combination of transactions, Fiori applications and underlying authorization objects. These need to revised to incorporate the latest S/4 Hana changes.



New Fiori Apps

Old transactions will be replaced by new Fiori Applications with similar functionalities.

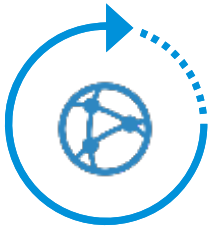
Example:
F-03 Clear G/L Account into F1579 – Clear G/L Accounts



Changed transactions

Functionality of transactions might be changed an therefore requires an update in the SoD Matrix

Example:
XK01 is replaced with new transaction BP



Changed objects

New or adjusted authorization objects and values should be properly incorporated into the SoD Matrix

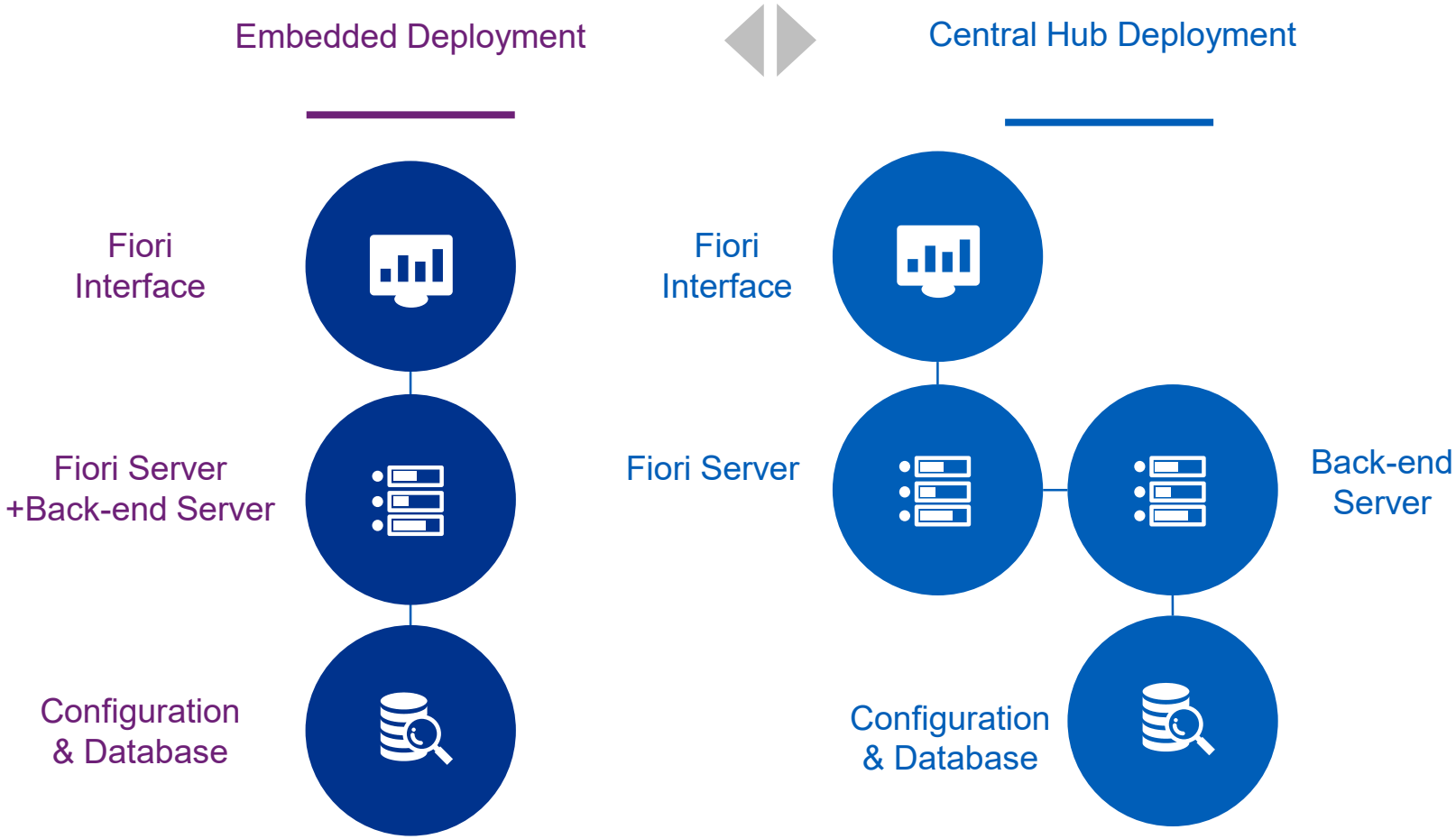
Example: S_Service object should be considered for oData services.



KPMG

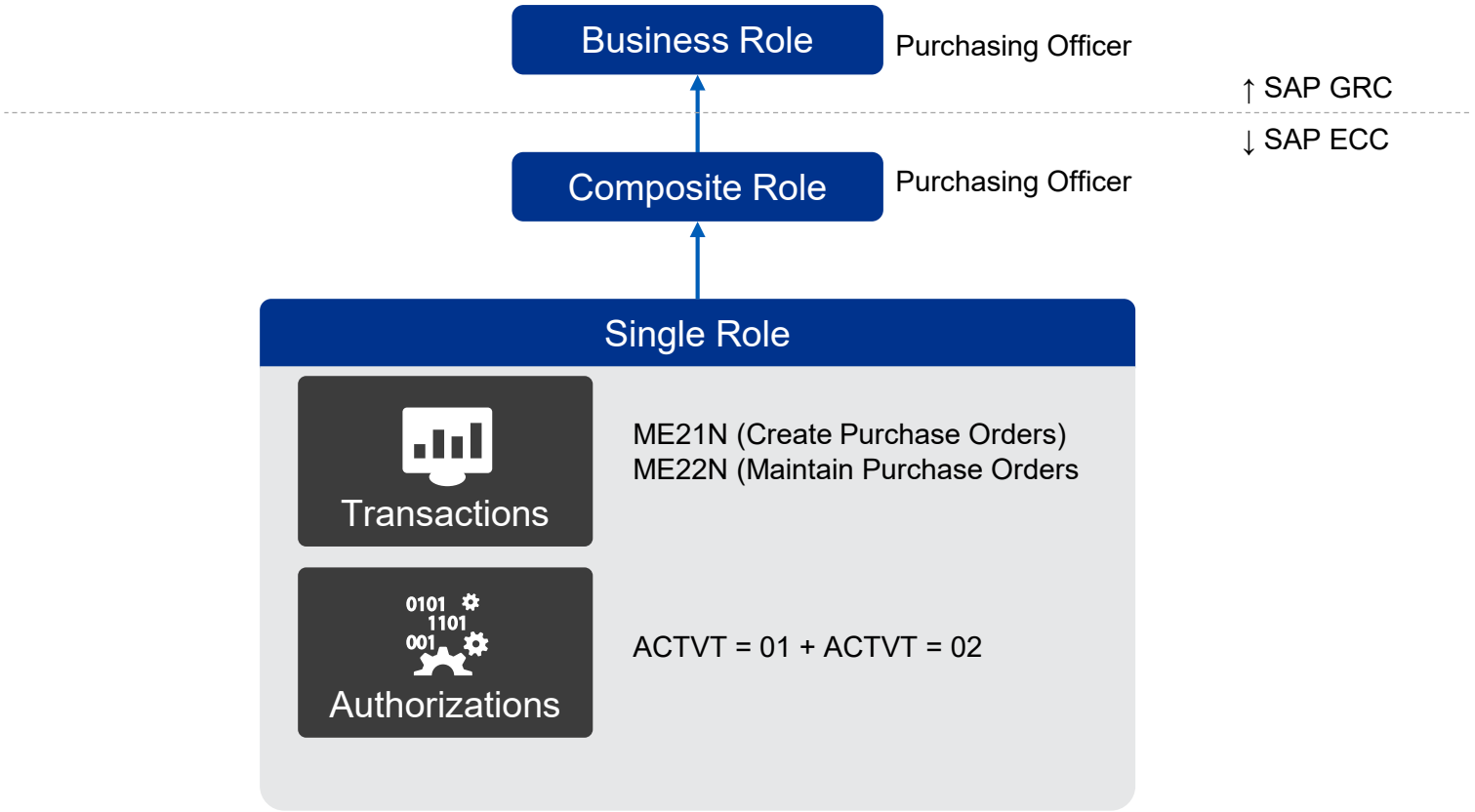
# Building the roles

The complexity of the roles depends on the architecture used in the setup of the Fiori Gateway Server:

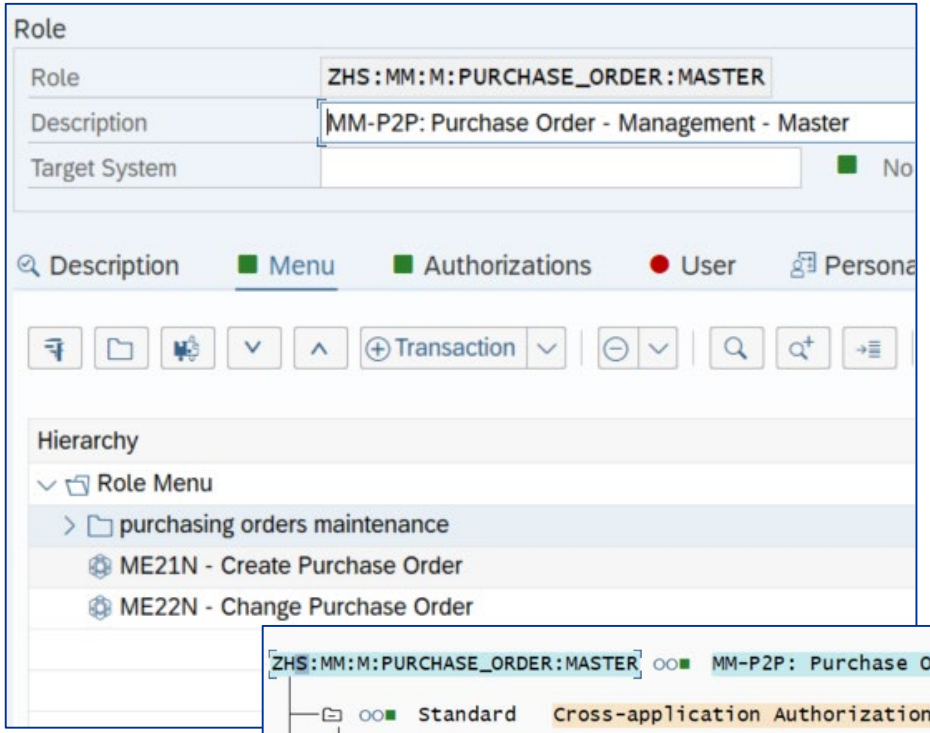


# Building the roles

The following diagram explains the ‘old’ ECC setup of roles:

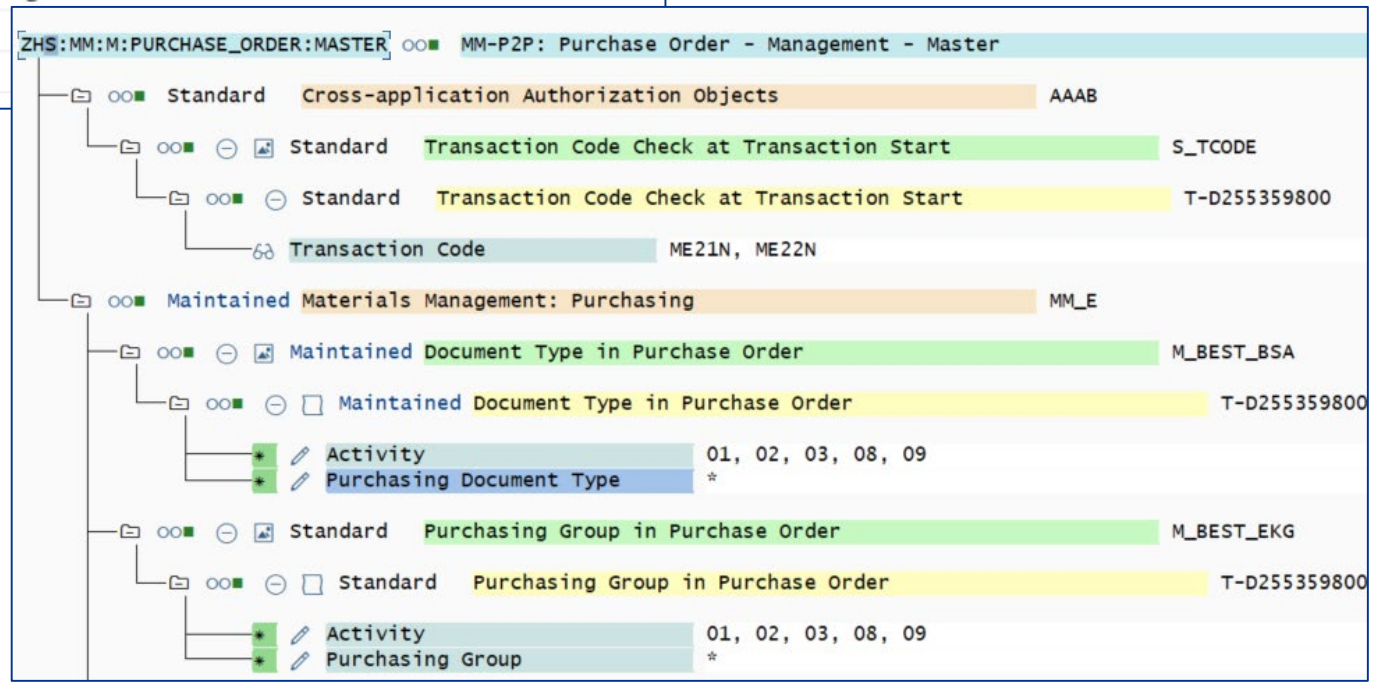


# Example: building a role in ECC



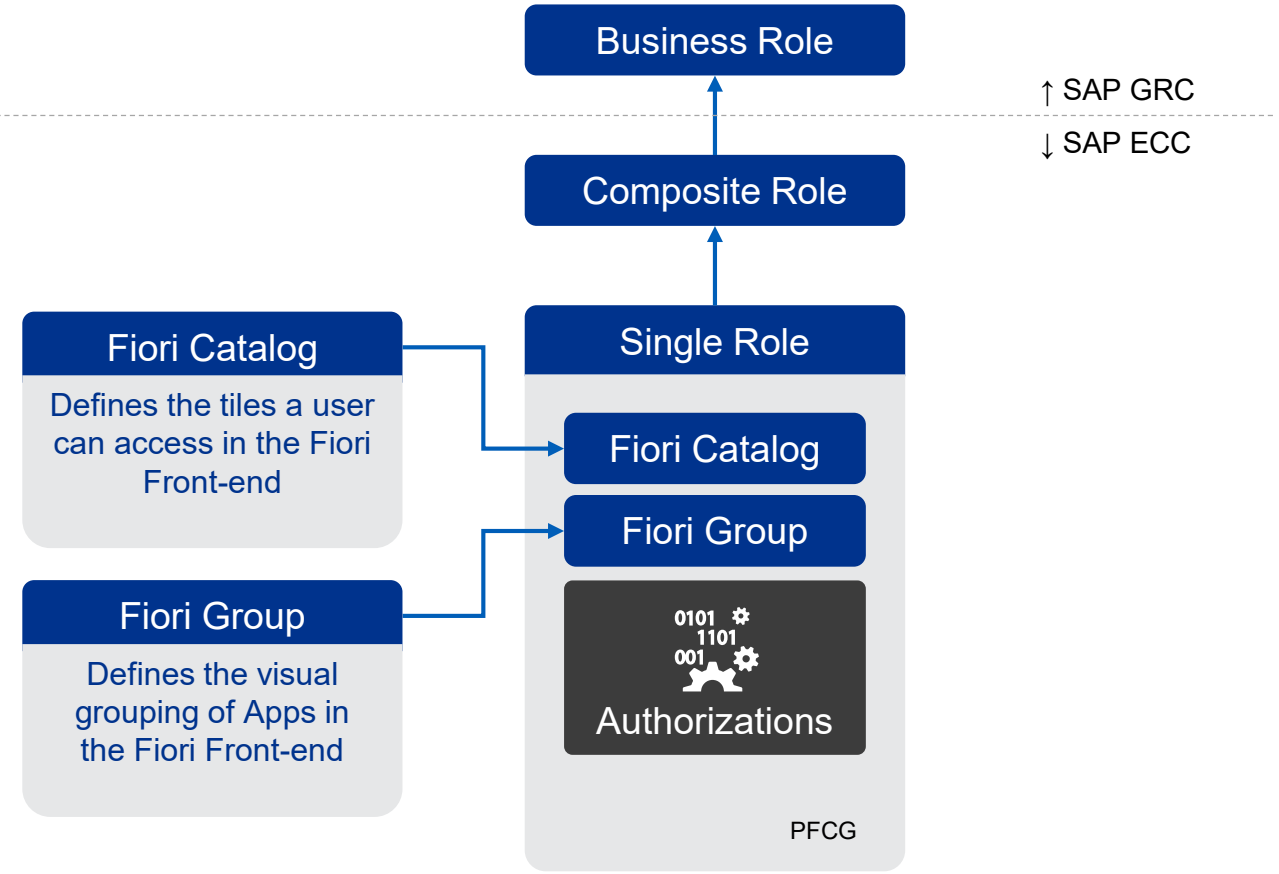

Step 1: Add transactions to the menu of your role.

Step 2: Maintain the related authorization objects.



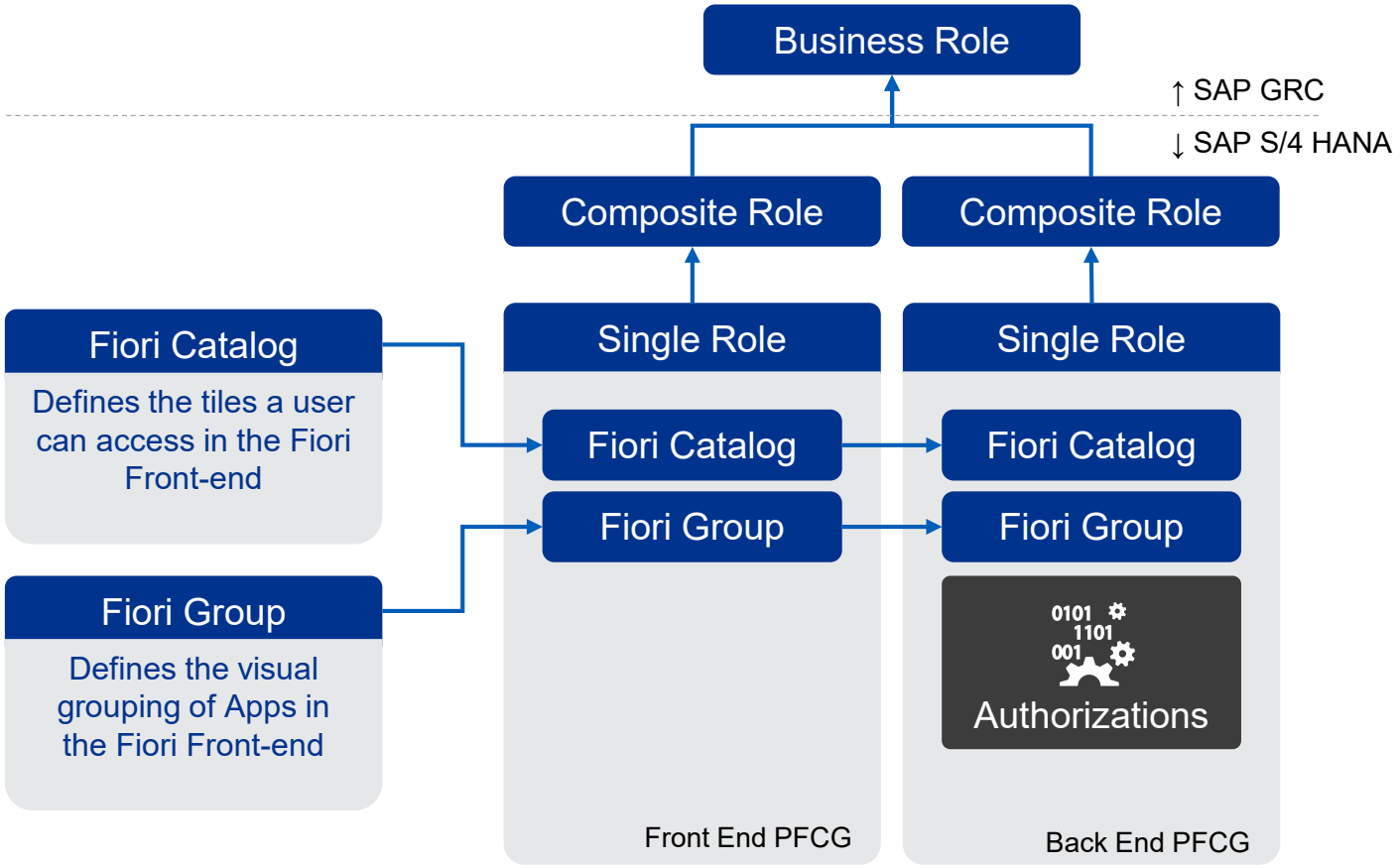
# Building the roles

The following diagram explains the new step in case of an ‘Embedded Deployment’:



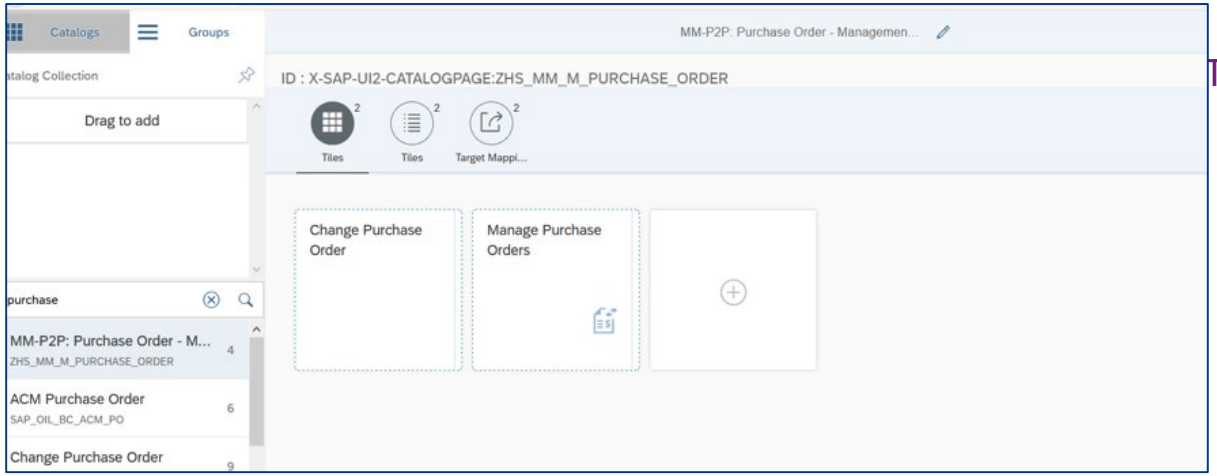
# Building the roles

The following diagram explains the new step in case of an 'Central Hub Deployment':



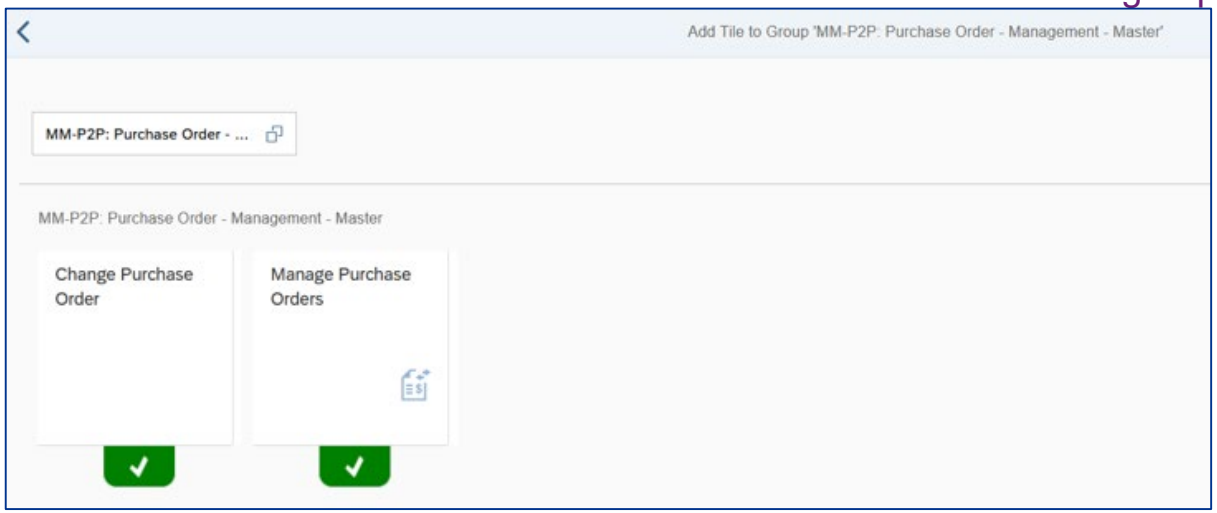
# Example: building a role S/4 Hana

## Part 1. Creation of a group & catalog



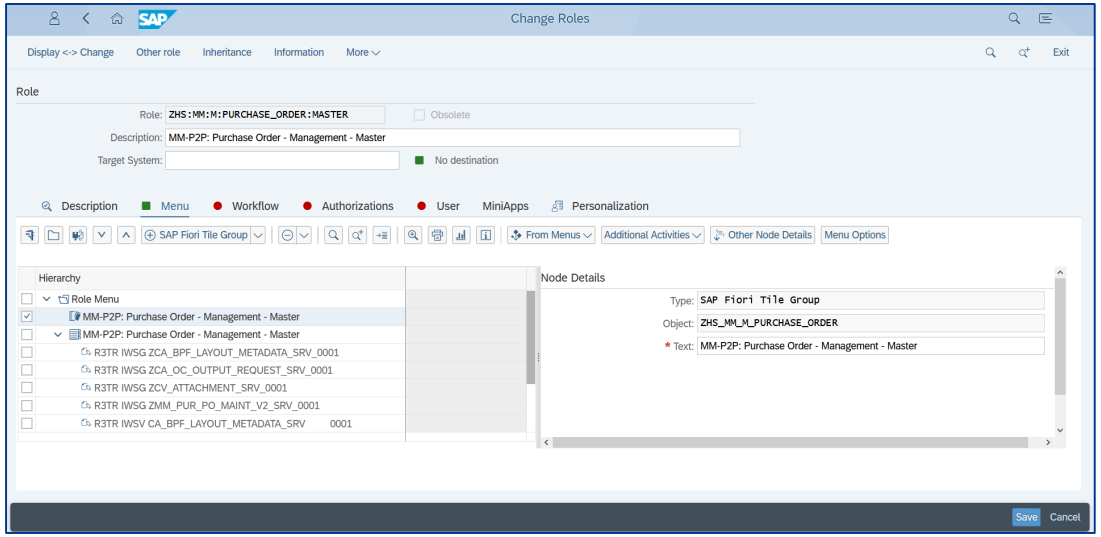

Step 1: Add Fiori Apps & Transactions to a catalog.

Step 2: Add Fiori Apps & Transactions to a group

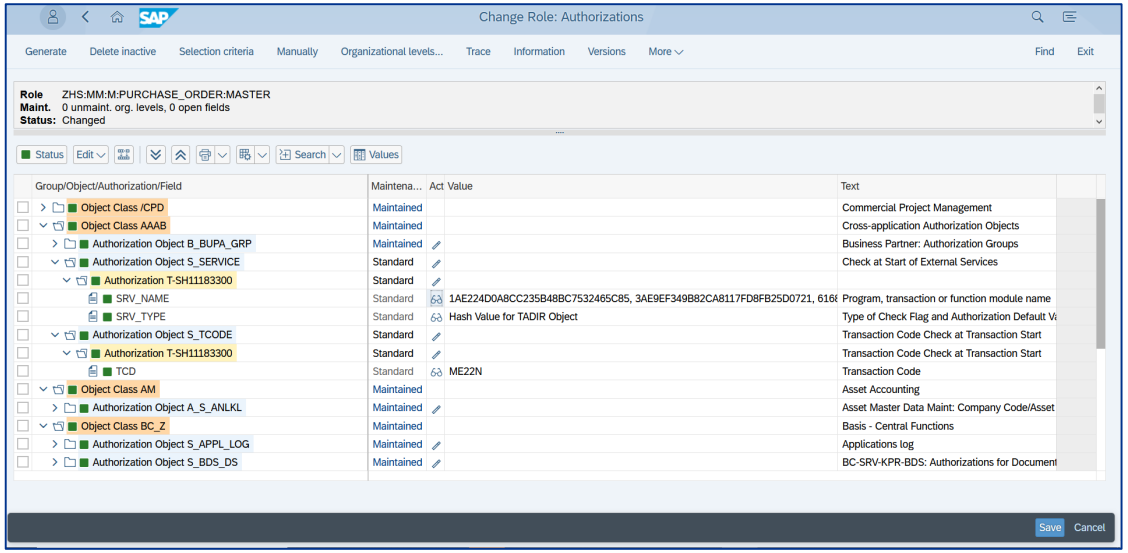


# Example: building a role S/4 Hana

## Part 2. Creation of a PFCG Role




Step 3: Add Catalogs & Groups to PFCG Roles



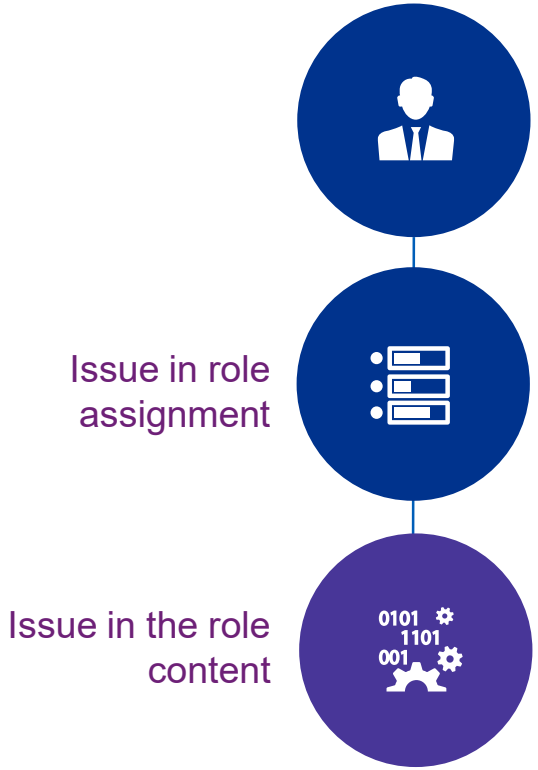

Step 4: Maintain the related authorization objects.

# Testing

The complexity of authorization issues greatly increased, due to the increased points of failure. This has an impact during both testing and after go-live:

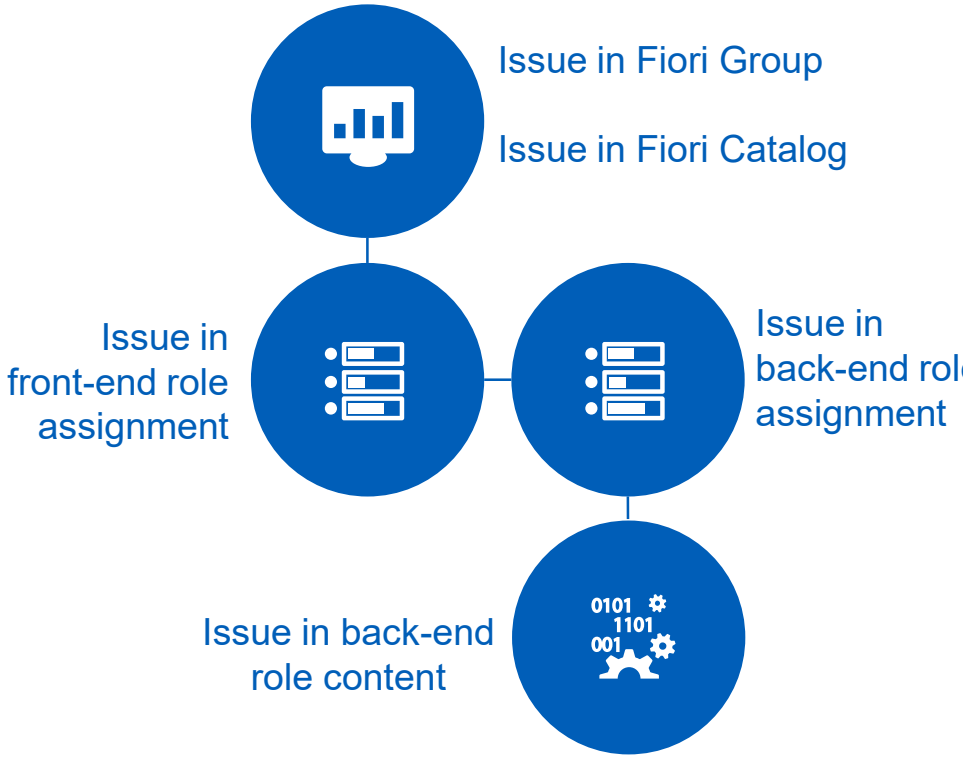
## SAP ECC

2 points of failure




## SAP S/4 Hana

5 points of failure



# SoD Conflict Reduction & Remediation

01 Functional SoD Matrix

02 Technical SoD Ruleset

03 Building The Roles

04 Testing

05 SoD Conflict Remediation

## SOD Reduction

Reduce number of SoD conflicts by finetuning roles and user assignments.

- Cleanup at role level
- Cleanup at user assignment level

## SOD Remediation

Evaluate the remaining risks and define controls to mitigate this risk where required.

- Focus on existing controls from control matrix
- Focus on automated controls where possible

KPMG

# KPMG Powered Enterprise

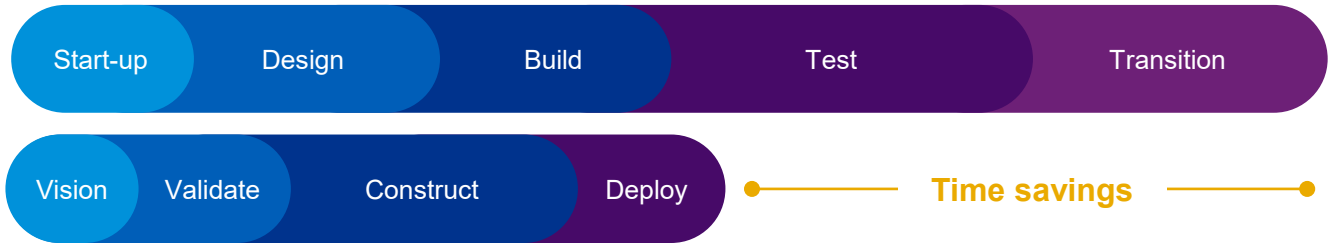
KPMG's toolbox "Powered Enterprise" can help to shorten your transformation journey and let you focus on your day-to-day business.

## What is KPMG Powered Enterprise?

- Comprehensive method and set of assets based on decades of business and technology experience in business transformation
- Tools that support organization, operating model, business process and control design
- Accelerates value delivery with leading practice performance measurement, data modelling/reporting, training, and project delivery capabilities

## How will Powered Enterprise benefit your organization?

- Validate pre-built operating models instead of starting from scratch
- Immediate access to industry insights, practices and processes to support your decision making
- Shift your focus to high value business decisions
- Increase certainty of outcomes and reduce risk with our end-to-end approach



# Our toolbox covers each layer of an organization

Powered Enterprise is designed specifically for SAP S/4HANA


**6 Design layers**

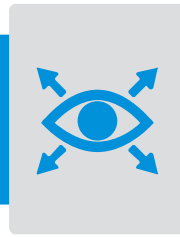
| Service delivery model | People | Functional process | Technology | Performance insights & data | Compliance & Security |
|---|---|---|---|---|---|
| Service delivery options | Organization & role mappings | Functional decomposition | Application architecture & integrations | Reporting package & dashboards | Risks & controls |
| Service management framework | Global process owners | Maturity models | Application module by process decomposition | Value driver KPIs | Policies |
| | Role based job descriptions | Leading practices | Environment architecture | MDM implementation designs | |
| | | Role based process flows | | | |

# Wrap up

# Wrap up

Make sure security & compliance is embedded in your project approach

01



Make sure the team responsible for implementing authorizations has a background in risk & compliance

02

Make sure SoD is assessed and roles are clean before testing and go-live

03

Do not underestimate the complexity of security in S/4 Hana

04

**kpmg.com/poweredenterprise**