SAP AUDIT UPDATE 2021
PART 2
FOCUS ON SOD

9/11 2021

9.00-9.45

AGENDA

1. Introduction to financial audit of SAP
2. Current audit focus areas – deep dive: segregation of duties
3. SoD process supported by tools
4. The SoD method & best practices

PRESENTERS

Troels Lindgård
E: troels.lindgaard@1digitaltrust.com
M: +45 5363 5787

1DigitalTrust
www.1DigitalTrust.com

Jesper Parsberg Madsen
E: jesper.parsberg.madsen@pwc.com
M: +45 2141 5985

PwC
www.PwC.dk

Ole Sølvsten Hemmingsen
E: ole.solvsten@compliancenow.eu
M: +45 3053 3920

ComplianceNow
www.complianceNow.eu

1

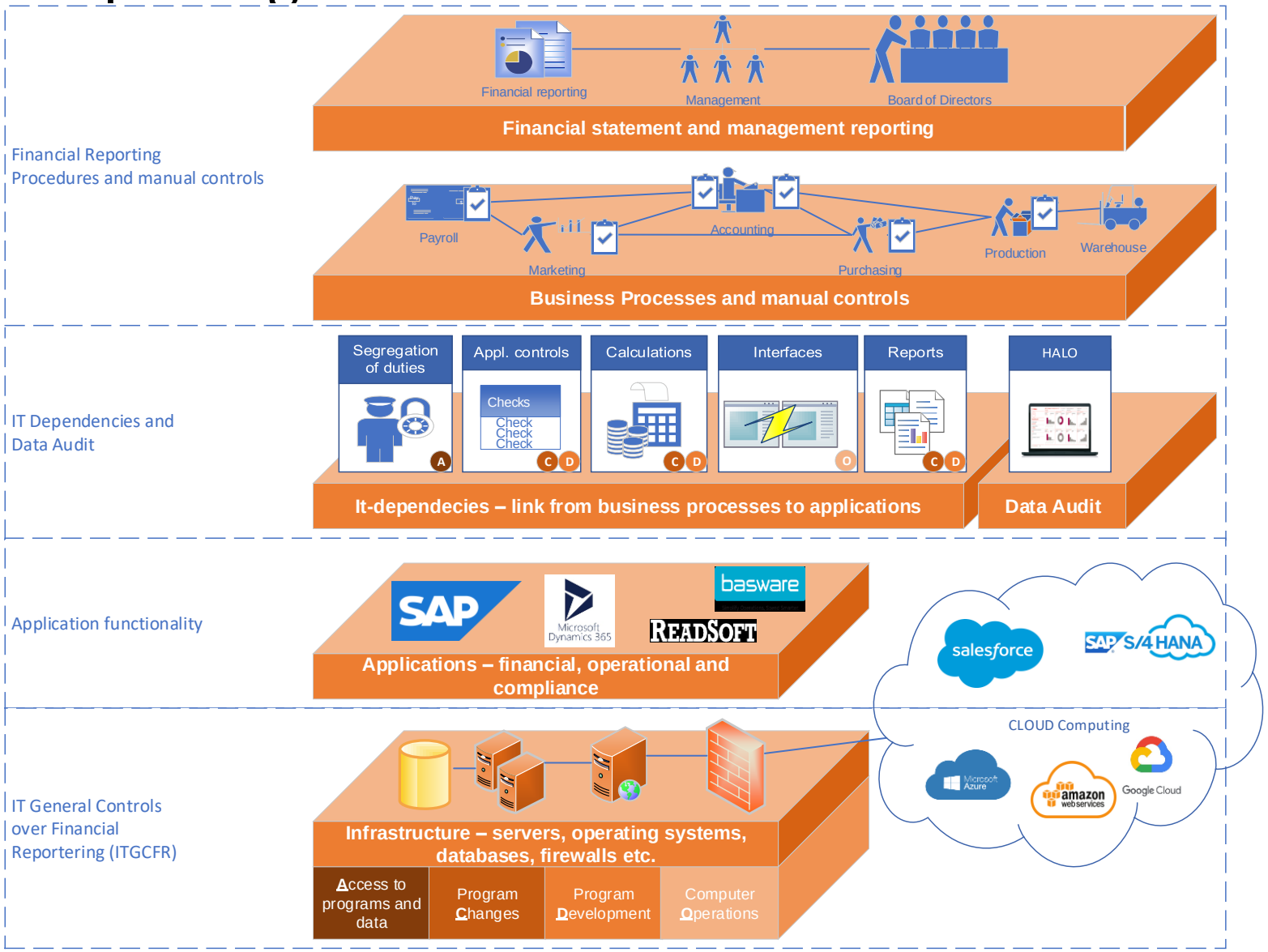
Introduction to financial audit of SAP

Compliance requirements impacting the audit

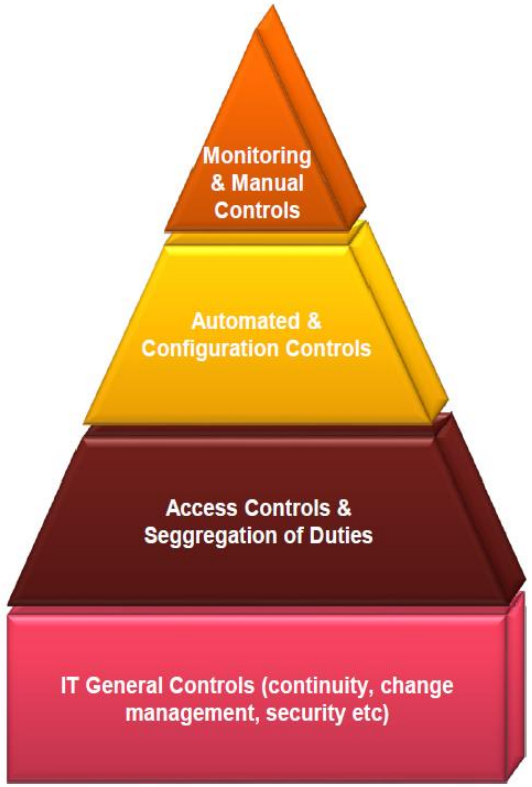
Compliance requirements are multi-layered in the business as well as in the IT environment.

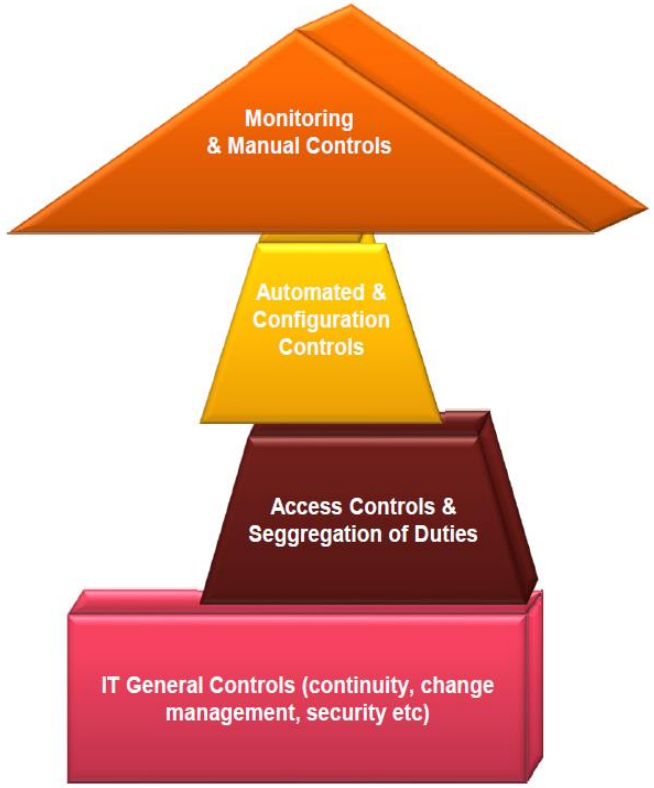
The requirements also apply to vendors.

Compliance requirements trigger the need for internal controls.



Getting the right balance in controls





Preventive controls (before the event)		Detective controls (after the event)	
Security roles	Workflow	Segregation of duty Function	Alerts based on compli-ance rules
Segregation of duty Function	Module set-up	Utilisation KPIs	Database logging

2

Current audit focus areas – deep dive: Segregation of Duties

Authentication vs. Authorization

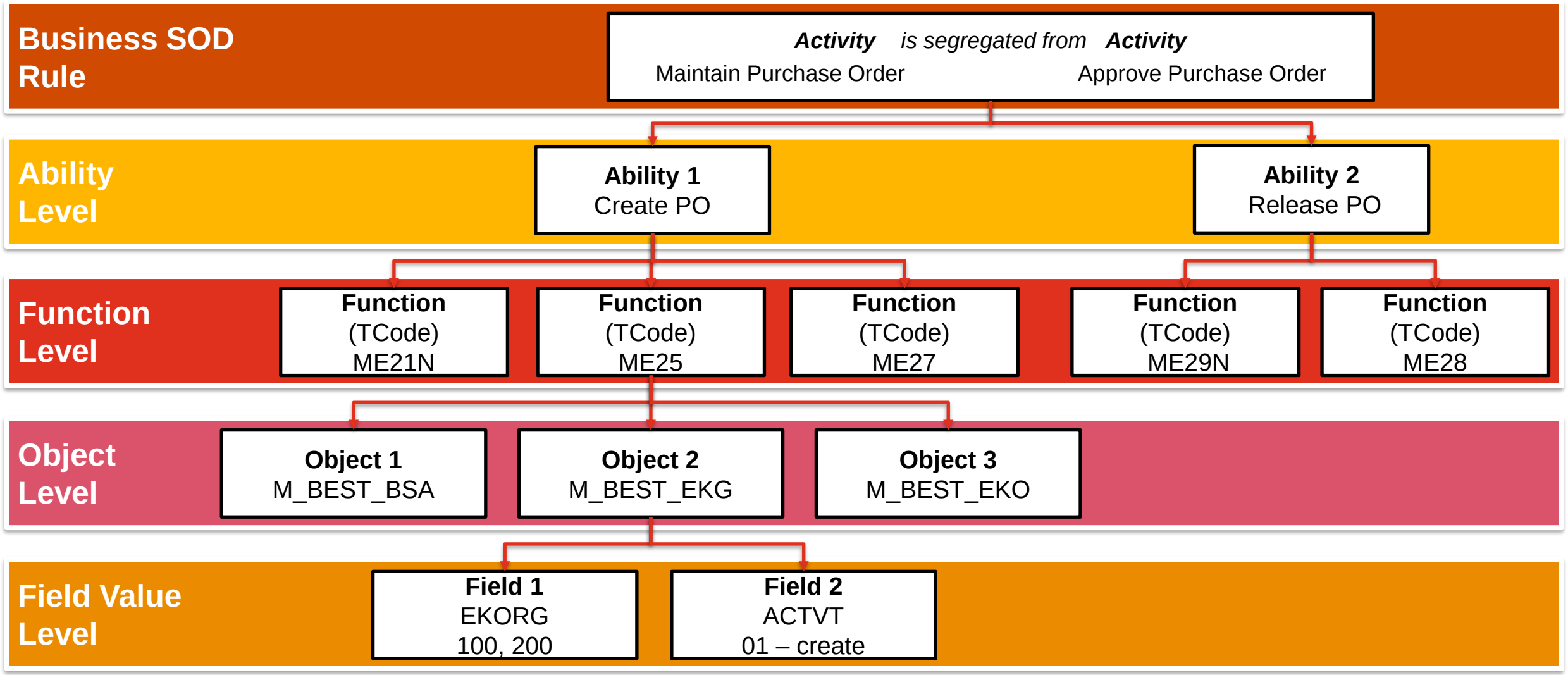
What is AUTHENTICATION?

- Relates to who you are
- Determines whether you can get into SAP

What is AUTHORIZATION?

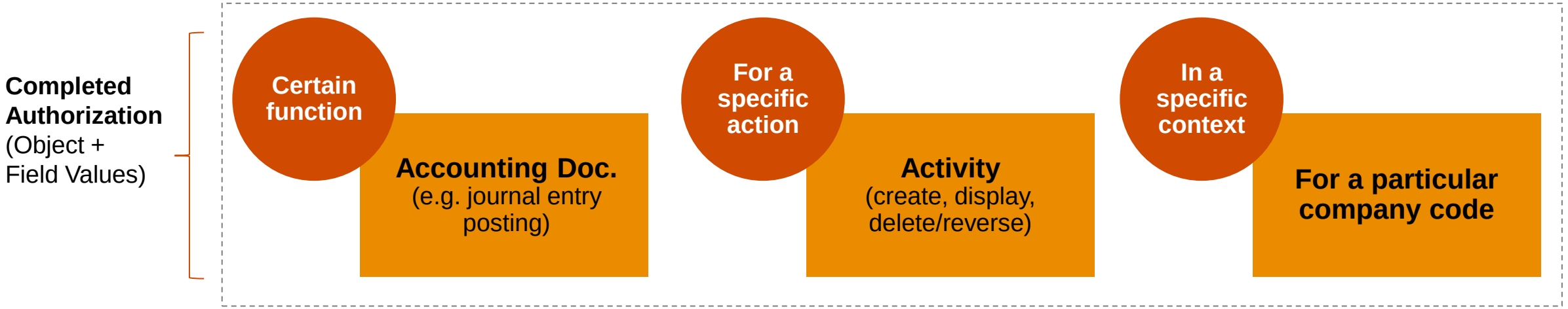
- Relates to what you can do
- Determines what activities you are permitted to perform while in SAP

Authorizations and Segregation of Duties



Authorization objects

Authorization objects are the basic building blocks of SAP security, and allow you to define complex authorizations. SAP is delivered with about 1500 authorisation objects! They are used to grant access to:



All authorization objects are named based on 3 structures, e.g. F_BKPF_BUK:

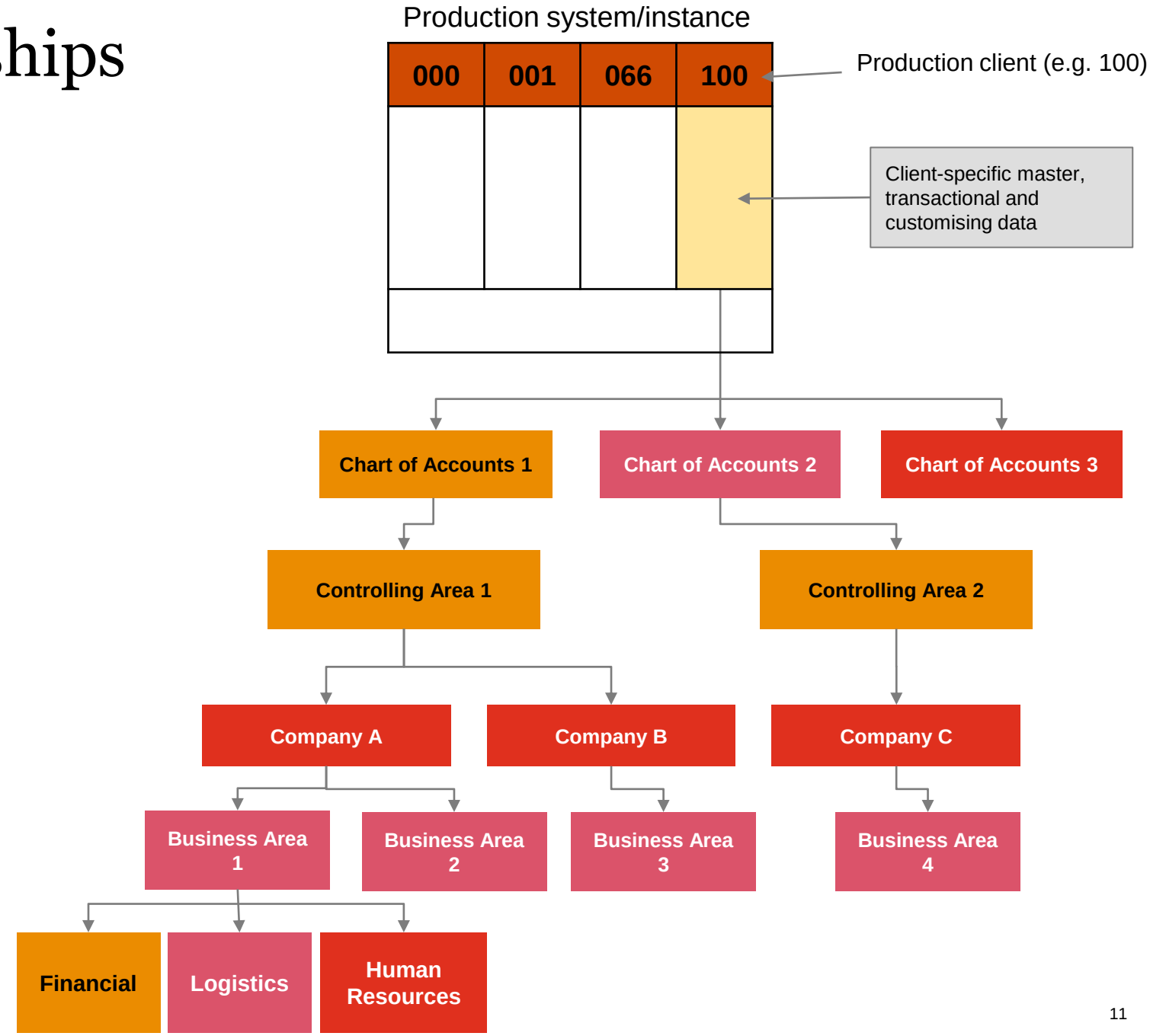
Module	F = Finance
Business object	BKPF = Accounting documents
Context	BUK = Company code

All authorization objects related to Accounting documents in FI start with F_BKPF_

SAP structural relationships

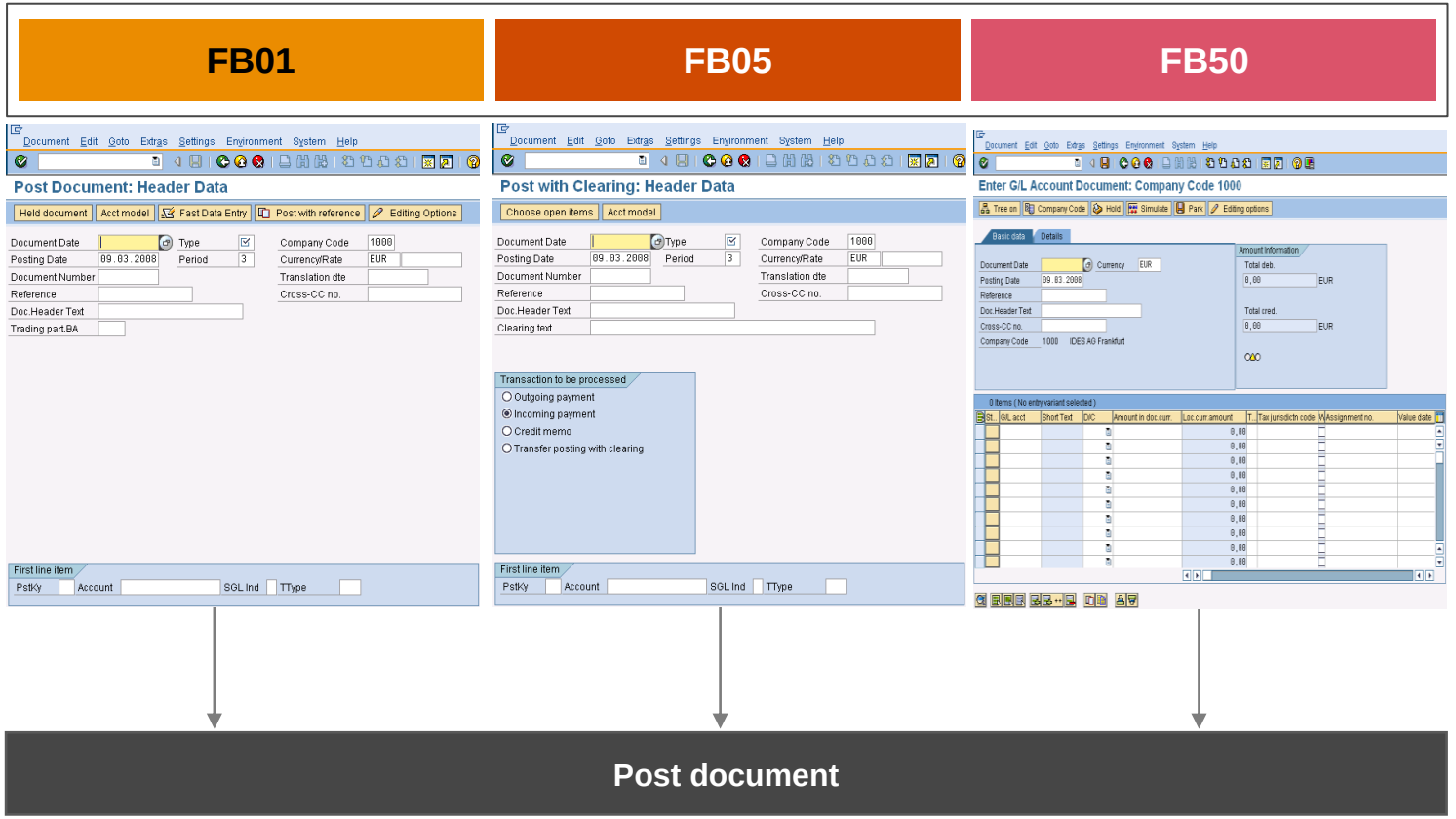
What is a Client?

- Highest organizational level in SAP
- A self-contained commercial, organizational, and technical unit within an SAP System.
- All business data within a client is protected from other clients.
- Each client has its own master data, which can be considered as the exclusive property of this client.



Transaction codes

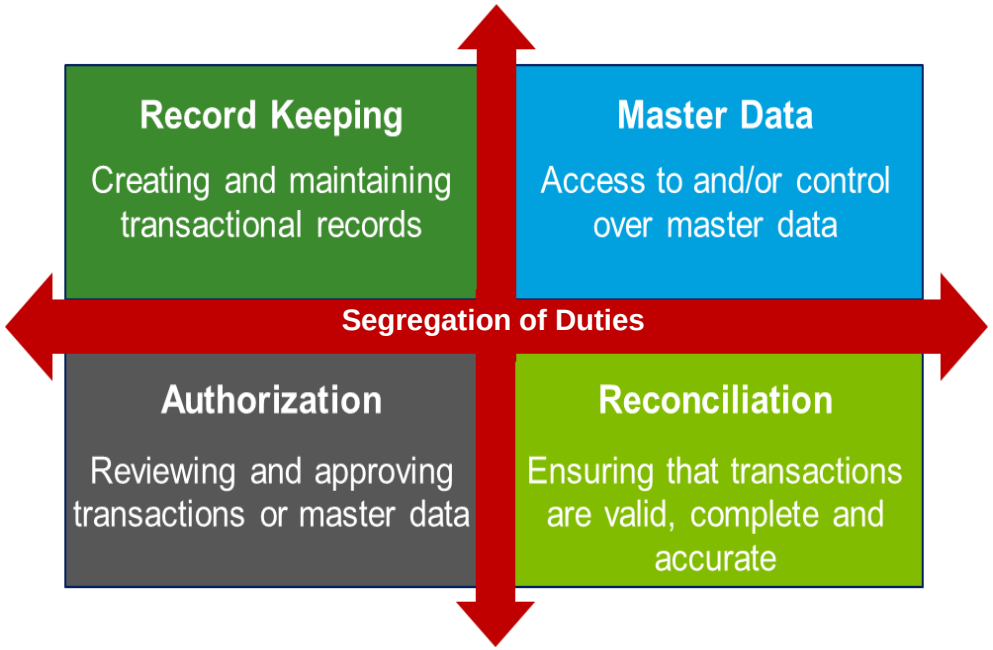
The underlying structure of SAP is a collection of programs which we can directly access through transaction codes ("Tcodes"). TCodes can be either executed directly using the command field or indirectly through on-screen menu path based navigation. In SAP, there are often multiple different transactions that can perform the same function.

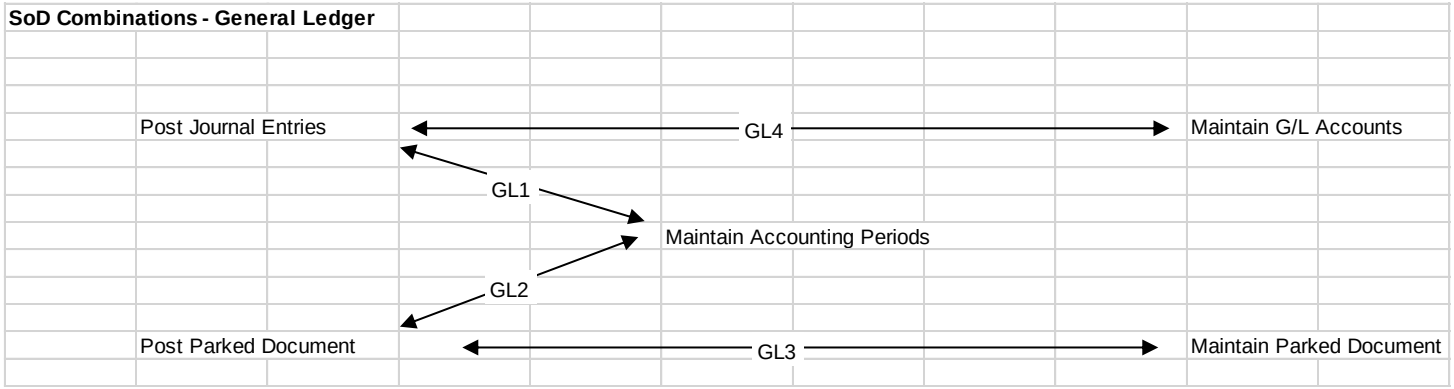


Standard vs. Custom Transactions

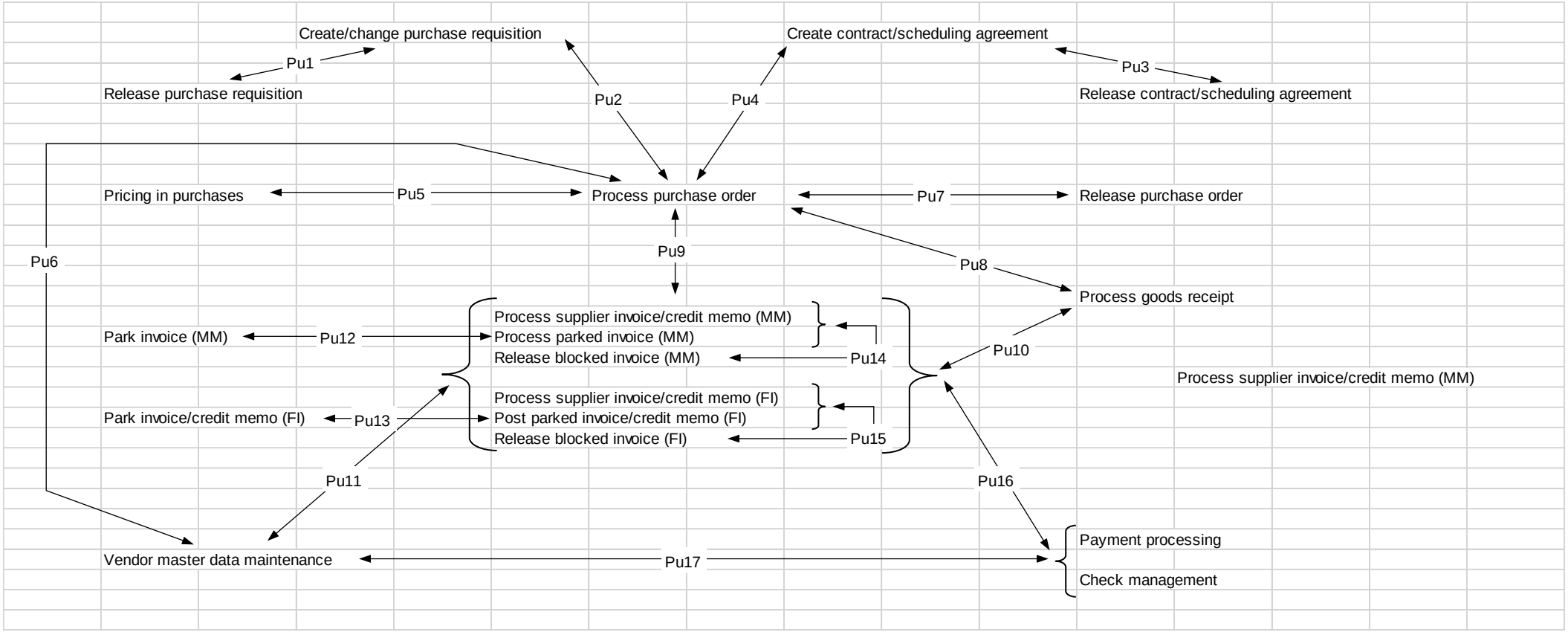
- Custom transactions can be configured to execute custom (i.e., client management developed) programs or to execute standard (i.e., SAP developed) programs.
- Custom TCodes usually begin with Y* or Z*, or can be delivered through a non-SAP namespace that's registered with SAP.
- Custom transactions generally represent a higher security risk.

Segregation of duties is simple

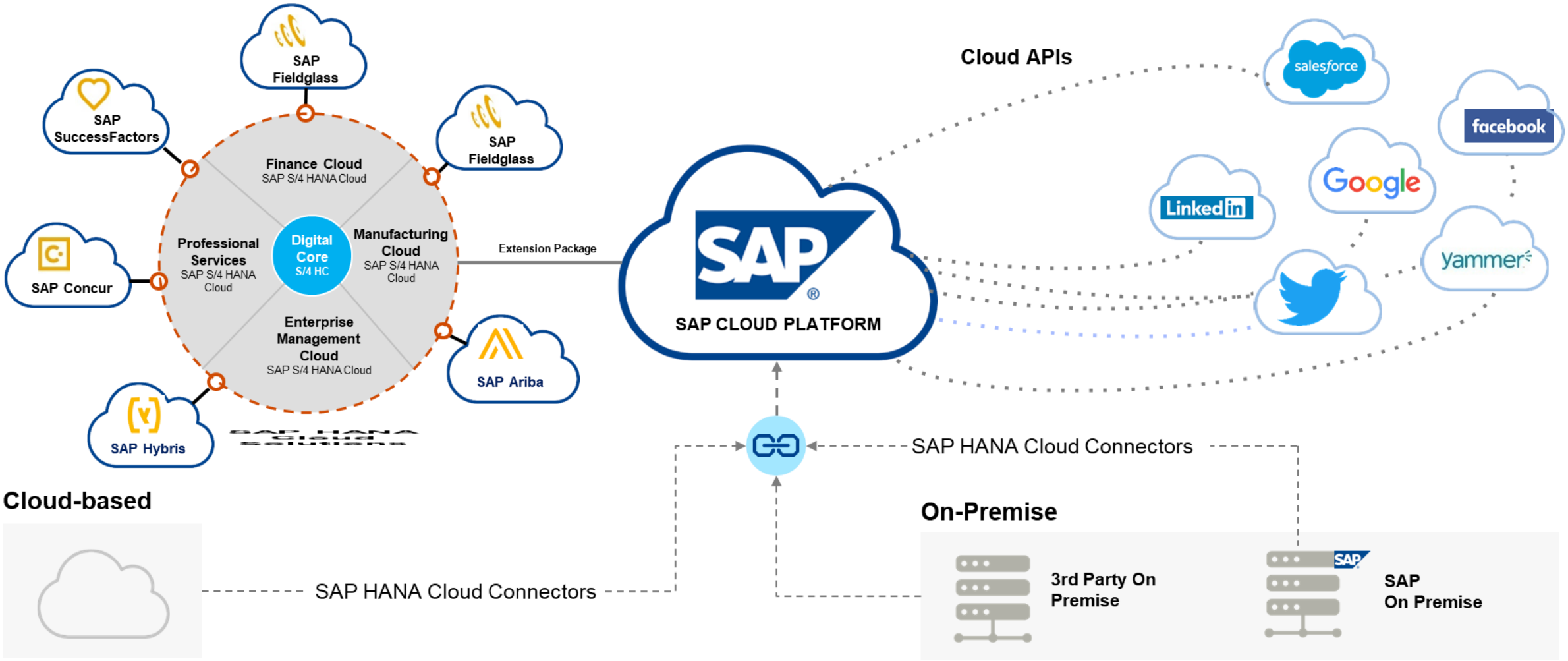




Segregation of duties is complex



Complexity increases with more add-on applications



Risk assessment is key

SoD Risk Assessment

When assessing the risk of any given combination of duties, the potential impact as well as the likelihood of the risk should be considered.

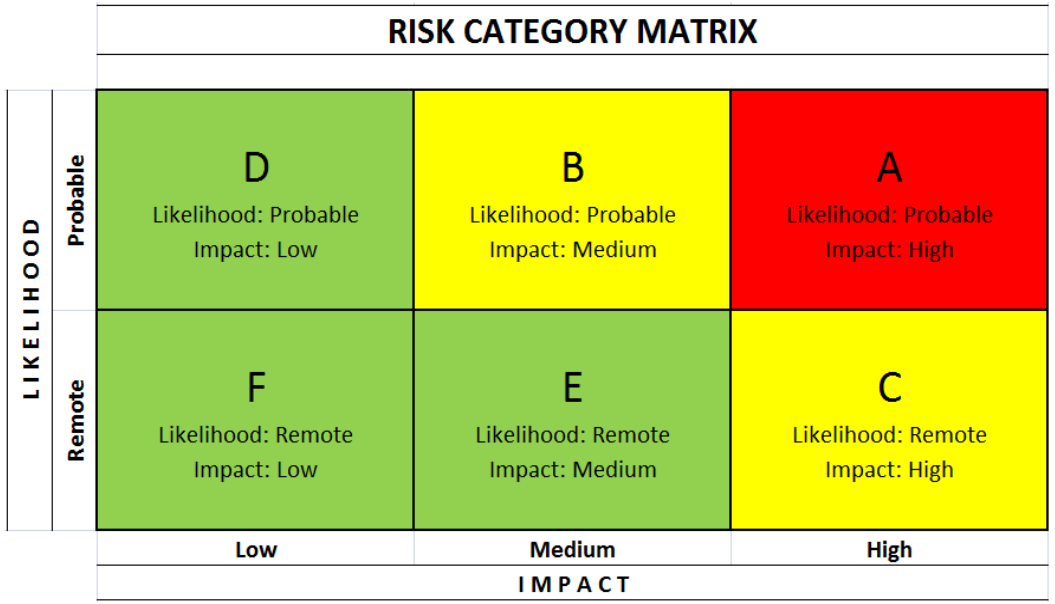
Likelihood
The likelihood that any given combinations of duties will be used by an individual to perpetrate and to conceal errors or fraud in the normal course of their duties is divided into two categories

Likelihood	Description
Probable	The event or events are likely to occur, e.g. if the combinations of duties are easy to exploit for direct or indirect personal gain or if the risk of being caught is low.
Remote	The chance of the event or events occurring is slight, e.g. if the combinations of duties require collusion of others to gain personal benefits or if the risk of being caught is high.

Impact
The potential impact (financial, business, operational etc.), if any given combination of duties is exploited can be divided into three categories:

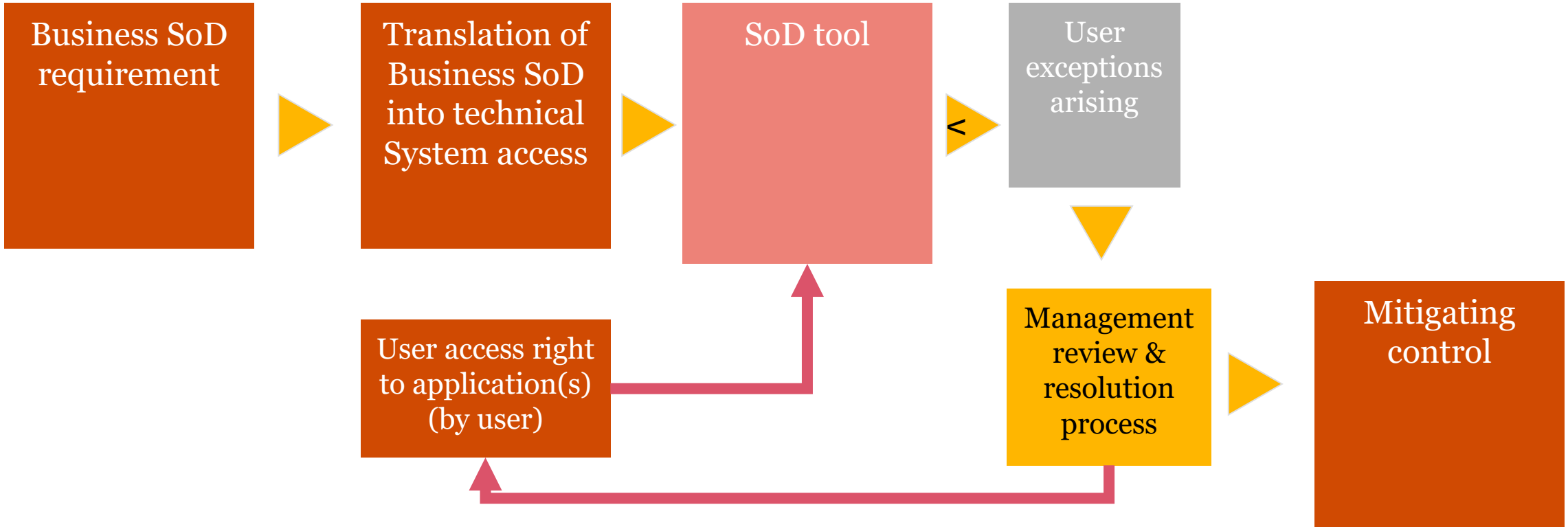
Impact	Description
High	High impact risks may result in significant financial losses due to loss of costly assets, disruption of operations or fraudulent activities etc.
Medium	Medium impact risks may result in financial losses due to loss of assets, disruption of operations or fraudulent activities etc
Low	Low impact risks may result in the loss of some assets or may noticeably affect operations.

Taking likelihood as well as impact into consideration, the following matrix can be used to categorize the risk of any given combinations of duties being exploited:

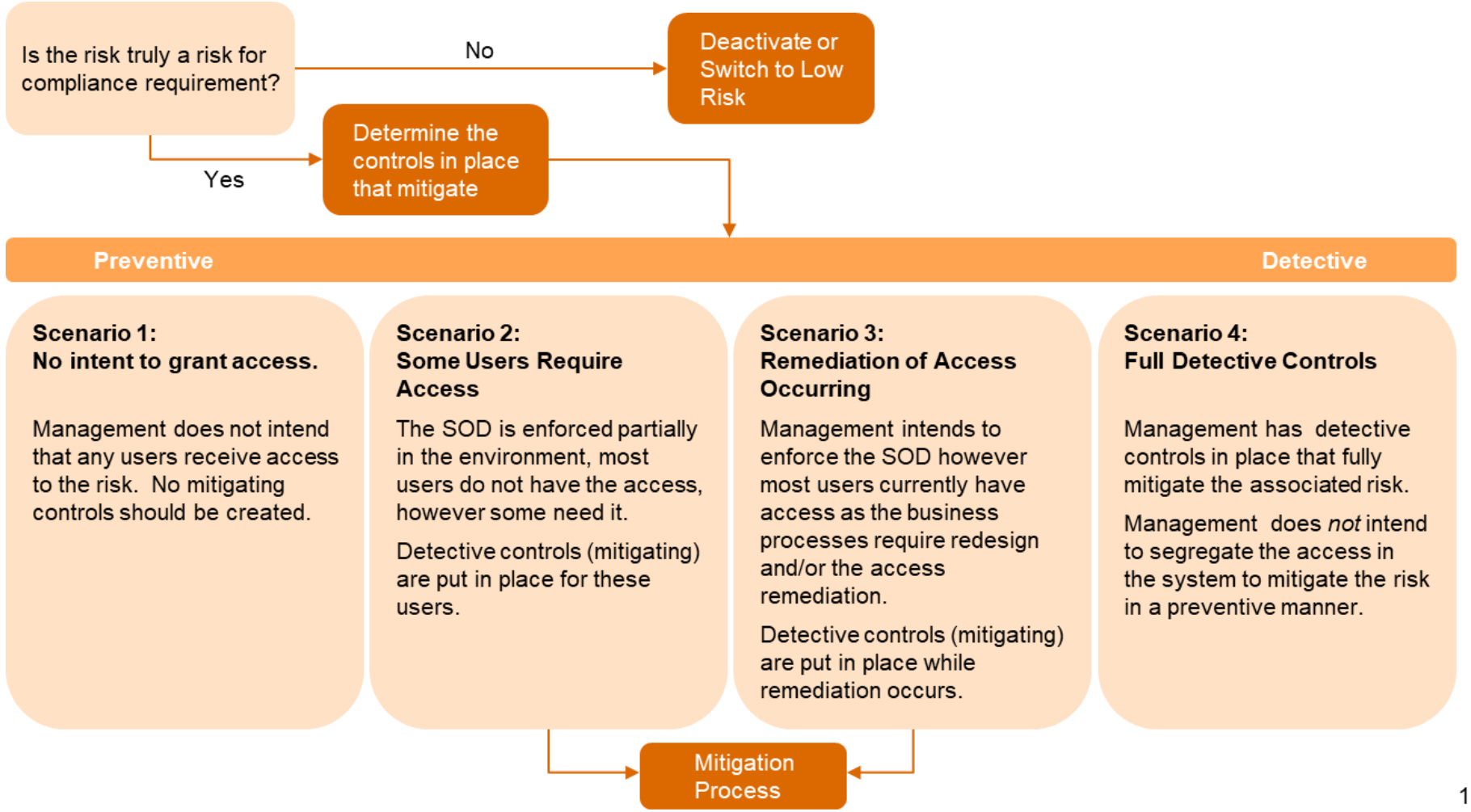


Risk Category	Description
High	High risk SoD conflicts are defined as combinations of duties where the Likelihood is Probable and the Impact is High (Category **A**)
Medium	Medium risk SoD conflicts are defined as combinations of duties were the Likelihood is Probable and the Impact is Medium (Category **B**) or where the Likelihood is Remote and the Impact is High (Category **C**).
Low	Low risk SoD conflicts are defined as combinations of duties were the Likelihood is Probable and the Impact is Low (Category **D**); or duties were the Likelihood is Remote and the Impact is Low or Medium (Categories **E**

Process for handling SoD



Approach to designing mitigating controls



18

3

SoD process supported by tools

TOOL SUPPORT IN AN AUDIT PERSPECTIVE

What to gain from using tools in the preparation for audits?

Support you to

Maturing your compliance processes

What to gain from using tools in the preparation for audits?

- Standardisation of compliance processes
- Organize & mature organisation
- Involve & delegate
- Documentation & structure
- Transparency & information sharing
- Preparation for the audit
- Best practice
- Three line model

Why consider SAP integrated tool for the SoD and IC process?

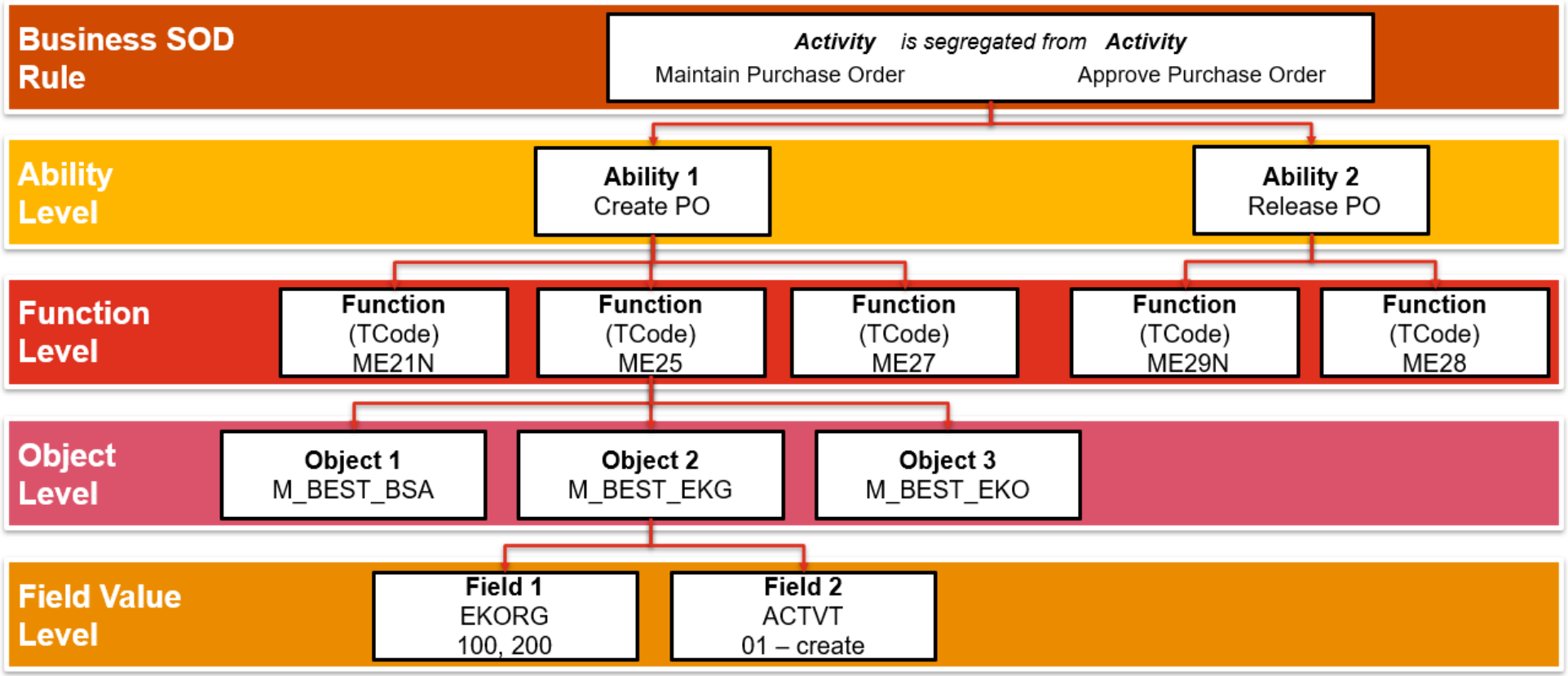
- Many of your key processes are running is SAP
- Preventive SoD in SAP you will need a SAP based tool
- SAP is proven and secure platform
- SAP's user & access management concept
- Confidential / personal / sensitive data (GDPR)

Trends implementing audit tools & consideration for choice of tool?

- **Trends**
- Increasing interest to automate SoD
- Request support in the implementation process
- SoD and Controls part of S/4HANA roadmap
- **Choose the right tool**
- Organization maturity and roadmap?
- Internal competences
- Standard, flexibility and complexity

RISK DEFINITION

Authorizations and Segregation of Duties



RISK DEFINITION

Function A

Payment to Vendor

Function B

Vendor Master Maintain

Function C

Maintain Purchase order

Function D

Vendor Master Maintain

Function E

Payment from Customer

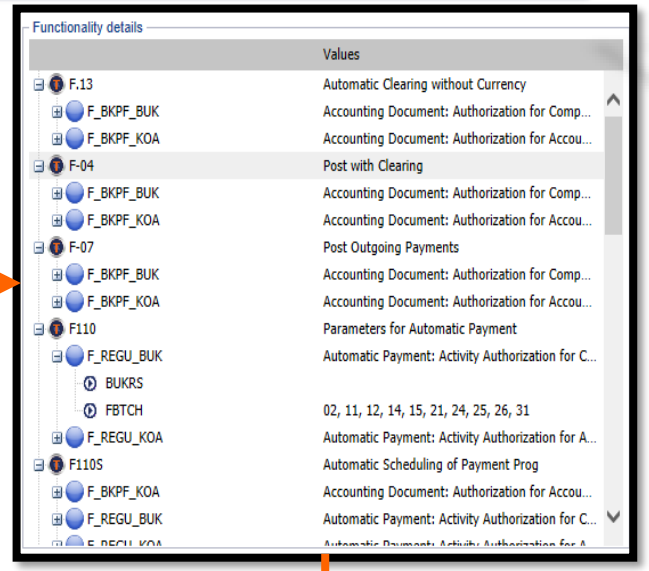
Potential Risk

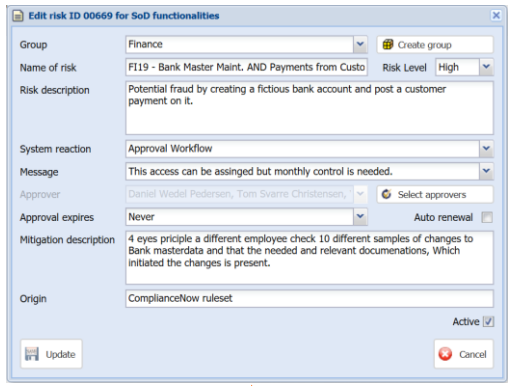
Creating a fictive bank account

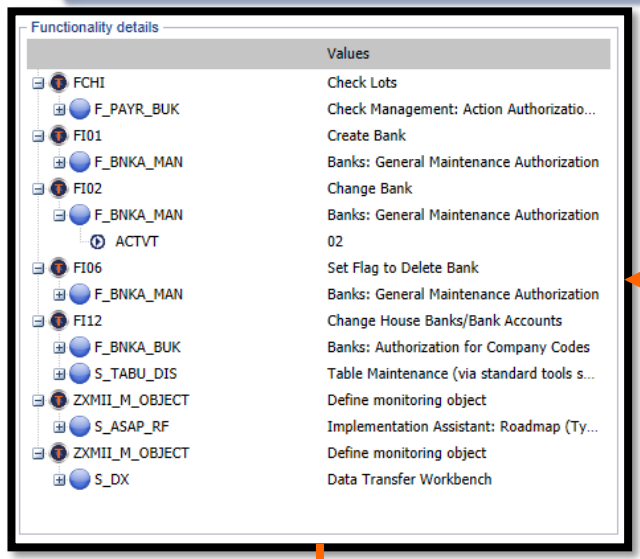
and post a customer payment on it.

Function F

Bank Master Maintenance







FI19 - Bank Master Maint. AND Payments from Customer	Potential fraud by creating a fictious bank account and post a customer payment on it.
FBK02	Bank Master Maintenance
FAR07	Payments from Customer

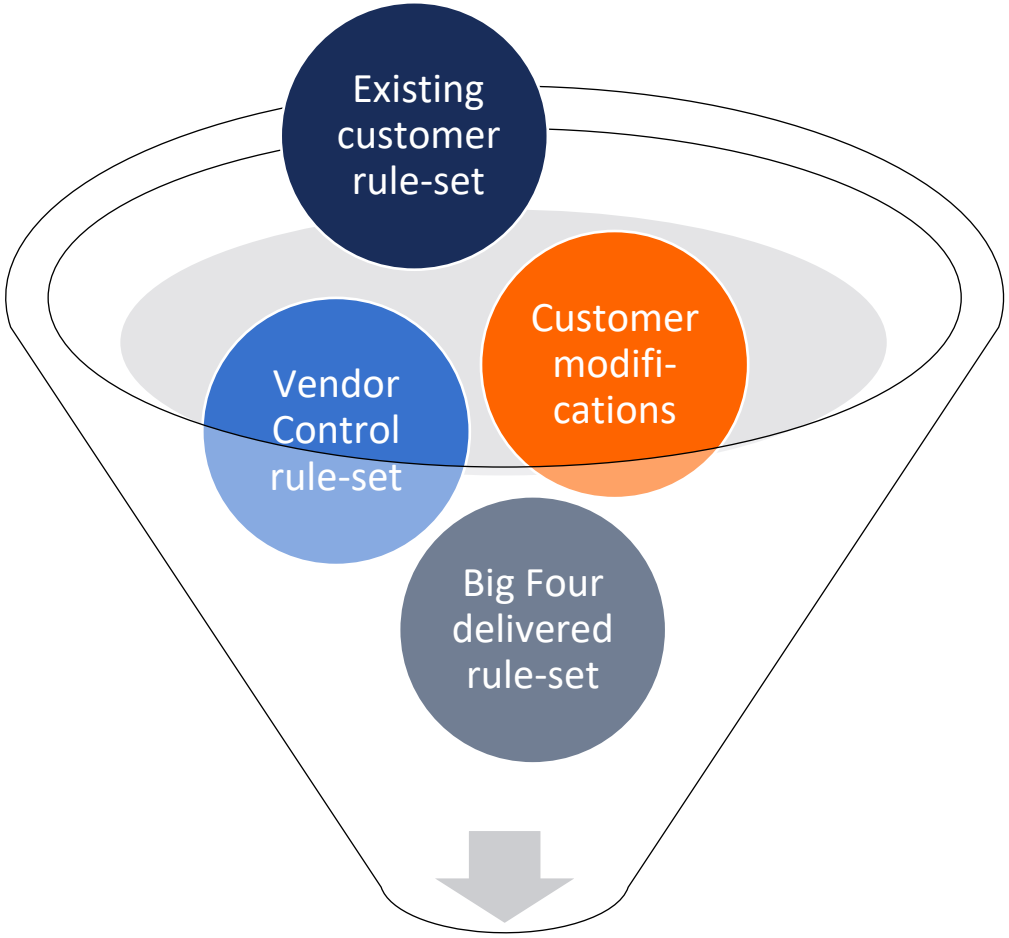
RISK LIBRARY

Tool vendor Baseline Risk Library

- Most important & common risks
- Supporting the core business processes in SAP (Finance, Procure to Pay, Order to Cash, HR & Payroll, Basis & Security)
- Risk library will typically consist of SoD functionalities and critical access
- Continuous being updated – also supporting S/4HANA (Services)
- Avoid the SoD chaos

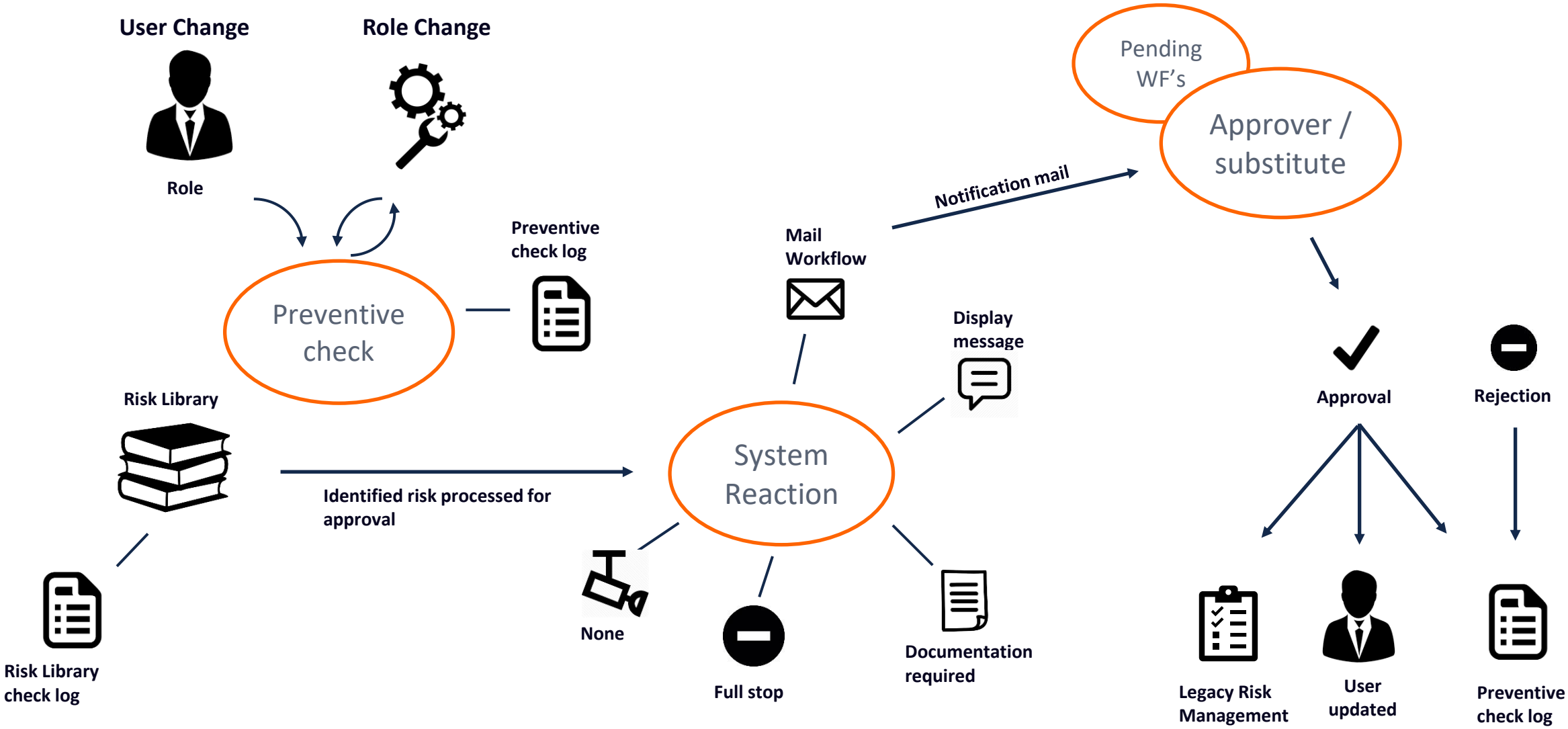
BIG Four Risk Library

- Align with own auditor requirements
- Auditor risk library can typically be integrated in your SoD engine

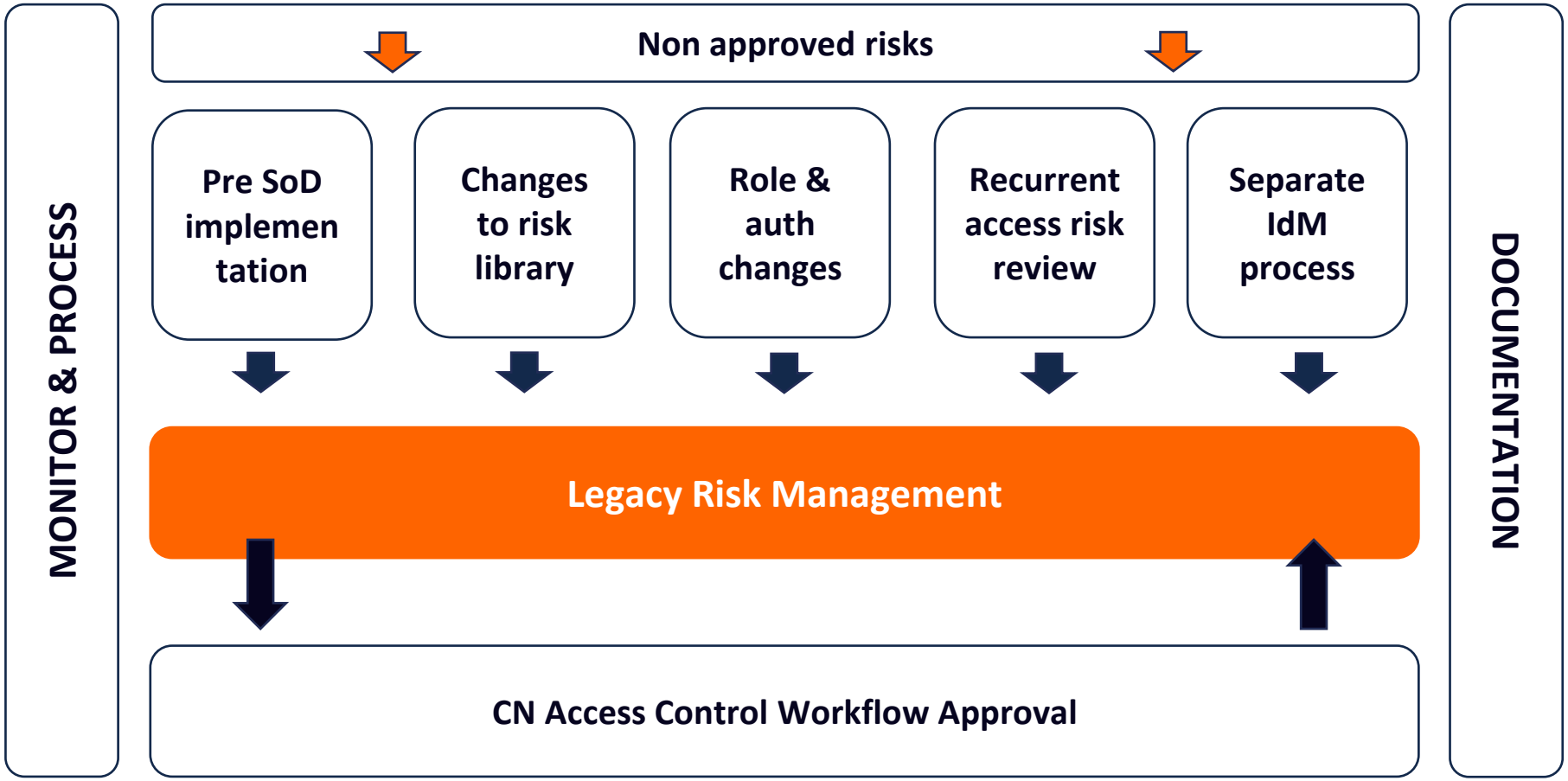


Company specific risk library

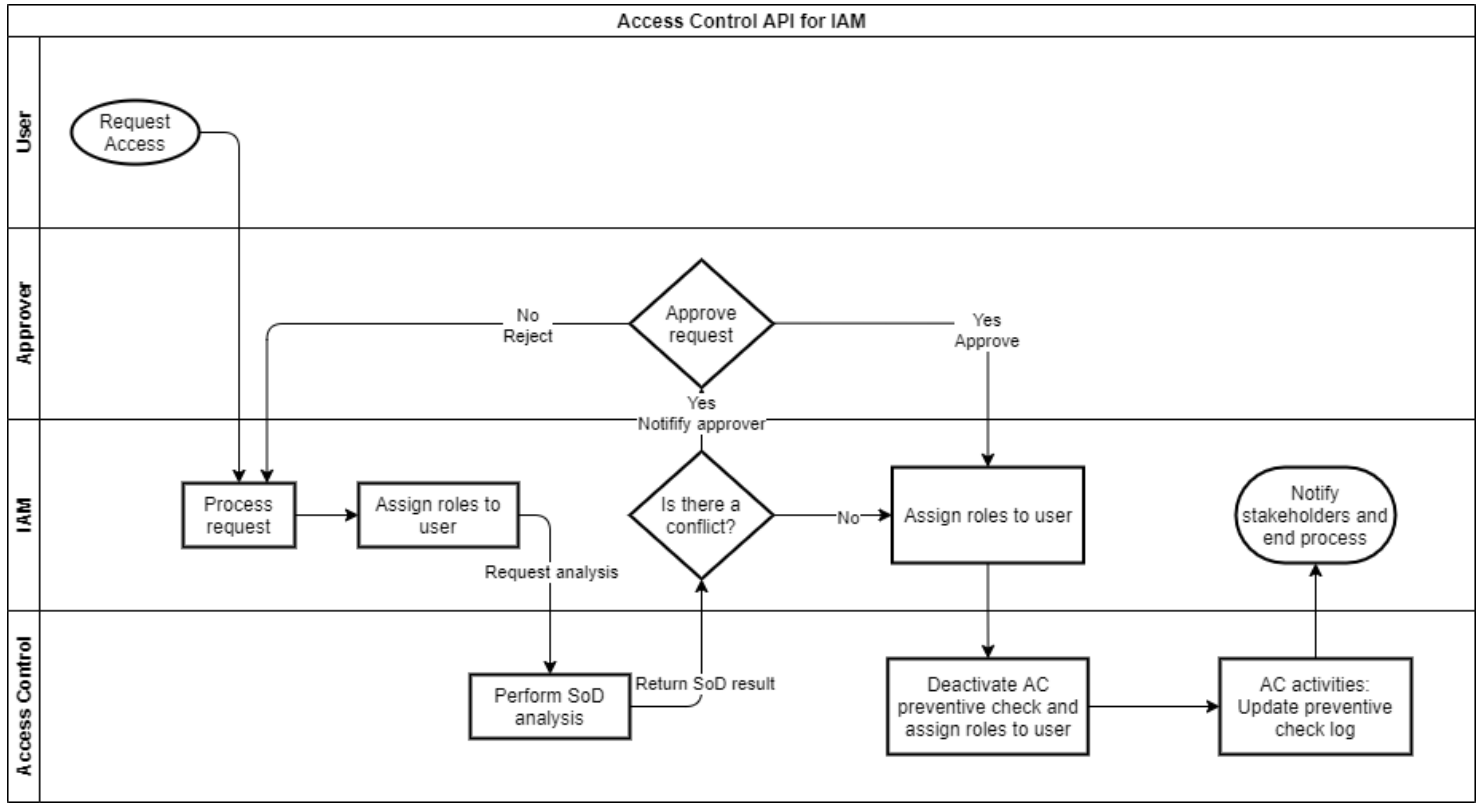
ACCESS CONTROL – PREVENTIVE PROCESS



LEGACY RISK MANAGEMENT



IDM INTEGTEGRATION - IS THIS A GOOD IDEA?



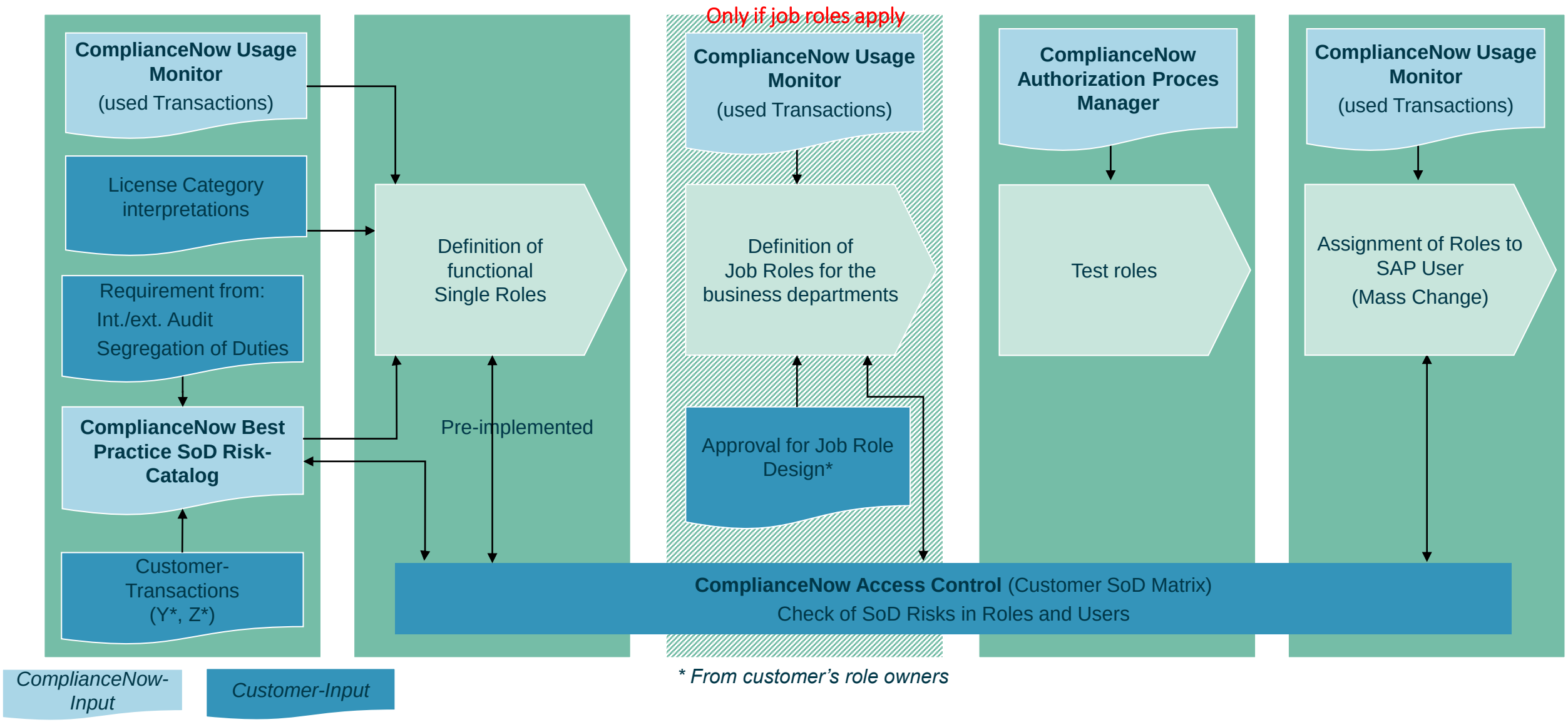
Integration Risk Management (SoD) with User Provisioning

- One guarantee – complexity goes up!
- It is two different needs
  - Access Approval
  - Risk Approval
- Access Approver are not necessary the same as Risk Approver
- Does it have the same urgency for approval?
- Where do you want the risk approval to be executed
  - In IdM or SoD tool?
  - How to handle legacy risk?

4

The SoD method & best practices

1DIGITALTRUST'S SOD METHOD - BEST PRACTICE



SOD PROJECT PLAN EXAMPLE

Activity	Hours Total	Week 1		Week 2		Week 3		Week 4		Week 5		Week 6		Week 7		Week 8		Month 3		Month 4	
Project management (1 day pr. week)																					
Analysis																					
Initial workshop	16																				
Analysis of used transactions on the systems - SOD	40																				
Analysis of used transactions on the systems - GDPR	20																				
User license optimization analysis	40																				
Workshop with business concerning SoD and GDPR risks (FI, HR, Procurement, IT 6 hours each business area)	48																				
Document detailed Authorization Concept	20																				
Design																					
Presentation of Authorization concept incl. SoD and GDPR ruleset	8																				
Development of 16 GDPR roles (3 hours pr. role)	42																				
Development of 14 non SoD roles (3 hours pr. role)	48																				
Development of 40 SoD roles (3 hours pr. role)	120																				
Define processes for license and compliance reporting incl. Housekeeping activities	16																				
Test & Go live - Support																					
User mapping	18																				
User assignment	10																				
Communication to users and stakeholders	8																				
Hyper Care																					
Monthly correction of roles based on auth. Errors from users (16 hours pr. month for 2 month	64																				
Update of Authorization concept	8																				
Total hours	**526**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**			**0**	**0**			**0**	**0**	**0**	**0**

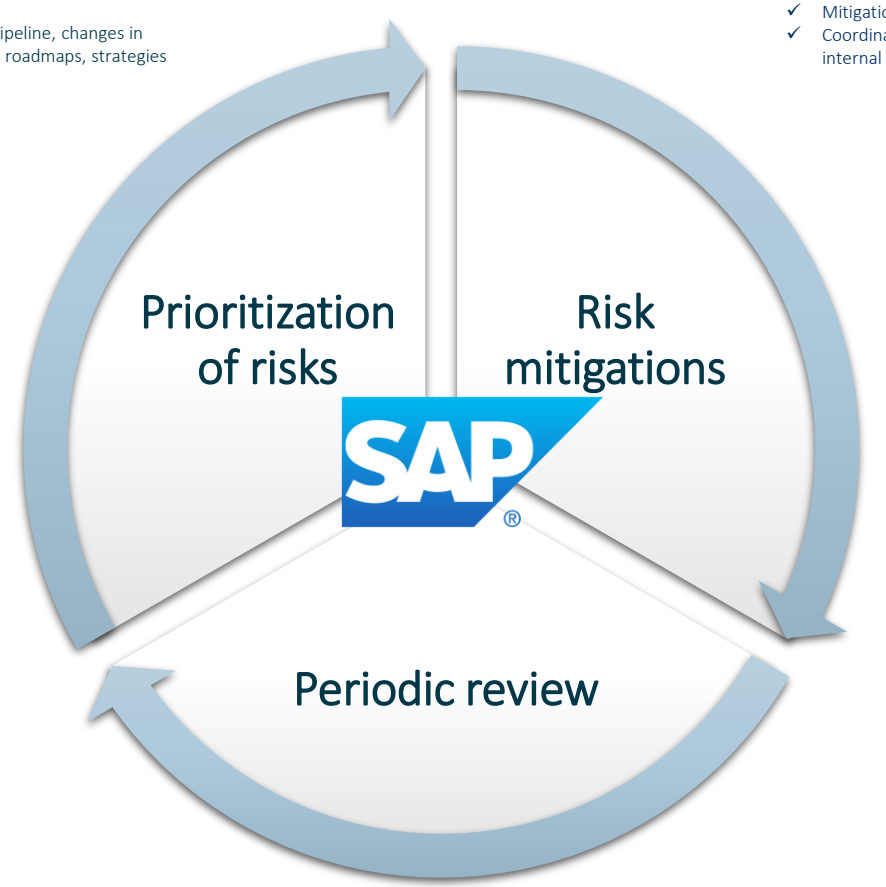
SAP COMPLIANCE PROCESS

Annual Audit report / Risk baseline

- ✓ Identification of risks
- ✓ Estimation on mitigation of risks

Governance model

- ✓ Create or update governance structure and processes
- ✓ How, when, whom?
- ✓ Escalation paths



- ✓ New projects in the pipeline, changes in organization, product roadmaps, strategies

- ✓ Mitigation of prioritized risks
- ✓ Coordination of remediation activities among internal and external stakeholders.

- ✓ Monthly risk report with recommendations and status on ongoing activities.
- ✓ Monthly meeting to align and discuss risks and activities.
- ✓ Changes (organization/processes/usage/new threats)
- ✓ Update of risks and mitigations
- ✓ Update prioritization of risks
- ✓ Update estimation for risk mitigations

THANK YOU

Troels Lindgård
E: troels.lindgaard@1digitaltrust.com
M: +45 5363 5787

1DigitalTrust
www.1DigitalTrust.com

Jesper Parsberg Madsen
E: jesper.parsberg.madsen@pwc.com
M: +45 2141 5985

PwC
www.PwC.dk

Ole Sølvsten Hemmingsen
E: ole.solvsten@compliancenow.eu
M: +45 3053 3920

ComplianceNow
www.complianceNow.eu