



2019

THE ICC, BIRMINGHAM
1-3 DECEMBER

Access Role Management

December 2nd, 2019

ENGAGING MINDS | EMPOWERING SUCCESS

#UKISUGCONNECT

Access Role Management: the most important aspects of Access Control

johan.hermans@csi-tools.com

GDPR

- The European Commissions' regulation for data protection rules (GDPR - General Data Protection Regulation) shall apply from 25 May 2018
- Is nothing new since it replaces 25 local privacy laws
- 4 initial steps
 - Step 1 – Analyze your environment (→ Data Register)
 - Step 2 – Audit who has access to the personal data
 - Step 3 – Remove access to personal data for unauthorized users (→ **Role Concept is needed**)
 - Step 4 – Stay compliant (→ It is not a project)
 - Tip: Deletion of data can be helpful

Role Concept Stakeholders: Their requirements



Roles

Reality

Reporting

1

Roles

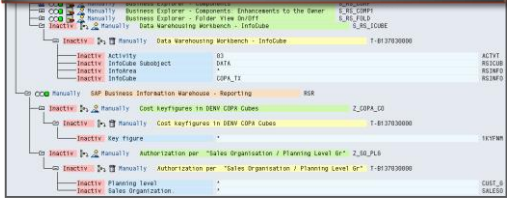
Transactions
URL's
Reports
...

pfcg supc

2

Authorization Button

Auth. Objects + Values

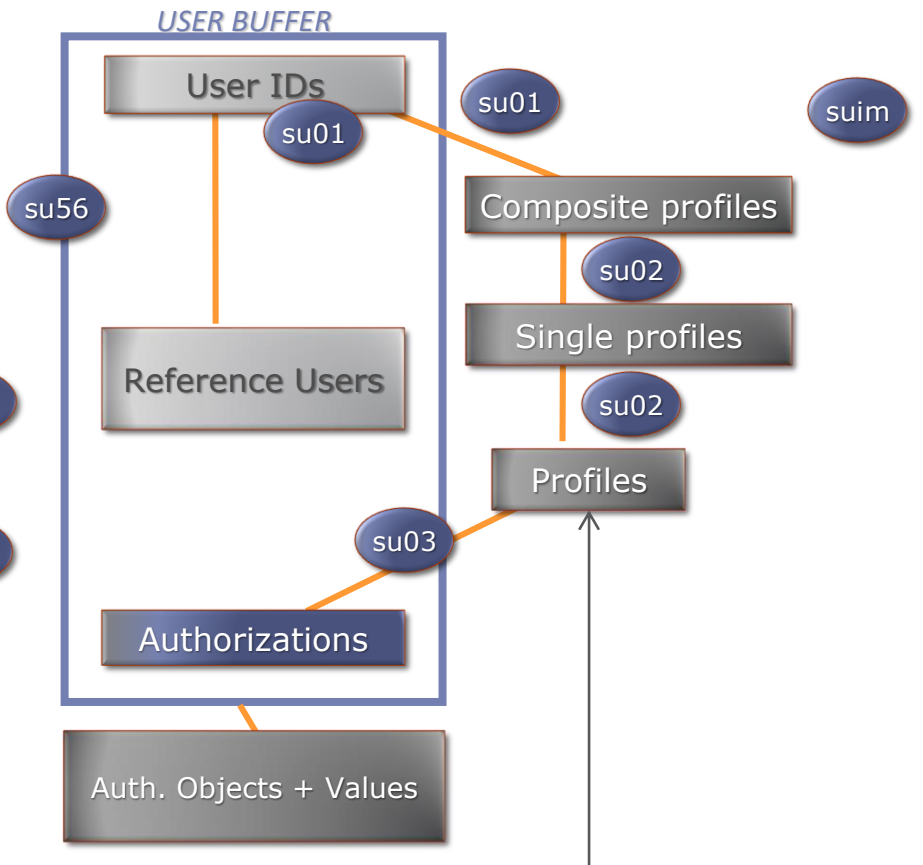


su24

su25

3

"Generate"



AGR* Tables

UST* Tables

USR* Tables

UST* Tables

USH* Tables

Roles can also be used for the user menu

Role Concept Criteria

- User Provisioning
- Role Maintenance
- Overall Transparency
- Ownership

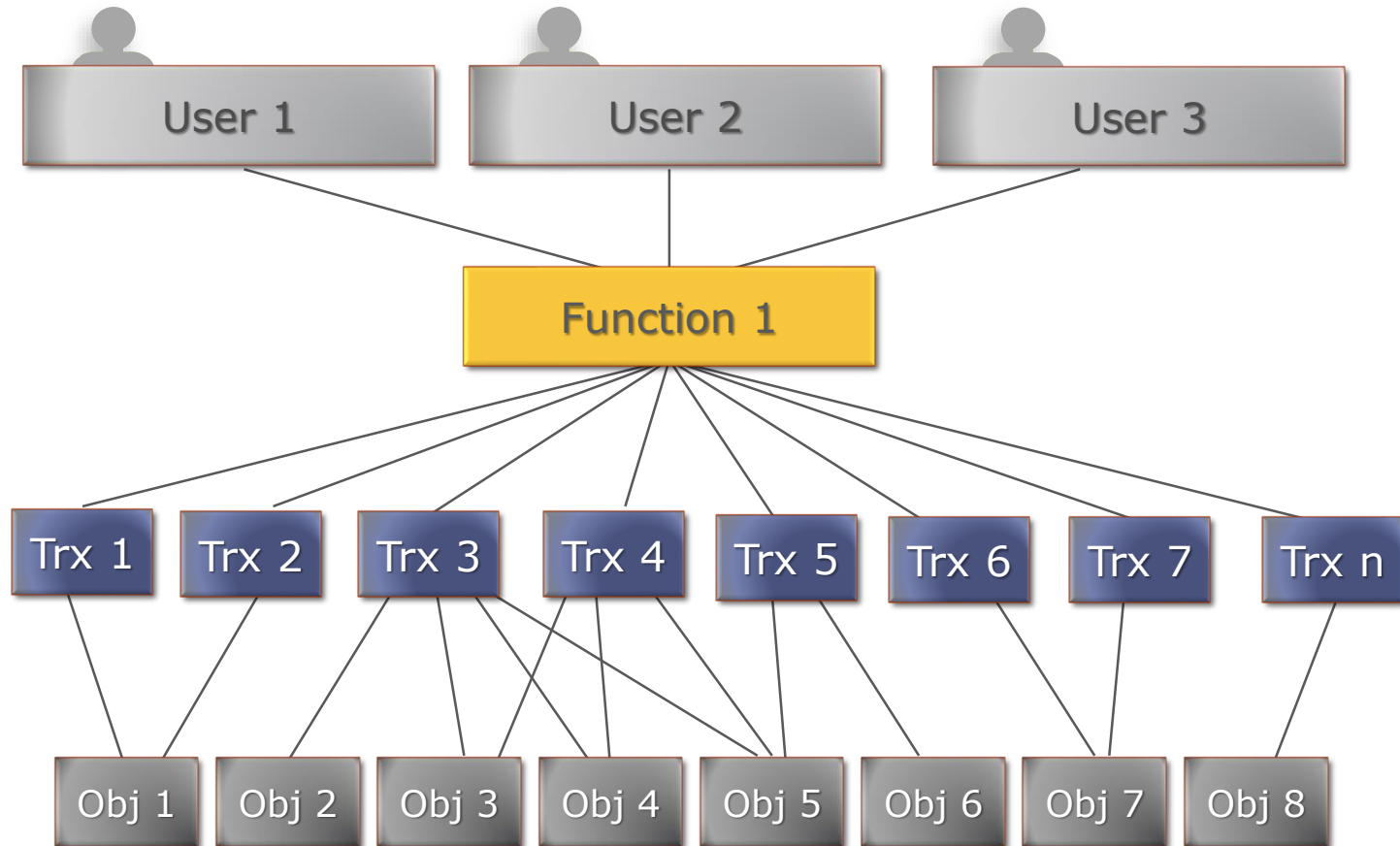
Overview of Authorization Concepts

- One-layered function-based concept
- One-layered task-based concept
- Two-layered function-task-based concept
- Hybrid authorization concept
- Complementary concept

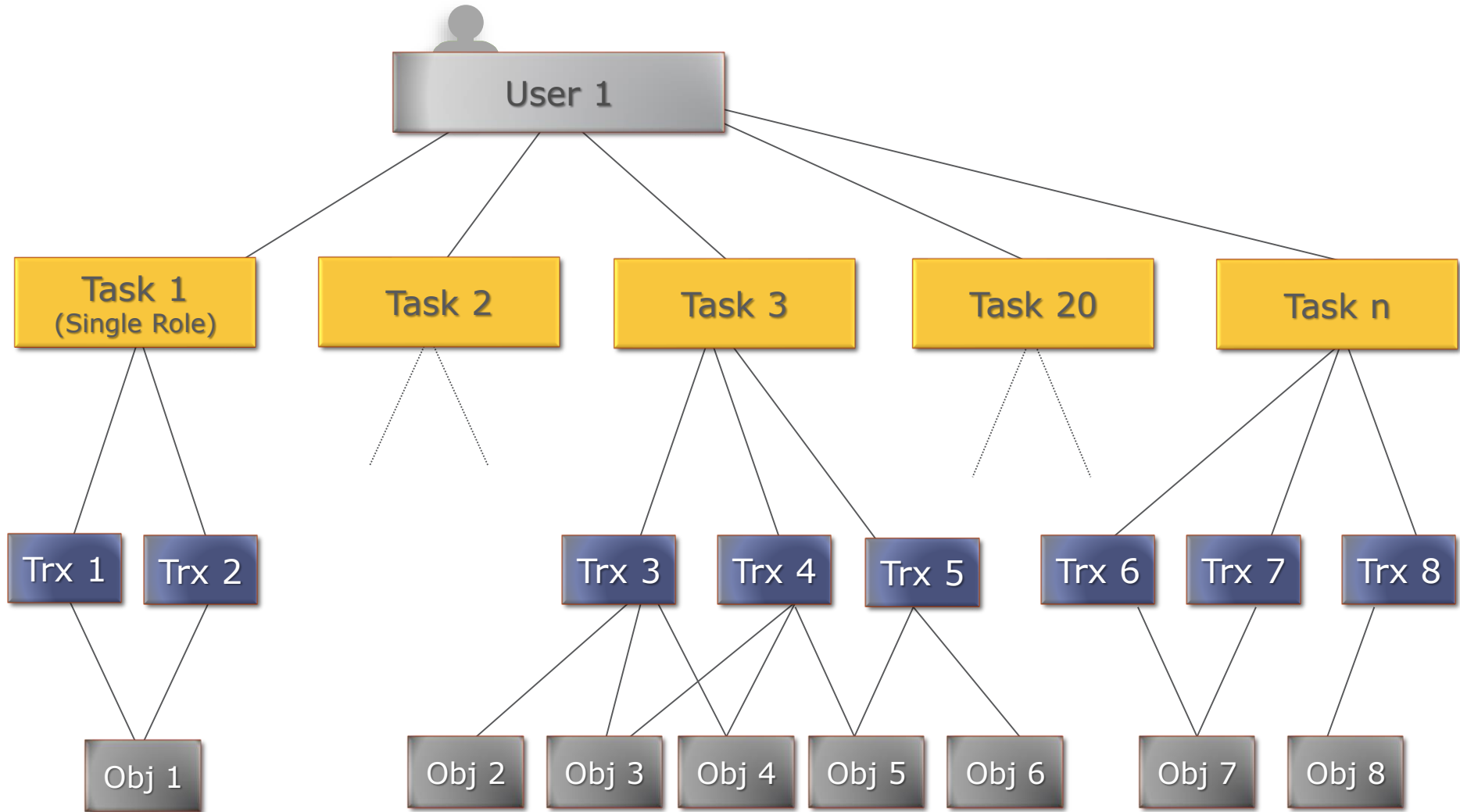
Definition

- Function is for example: sales manager; accounting clerk; ...
- Task is for example: vendor master maintenance; printing; ...

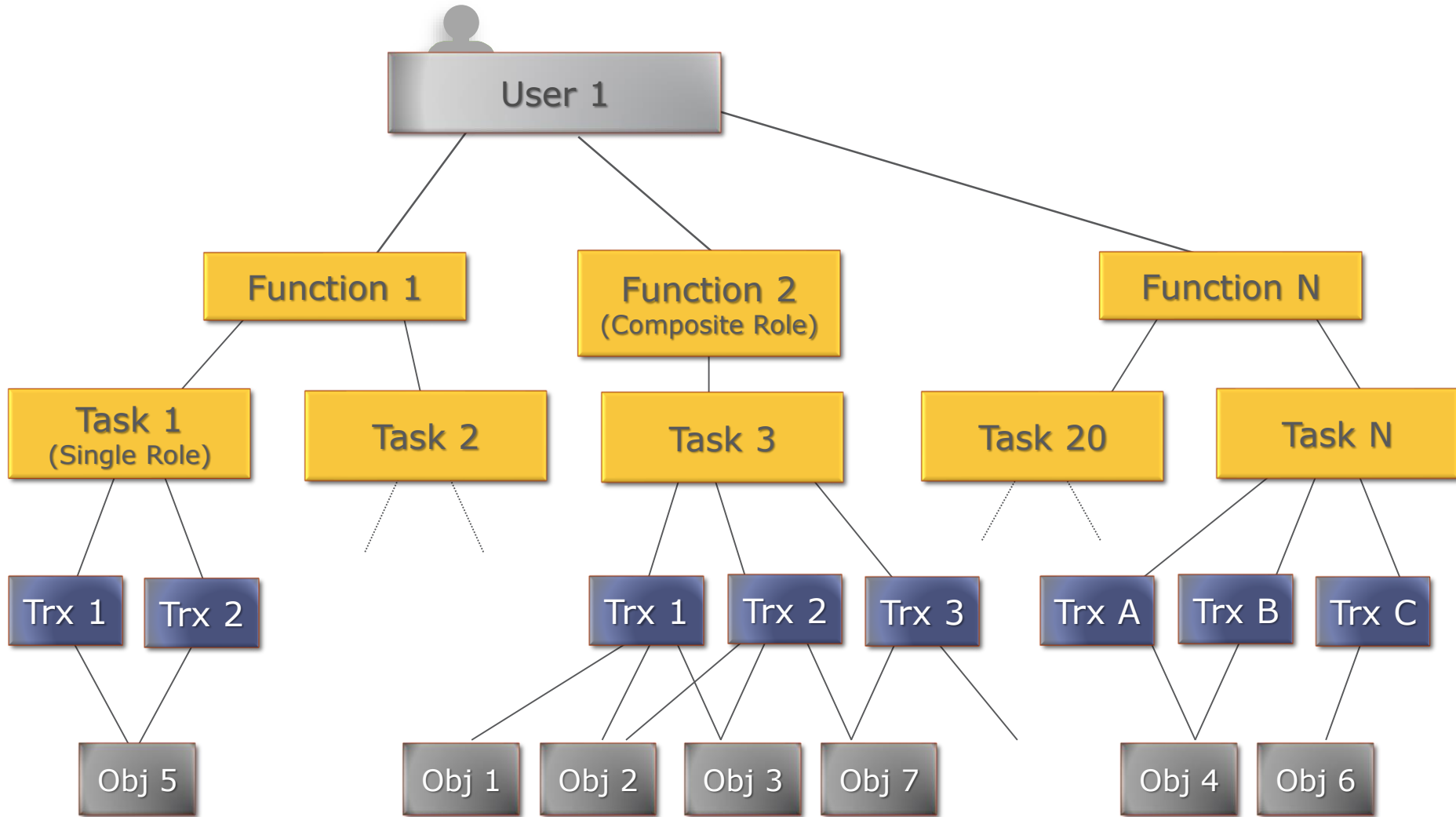
One-Layered Function-Based Concept



One-Layered Task-Based Concept



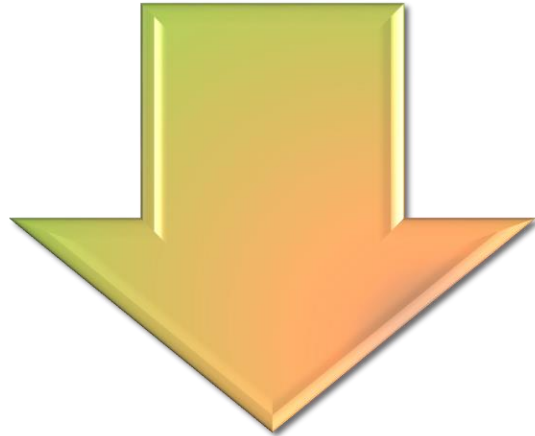
Two-Layered Function-Task-Based Concept



Comparison Authorization Concept Types

Auth. Concept Criterion	One-Layered Function-Based	One-Layered Task-Based	Two-Layered Function-Task
User Provisioning	"Impossible": a change requires modification of the role in development	Difficult: large number of roles	Easy: small number of roles
Role Maintenance	Every change (request) impacts technical layer	Easy: Changes will rather impact user provisioning	Clear split between business responsibility and IT responsibility
Overall Transparency	"Impossible": a function is different per operating company	Transparent: content of a role is clear	Single role ~ one sub-process / composite role ~ business function
Ownership	Mixed Ownership	Easy on data \ business process level;	Easy on data \ business process level; Easy on user level

Role Concept Considerations



Building a **Role** is Easy

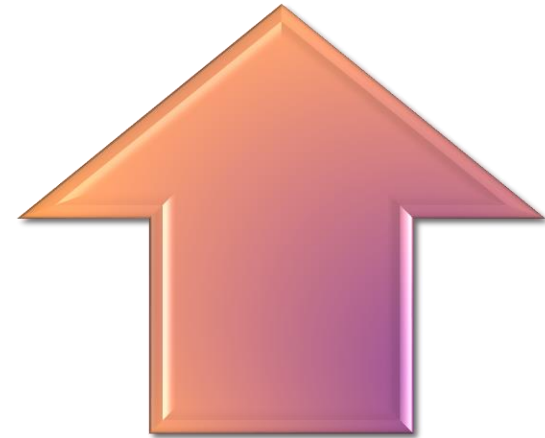
- Open PFCG
- Define Role
- Add transaction
- Set authorization objects
- Generate
- Transport across



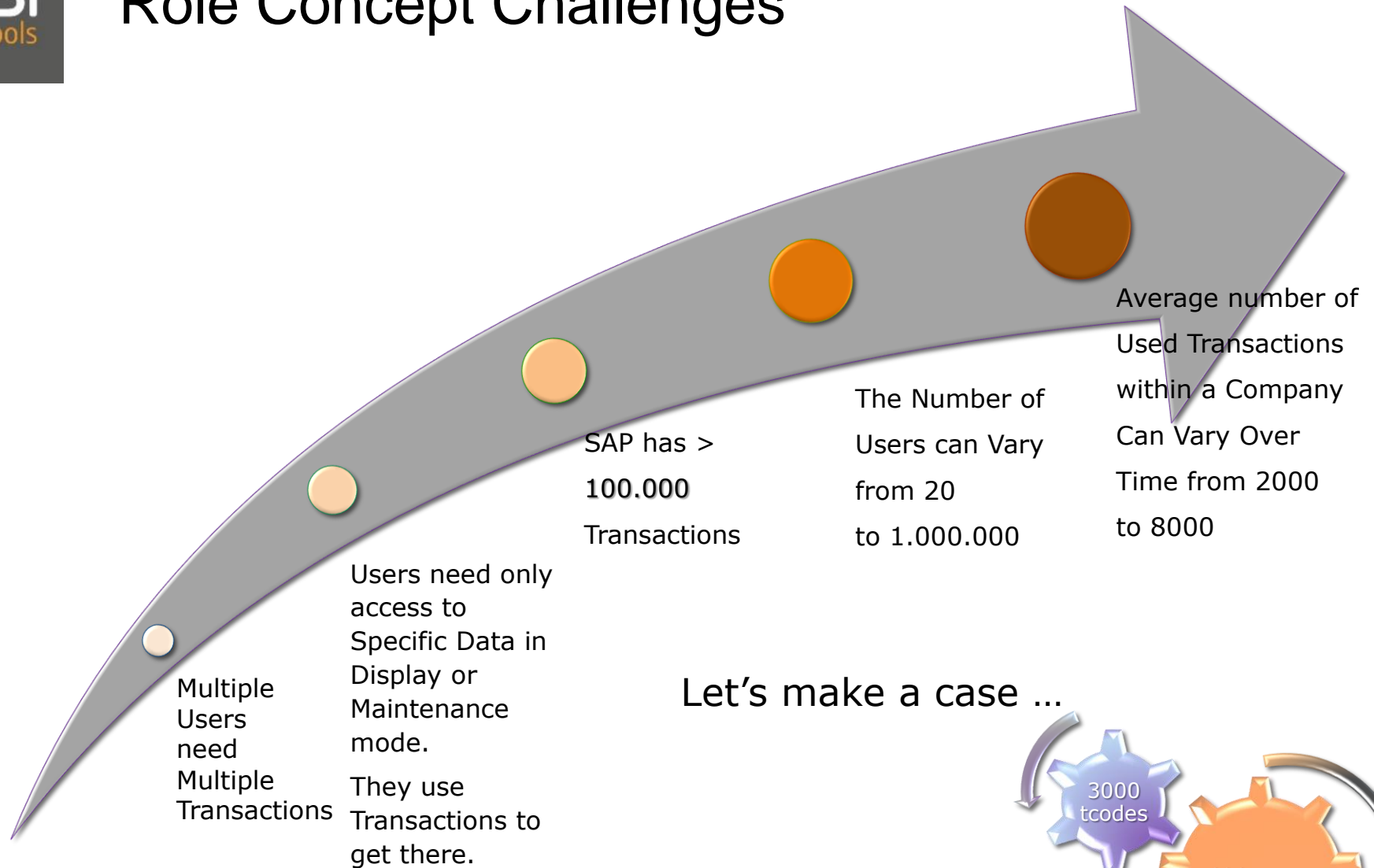
Building a **Concept** is Difficult

Being In Control of

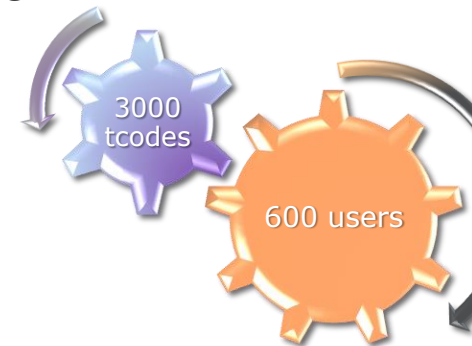
- Access Rights and Provisioning
- Change Management
- Anticipating Change
- Coping with Technical & Functional Constraints



Role Concept Challenges

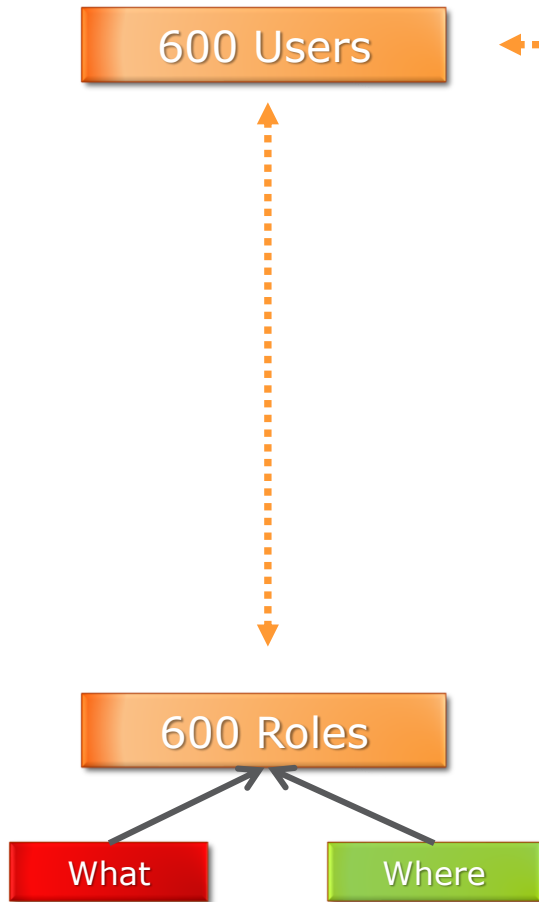


Let's make a case ...

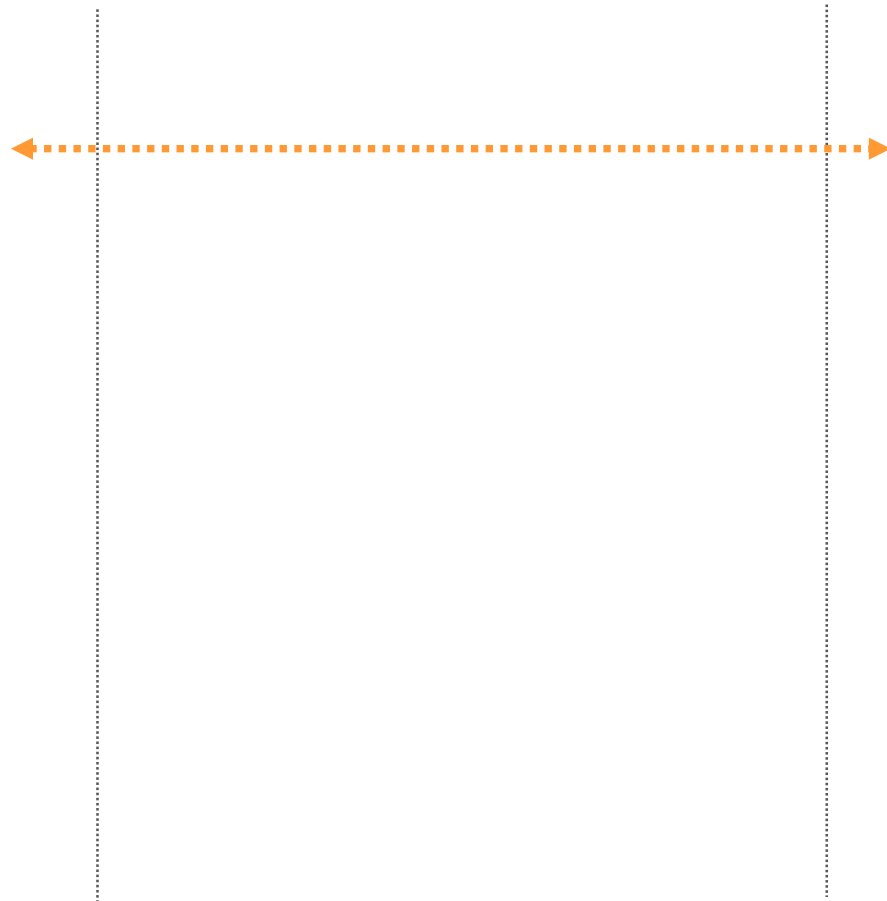
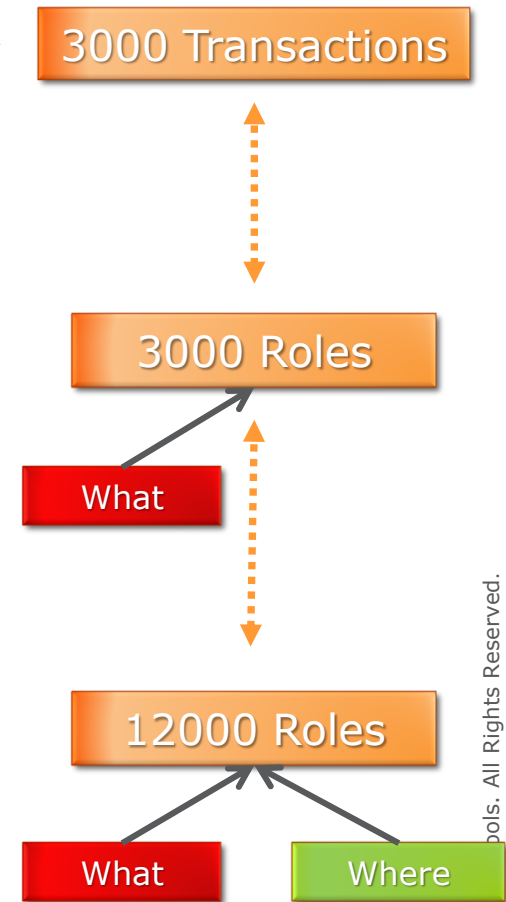


Possible Scenarios : Extreme Cases

Organizational



Technical



Possible Scenarios : 1 Role per User



	Advantages	Disadvantages
Technical	Easy to Build: Group Transactions and Create Role	Cannot Separate "create for company code 1000" and "display for company code 3000" without breaking PFCG best practices
Functional	Nice Overview of all Transactions per User	<ul style="list-style-type: none"> • No automated user provisioning is possible • Nightmare from change management perspective • Grouping is needed for S/4HANA • Unclear ownership (access to multiple (sub)processes and organizational data in one the role) • SoD Rules Changes have major impact on the roles

Possible Scenarios : 1 Role per Transaction

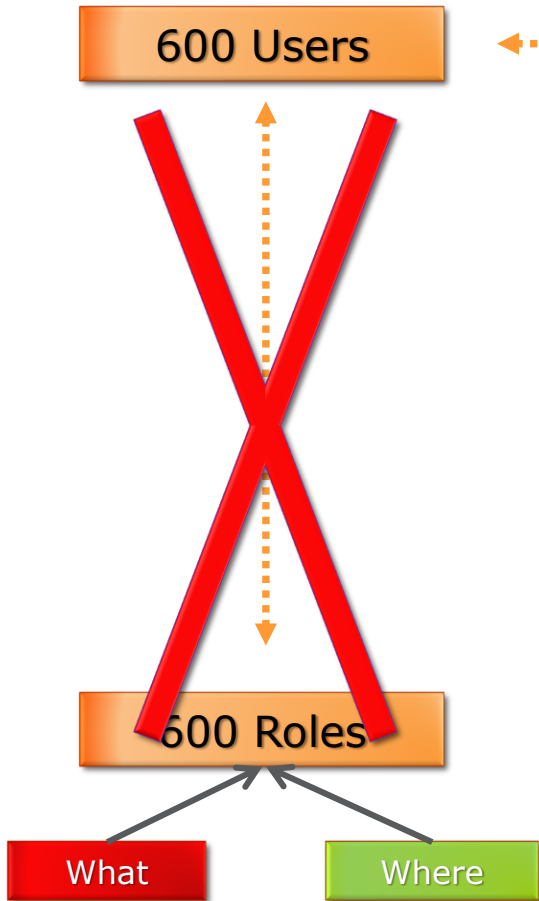


	Advantage	Disadvantage
Technical	Very easy to build: put each transaction in separate role	<ul style="list-style-type: none"> Huge Amount of Roles to initially create and to maintain after data restriction changes User cannot have not more than 300 assigned roles (*)
Functional	Very transparent: all is at user assignment level	<ul style="list-style-type: none"> Grouping is needed for S/4HANA No automated user provisioning is possible Nightmare from change management perspective Heavy User Request Procedure: user needs to request 300 to 400 roles and does not have this knowledge

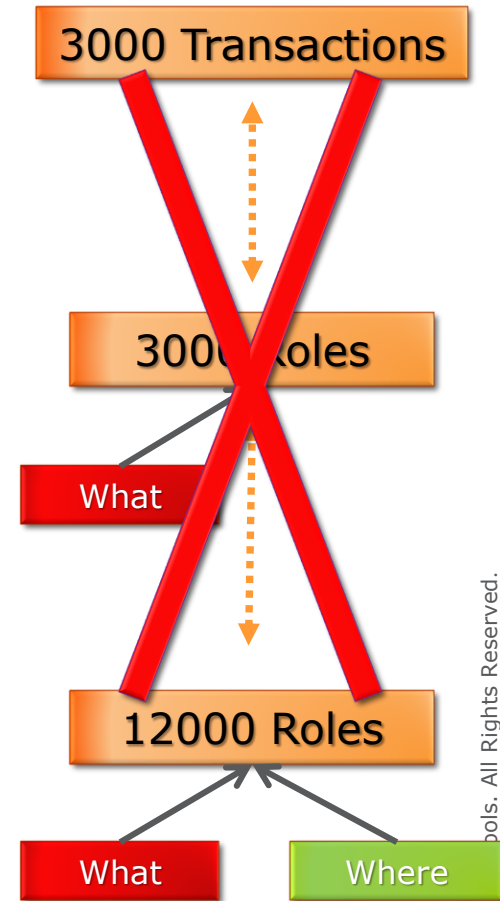
(*) Simplified: real limit is 312 profiles in user-id, unless OSS note is implemented

Possible Scenarios : Solution in Between

Organizational

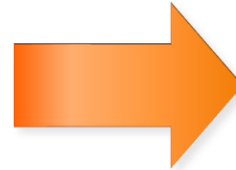


Technical



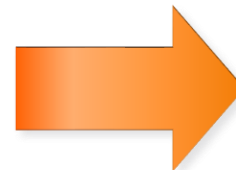
Possible Scenarios: Intermediate Conclusion

A SAP role concept is built based on the technical view



Grouping of transactions is needed

A SAP role concept is built based on the organizational view



Roles should be transparent for business, easy-to-manage and flexible

Intelligent grouping of transactions and authorizations is needed

Try to Group 2 Transaction Codes in 1 Role

Create vendor for company code 1000

Display all A/P postings



```

F_LFA1_APP    ACTVT    01
F_LFA1_APP    APPKZ    F
F_LFA1_BUK    ACTVT    01
F_LFA1_BUK    BUKRS    $BUKRS
F_LFA1_GEN    ACTVT    01
F_LFA1_GRP    ACTVT    01
F_LFA1_GRP
    
```

```

F_BKPF_BUK    ACTVT    03
F_BKPF_BUK    BUKRS    $BUKRS
F_BKPF_KOA    ACTVT    03
F_BKPF_KOA    KOART    K
    
```

\$BUKRS = 1000

\$BUKRS = *

create vendor for company code 1000 and display all A/P postings

What

Where

```


F_LFA1_APP    ACTVT    01
F_LFA1_APP    APPKZ    F
F_LFA1_BUK    ACTVT    01
F_LFA1_BUK    BUKRS    $BUKRS
F_LFA1_GEN    ACTVT    01
F_LFA1_GRP    ACTVT    01
F_LFA1_GRP

F_BKPF_BUK    ACTVT    03
F_BKPF_BUK    BUKRS    $BUKRS
F_BKPF_KOA    ACTVT    03
F_BKPF_KOA    KOART    K
    
```

\$BUKRS = ????

Different Business Processes
use Same Master Data:
so process based grouping
is NOT the Solution

Possible Scenarios : Data Level Based !

- 9 for posting FI documents → F_BKPF_...
 - 9 for vendor master data → F_LFA1_...
 - 9 for customer master data → F_KNA1_...
 - 24 for material master data → M_MATE_...
 - 2 for payments → F_REGU_...
-
- 1.200 objects are grouped into → 300
- 

Example: company code BUKRS

Your authorizations requirements
need to be simplified into 300 one-liners

Possible Scenarios: Data Level Based?



Post FI docs: FB01

F_BKPF_... ACTVT 01
BUKRS 1000

Display vendor master data

F_LFA1_... ACTVT 03
BUKRS *

Display material master

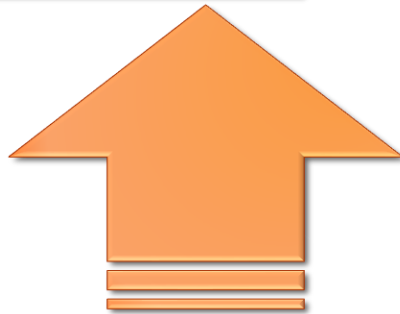
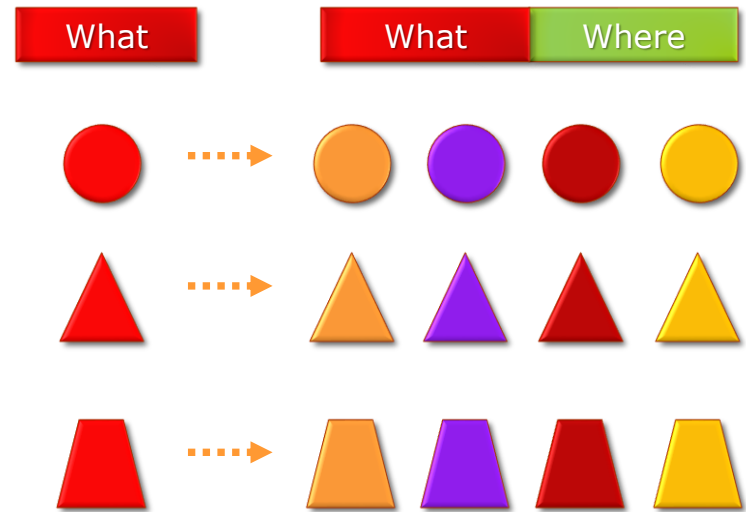
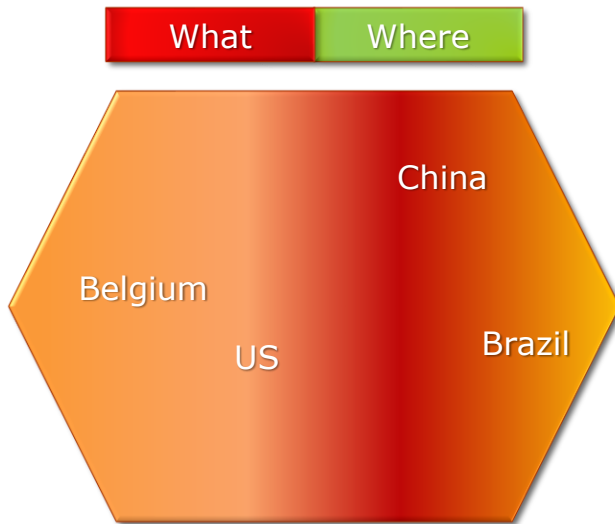
M_MATE_... ACTVT 03
WERKS 3000

Update customer master data

F_KNA1_... ACTVT 02
BUKRS 2000

Full Flexibility on **What** and **Where**

More Roles but Much Less Work



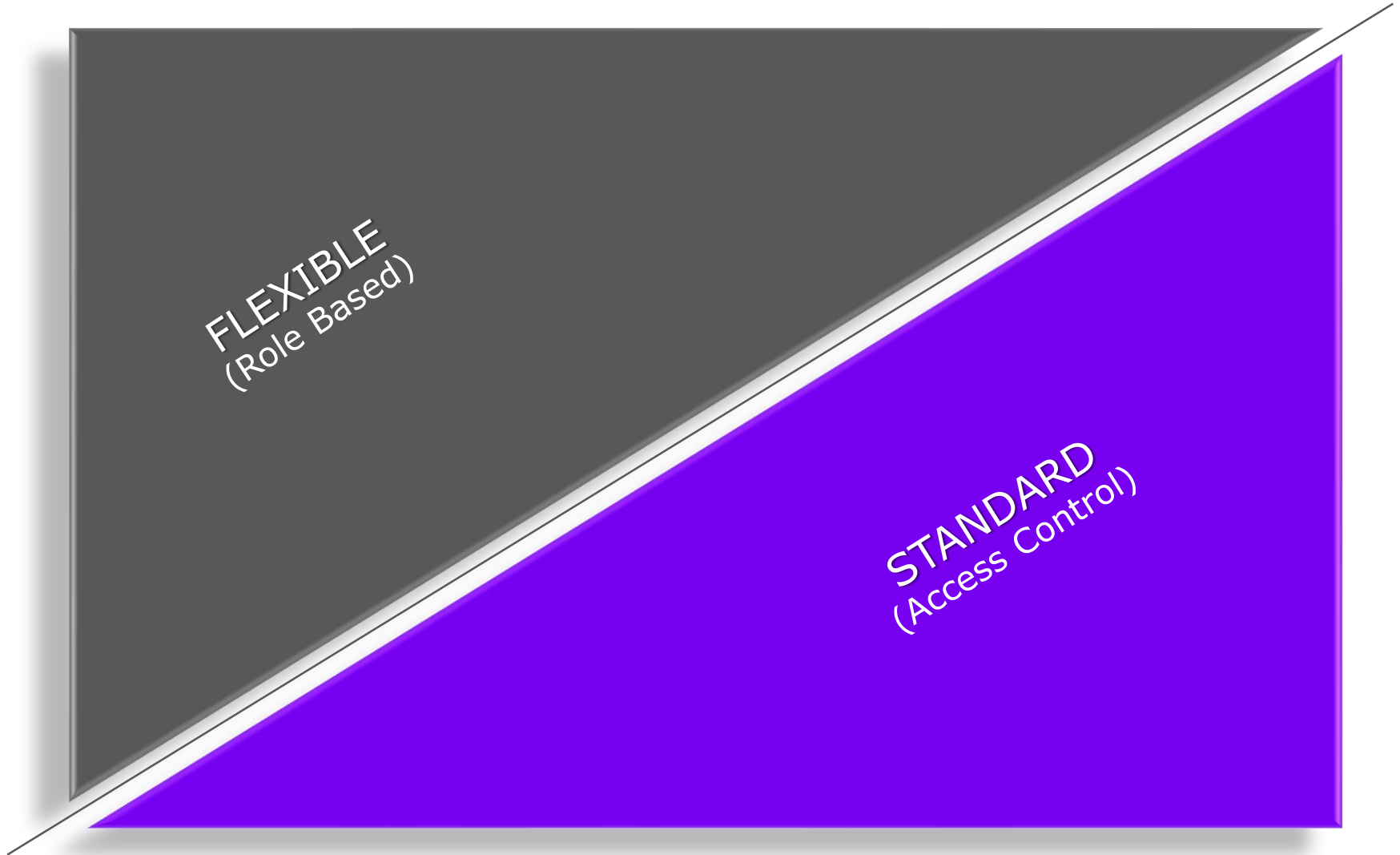
Upgrade SAP	Changed buss. reqs	Changed organization
New SAP module	Changed SoD rules	New affiliates
New legislation: GDPR		

Possible Scenarios: Best of Both Worlds

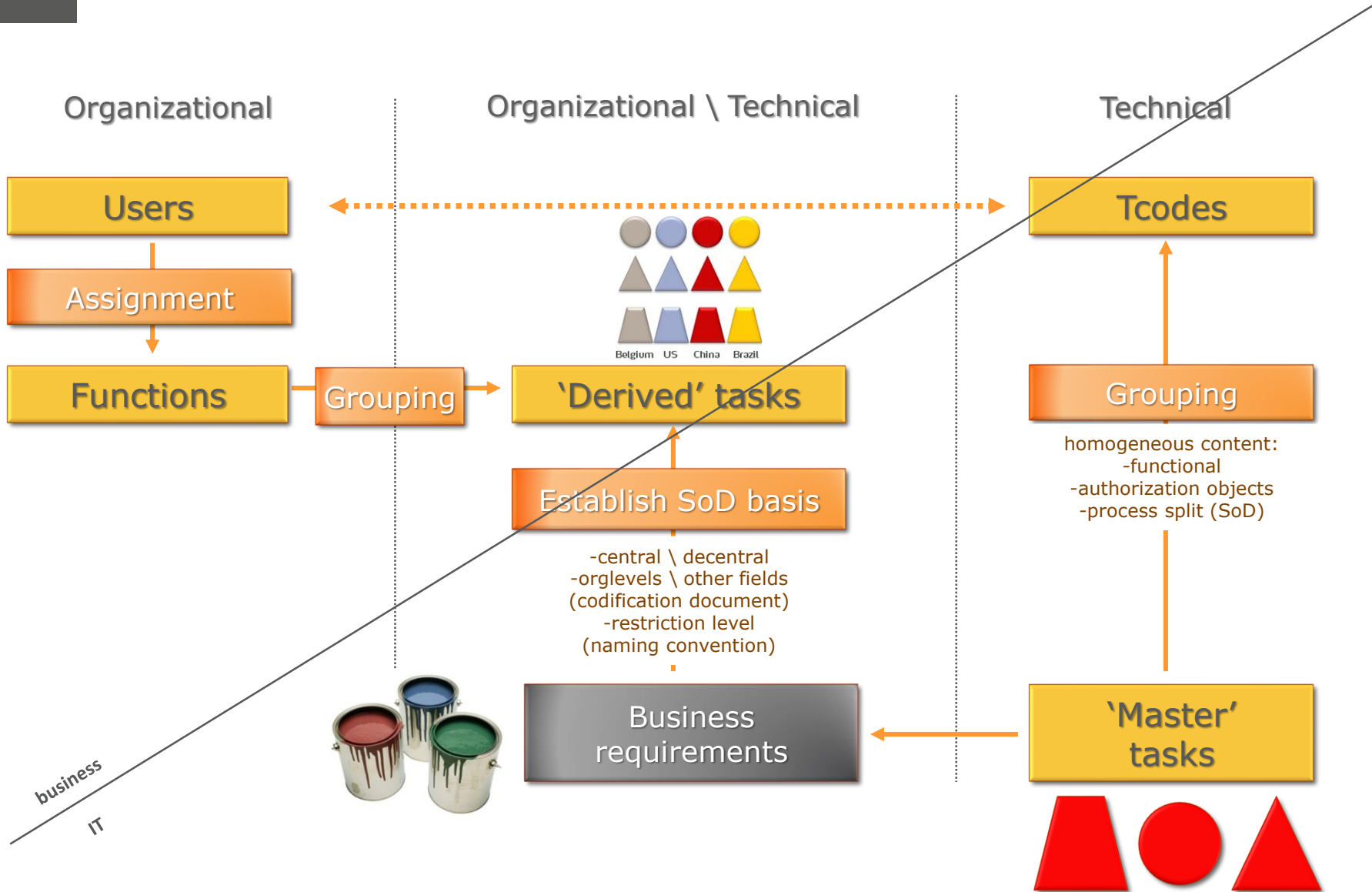
1 role / transaction

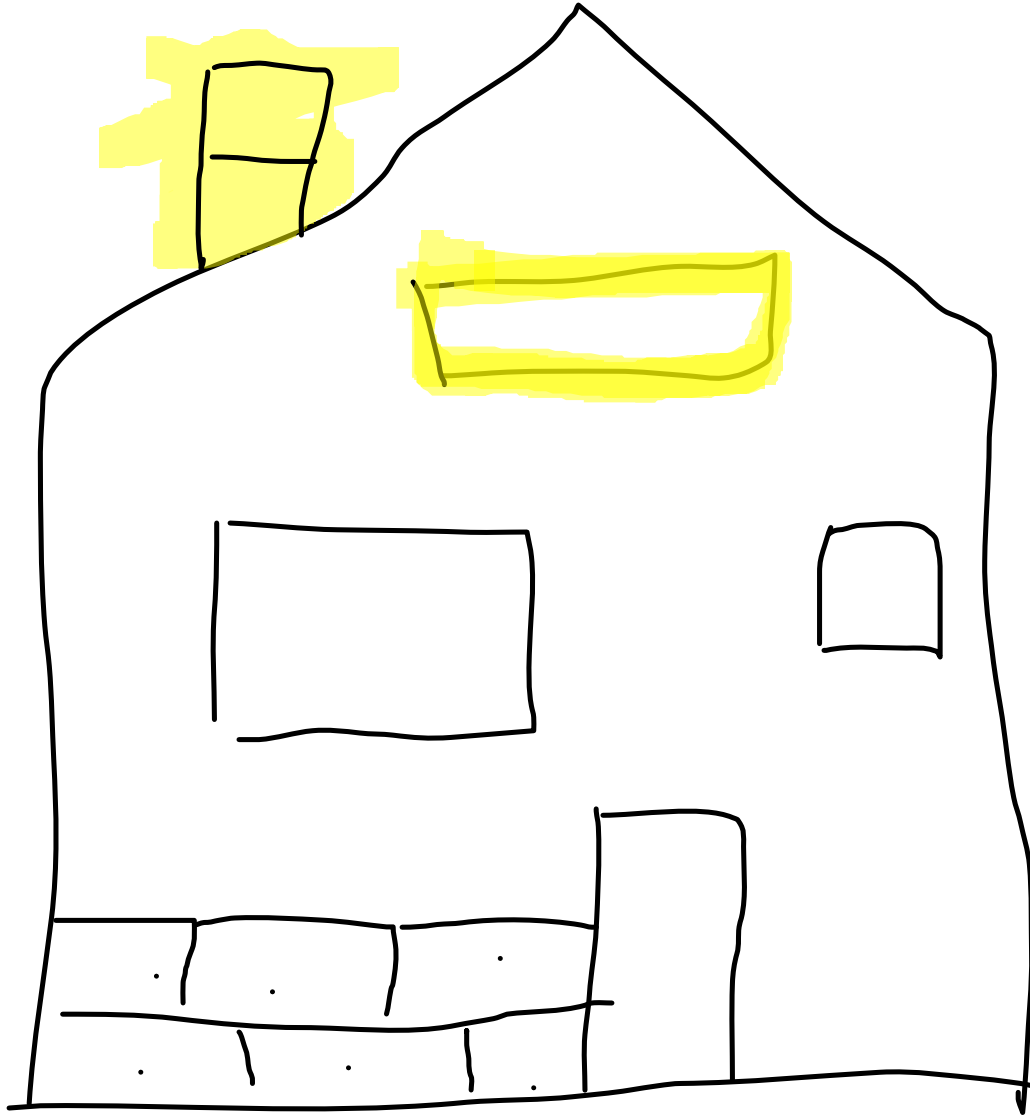


RBAC Concept Implementation



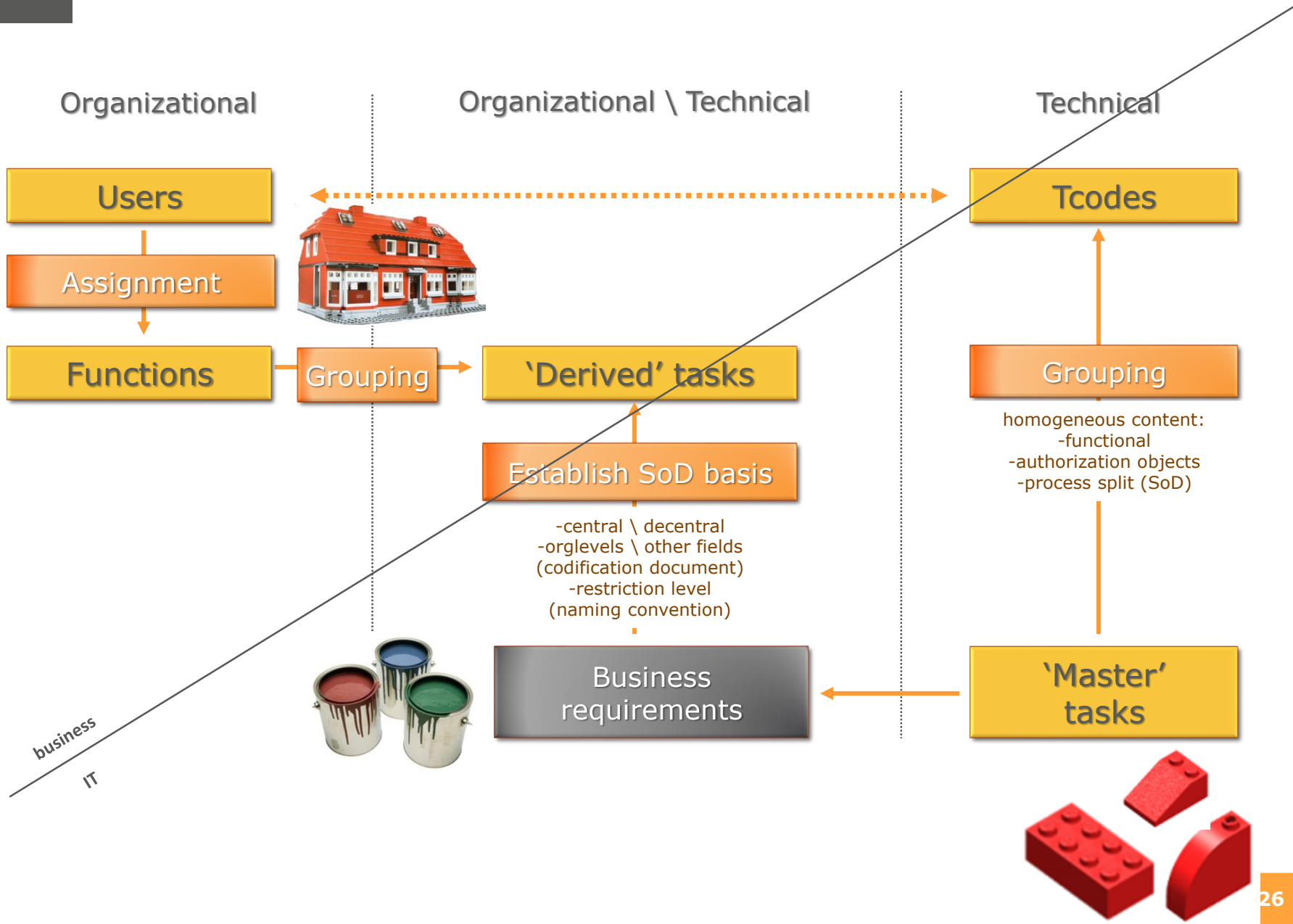
RBAC Concept Implementation





168

RBAC Concept Implementation



Grant Access to a User



This (Authorization Object Based) RBAC concept ...

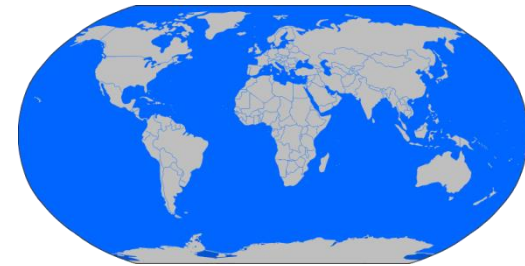
- is a proven concept that is per definition SoD free
- works for small and big companies
- supports acquisitions and mergers
- supports departmental consolidation
- is used in a SaaS model (**S**oftware **as** a **S**ervice)
- supports the definition of clear responsibilities
- supports central role concept
- can be used for APO, BI, ...
- display roles are isolated

Automate Role Maintenance: who – what – where !

- Organizational perspective
 - Define Requirements on data level
 - Define Requirements on process level
- System perspective
 - Codify the WHAT requirements
 - Codify the WHERE requirements
 - Build all SAP roles fully automated
- Assign roles using business language



WHAT



WHERE

Domains (*)

- XXXX - Master
 - BXXX - Belgium
 - NXXX - Netherlands
 - UXXX - USA
 - UNXX - New York
 - UTXX - Texas
 - UCXX - California
 - Vendors
 - UCLA - Los Angeles
 - UCDX - Oakland
 - UCPX - Palo Alto
 - UCSX - San Diego
 - FXXX - France
 - YYYY - TaskWorkbook - Type 2

Workbook: Domain workbook

Drag a column header here to group by that column

General					Authorization restrictions						
Modu	Field	Description	Objects	M	T	A	Master XXXX	Belgium BXXX	Netherlands NXXX	USA UXXX	New York UNXX
*	*	*	*	*	*	*	*	*	*	*	*
F	KTOPL	Chart of Accounts	*	*	*	*	*	EURO	EURO	EURO	EURC
F	BUKRS	Company Code	*	*	*	*	*	3200	3100	0100, 0101	NEW
F	BRGRU	Authorization group	F_LFA1_BEK	*	*	*	*	TBD	NET	ACC, LOS, NEWY, OAK, PAL, SAN, TEX	NEW
K	KOKRS	Controlling Area	*	*	*	*	*	EURO	EURO	EURO	EURC
M	WERKS	Plant	*	*	*	*	*	3200	3100	0101, 0102, 0103	0101
M	EKORG	Purchasing Organization	*	*	*	*	*	3200	3100	0100	0100

Codification

documenting the business requirements

WHERE

Authorization restrictions

Modu	Field		Master XXXX	Belgium BXXX	Netherlands NXXX	USA UXXX	New York UNXX
F	KTOPL	Chart of Accounts	*	EURO	EURO	EURO	EURC
F	BUKRS	Company Code	*	3200	3100	0100, 0101	.
F	BRGRU	Authorization group	F_LFA1_BEK	TBD	NET	ACC, LOS, NEW, OAK, PAL, SAN, TEX	NEW
K	KOKRS	Controlling Area	*	EURO	EURO	EURO	EURC
M	WERKS	Plant	*	3200	3100	0101, 0102, 0103	0101
M	EKORG	Purchasing Organization	*	3200	3100	0100	0100
V	VKORG	Sales Organization	*	3200	3100	0100	0100
V	SPART	Division	*	01, 02	01, 02	03	03

Total row count: 13

WHAT

Role name indicators | Authorization restrictions

Module	Field	Description	Objects	Modules	Taskcodes	Actions	TaskWorkbook - Type 2 YYYY
*	KOART	Account type	*	*	AP*	*	K
*	KOART	Account type	*	*	AR*	*	D
*	KTOKK	Vendor account group	*	*	*	*	NORM

Automated Translation of documentation into roles

Role (SAP): S99FBXXXAPRA (*) Workbook: Domain workbook Workbook: Task workbook

Role name: S99FBXXXAPRA Authorizations status: Actual synchronized

Short description: Payment Run Belgium

Description:

CSI Role Build & Manage®

i The authorizations are updated correctly.
Updated object field authorizations: 4

OK

Transactions | **Authorizations** | Domains | Attributes | Comment | Documents | Menu | Groups | Queries | Norm | Compositesroles | Users | Σ U

Drag a column header here to group by that column.

	Status	Object	Object description	Field	Field description	Authorization	Values	Codification	New	Updated
<input type="checkbox"/>	Standard	F_BKPF_BUK	Accounting Document: Authorization...	ACTVT	Activity	00	03	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_BKPF_BUK	Accounting Document: Authorization...	BUKRS	Company Code	00	3200	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Standard	F_BKPF_GSB	Accounting Document: Authorization...	ACTVT	Activity	00	03	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_BKPF_GSB	Accounting Document: Authorization...	GSBER	Business Area	00	*	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Standard	F_BKPF_KOA	Accounting Document: Authorization...	ACTVT	Activity	00	03	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_BKPF_KOA	Accounting Document: Authorization...	KOART	Account Type	00	K	K	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Standard	F_PAYR_BUK	Check Management: Action Authoriz...	ACTVT	Activity	00	03, 05, 17	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_PAYR_BUK	Check Management: Action Authoriz...	BUKRS	Company Code	00	3200	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Standard	F_PAYRQ	Authorization Object for Payment Re...	ACTVT	Activity	01	02, 03, 85	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_PAYRQ	Authorization Object for Payment Re...	BUKRS	Company Code	01	3200	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Maintained	F_PAYRQ	Authorization Object for Payment Re...	ORIGIN	Origin Indicator	01	*	#No match#	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Maintained	F_REGU_BUK	Automatic Payment: Activity Authoriz...	BUKRS	Company Code	01	3200	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/>

WHERE **WHAT**

USOB*

Context & ABAC (Attribute Based Access)

Direct insight in impact of affected domains and roles

Domains (*)

- XXXX - Master
 - BXXX - Belgium
 - FXXX - France
 - NXXX - Netherlands
 - UXXX - USA
 - UNXX - New York
 - UTXX - Texas
 - UCXX - California
 - Vendors
 - UCLA - Los Angeles
 - UCOX - Oakland
 - UCPX - Palo Alto
 - UCSX - San Diego
 - XXXX - Task Restrictions HR
 - YYYY - Master Task

Workbook: Domain workbook

Drag a column header here to group by that column.

General				Role n			Authorization restrictions						
Mo	Field	Description	Objects	C	SA	T	A	Master XXXX	Belgium BXXX	France FXXX	Netherlands NXXX	USA UXXX	New York UNXX
<input checked="" type="checkbox"/>	*	*	*	*	*	*	*	*	*	*	*	*	*
F	<input type="checkbox"/>	KTOPL	Chart of Accounts	*	*	*	*	*	EURO	EURO	EURO	EURO	EURO
F	<input checked="" type="checkbox"/>	BUKRS	Company Code	*	*	*	*	*	3200	3300	3100	0100	.
F	<input type="checkbox"/>	BRGRU	Authorization Group	F_LFA1_BEK	*	*	*	*	TBD	TBD	NET	CUP, KOSTAL, NEW, OAK, PAL, SAN, TEX	NEW
K	<input checked="" type="checkbox"/>	KOKRS	Controlling Area	*	*	*	*	*	EURO	EURO	EU		EURO
M	<input checked="" type="checkbox"/>	WERKS	Plant	*	*	*	*	*	3200	3355	12		0101
M	<input checked="" type="checkbox"/>	EKORG	Purchasing Organization	*	*	*	*	*	3200	55	45		0100
V	<input checked="" type="checkbox"/>	VKORG	Sales Organization	*	*	*	*	*	3200	3300	31		0100
V	<input checked="" type="checkbox"/>	SPART	Division	*	*	*	*	*	01, 02	01, 02	01,		03
V	<input checked="" type="checkbox"/>	VTWEG	Distribution Channel	*	*	*	*	*	01	01	0		05
S	<input type="checkbox"/>	CLASS	User group in user master mai...	S_USER_GRP	*	*	*	*	BXXX	FXXX	NX		-
C	<input checked="" type="checkbox"/>	CSWRK	Plant	*	*	*	*	*	3200	3300	31		0101
B	<input type="checkbox"/>	/SAPTRX/...	/SAPTRX/CI	*	*	*	*	*	3200	3300	31		0100
B	<input type="checkbox"/>	0COMP	Company Code	*	*	*	*	*	3200	3300	31		0100
P	<input type="checkbox"/>	PERSA	Personnel Area	*	*	*	*	*	12*	06*	05		1001

Context menu for Affected domains ...:

- Open
- Open field
- Refresh
- Clear
- File info
- Affected domains ...
- Affected roles ...
- Copy
- Paste

The change of one value in the codification will trigger a change in all applicable roles!

A change in an organization is only seconds of work!

Potentially affected roles of: New York (field: BRGRU)

Drag a column header here to group by that column.

Role name	Description
AA1FUXXXAPSPA	Test USA
AAA1FUXXXAPSPA	Demo VNSG USA
BBB1FUXXXAPSPA	Demo VNSG USA
CS1FUXXXAPSPA	Demo CSI USA
CUP1FUXXXAPSPA	Demo CUP USA
CUQ1FUXXXAPSPA	Demo CUP 15 Feb USA
EBY1FUXXXAPSPA	Demo 17.26 ebay USA
EPC1FUXXXAPSPA	Demo for Carla USA

Total row count: 21

Close

Affected domains of: New York (field: BRGRU)

- UXXX - USA
- UNXX - New York

Close

Simplification & Automation = 100% Accuracy

since role description maps role content

150.000 +
Fiori + ...

1.200

300

40

Manage with
40
authorization object fields

Role ID

The screenshot shows two tables in an SAP authorization configuration tool. The top table, titled 'WHERE', lists authorization objects and their values for various domains. The bottom table, titled 'WHAT', lists role indicators and their corresponding authorization objects.

Modu	Field	Master XXXX	Belgium B0XX	Netherlands N0XX	USA U0XX	New Y L0XX
F	KT0PL	Chart of Accounts	*	*	*	*
F	BK0RS	Company Code	*	*	*	*
F	BR0RU	Authorization group	F_LFAT_BEK	*	*	*
K	K0KRS	Controlling Area	*	*	*	*
M	W0RKS	Plant	*	*	*	*
M	EW0RG	Purchasing Organization	*	*	*	*
V	VW0RG	Sales Organization	*	*	*	*
V	SPART	Division	*	*	*	*

Module	Field	Description	Objects	Modules	Taskcodes	Actions	TaskHorbook - Type 2
*	KOART	Account type	*	*	*	*	K
*	KOART	Account type	*	*	*	*	D
*	KT0RK	Vendor account group	*	*	*	*	NORM

Role Description
&
Role Content

Role Content is deviating from documentation

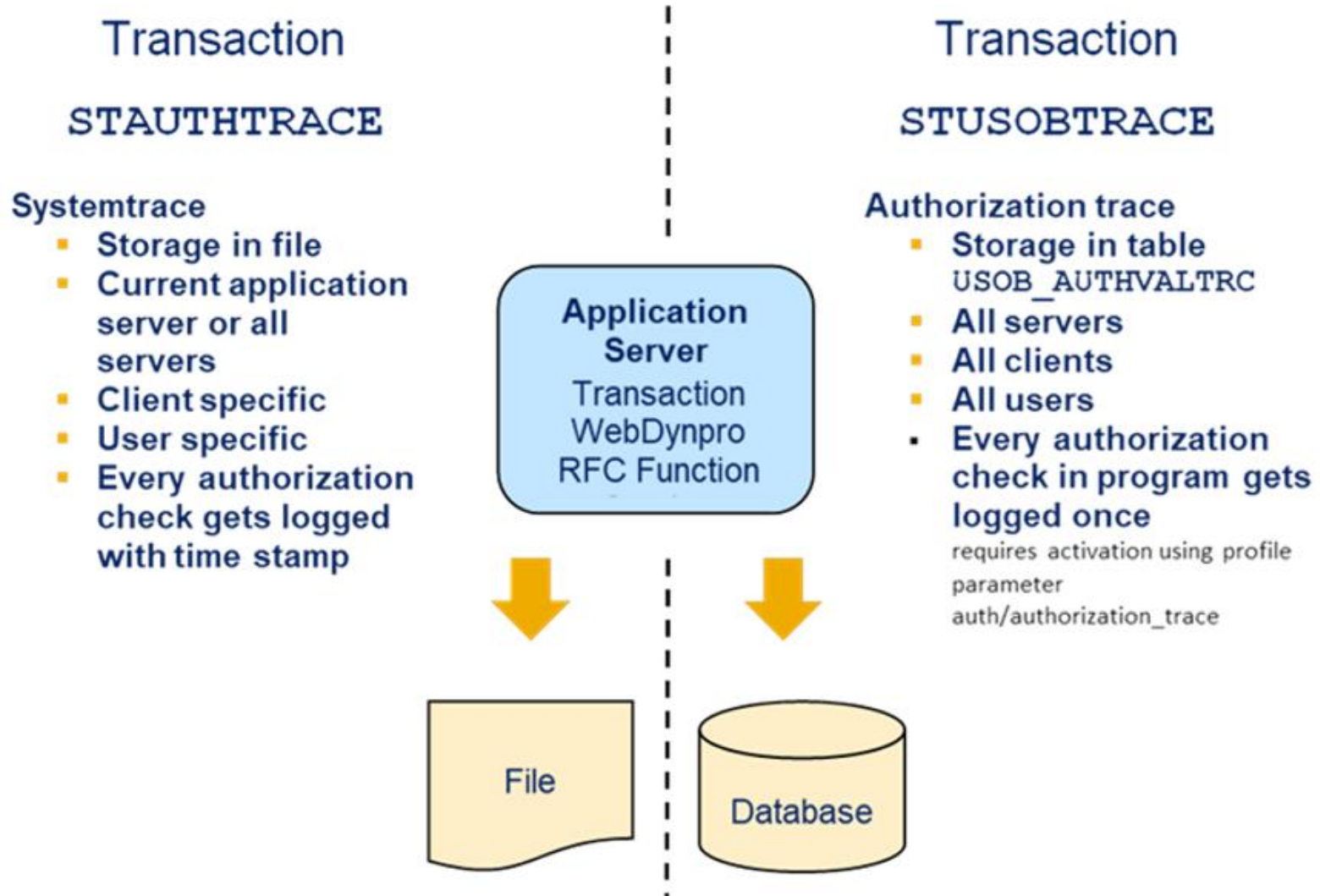
systems can have millions of authorization lines

Update role authorizations												
Roles Overview Updates												
Drag a column header here to group by that column.												
<input type="checkbox"/>	<input type="checkbox"/>	Role name	Description (SAP)	Status	Object	Field	Authorizatio	Values	Codification	<input type="checkbox"/>	<input type="checkbox"/>	Information
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	*	<input checked="" type="checkbox"/>	*			*	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*
<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99FXXARCMA	F-AR: Maintain A/R Credit Management	<input type="checkbox"/> Maintained	F_BKPF_BUK	BUKRS	00	HELLO	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99FXXARCMA	F-AR: Maintain A/R Credit Management	<input type="checkbox"/> Maintained	F_KNB1_ANA	BUKRS	00	HELLO	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFXXAPSPA	Demo Web	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	!	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFUXAPSPA	Demo Web USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LAX, LOS, NEW, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFUCLAAPSPA	Demo Web Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LAX, LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFUXAPSPA	NRB demo USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, NRB, OAK, PAL, SAN...	CUSTOMER, NEW, OAK, PA...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFUCLAAPSPA	NRB demo Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	HIHI, LOS, NRB	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFXXAPSPA	NRB demo Belgium	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	3333	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUNXXAPSPA	Demo 8 Aug New York	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	1111	0100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUCXXAPSPA	Demo 8 Aug California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	CLA, OAK, PAL,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUCLAAPSPA	Demo 8 Aug Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	CLA	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUCXXAPSPA	Demo IIA California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, OAK, PAL,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUCLAAPSPA	Demo IIA Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, XXX	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUXXXAPSPA	Demo 12-24 USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	FLOR, JEF,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUCXXAPSPA	Demo 12-24 California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, OAK, PAL,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUCLAAPSPA	Demo 12-24 Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	MOLFUXXXAPSPA	Demo May 10 USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, OAK,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	MOLFUCLAAPSPA	Demo May 10 Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	STEFUXXXAPSPA	Demo USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, OAK,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	STEFUCLAAPSPA	Demo Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, STE	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUXXXAPSPA	Demo IIA USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	FLOR, JEF,	CUSTOMER,	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorizations need to be updated

Which authorization are needed?

- Use SU24
 - But data is not always correct
 - Usually not documented for own developed coding
- Use SAP ABAP scanner to improve SU24
 - Transaction ATC (ABAP Test Cockpit)
 - Disadvantages ABAPs are nested so too many authority checks will be listed
 - ▣ Also the double / conditional authority checks
- Better: Perform an authorization check trace with transaction ST01
 - This will list exactly what a user need
- Best solution: Use the SAP new way of tracing
 - Reduces testing to zero and fully supports our concept

SAP New way of tracing



SAP New way of tracing

Transaction

STUSERTRACE

Authorization trace

- Storage in table
SUAUTHVALTRC
- All servers
- Client specific
- User specific
- Every authorization
check in program
gets logged with time
stamp once per
client and user

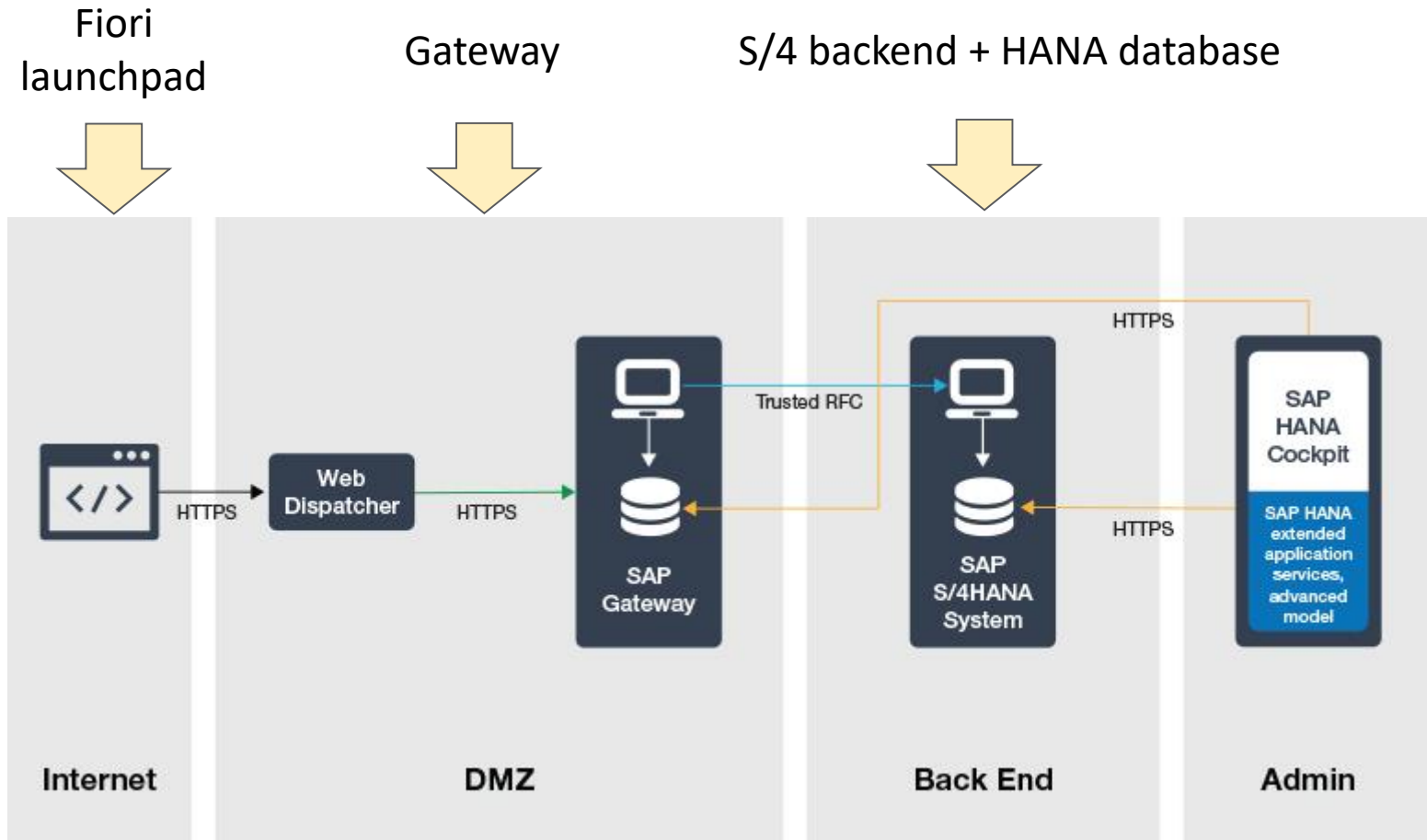
Transaction

STRFCTRACE

Analysis of statistic records for RFC

- All servers
- Client specific
- User specific
- Logging of external
RFC calls

S/4HANA architecture adds multiple layers



Copyright – SAP

Insider



Supports: Context, RBAC, ABAC & derivation on non-organizational levels !

Thank you!

Johan Hermans

johan.hermans@csi-tools.com

Acknowledgements

Microsoft Access, Microsoft .Net and Microsoft SQL are registered trademarks of Microsoft. SAP and other SAP products or services, mentioned herein, are trademarks or registered trademarks of SAP SE. CSI Accelerator, CSI Authorization Auditor, CSI Role Build & Manage, CSI Data Xtractor, CSI Integrate & Collaborate and CSI Automated Request Engine are registered trademarks of CSI tools.

Complementary Roles

- Complementary roles is not a concept but a principle that can be applied on every concept. We have seen two-tier, three-tier and even four-tier layer concepts
- The idea of a complementary roles is that certain access rights (usually organizational levels) are granted separately, using the SAP pitfall of accumulation of access rights
- We are not in favor of this principle for the following reasons:
 - Using a pitfall as principle will cause unexpected access rights and create bigger pitfalls
 - Only four-tier layer concepts will partially prevent this, but is then way too technical for end-users, so no transparency
 -/...

Complementary Roles

- CSI tools is not in favor of this principle for the following reasons:
 - ./..
 - SU24 / USOBT settings are no longer respected causing difficult and costly maintenance and upgrade effort
 - For some modules the organizational level access give enough access
 - Ownership is difficult to define, which is a key item in provisioning
 - Focus is set on reducing the number of roles.
 - This gives the impression that the role building process generates the main costs. Our experience learns, however, that the main cost of an authorization concept is in maintenance, roll out, adaption and re-use of a concept, not the building phase.
 - Automated tooling cannot – per definition – identify SoD conflicts on role level
 -