Our challenges on user authorizations and how we plan to attack them

Contents

- Shortly about Duni
- The challenges
- The way forward
- The future approach

Vision

At Duni we are passionate about being outstanding in our field; to grow into the world’s most attractive provider of inspirational table top concepts and creative take-away solutions.

With our minds set on food, people and design we have the ambition to always supply Goodfoodmood® to any eating and drinking occasion.

About us

- Duni has about 2,500 employees
- Headquarters in Malmö, Sweden
- Started 1949 with the production of wax coated paper cups and paper napkins
- Dominant market position in Europe
- Net sales: SEK 4,927 m (4,441)
- Operating income [1)]: SEK 430 m (491)
- Listed on NASDAQ Stockholm
- 75% of BioPak Pty Ltd, leading supplier of sustainable disposable packaging for the food service industry in Australia and New Zealand, was acquired in October 2018 with an annual approximate turnover of SEK 385 m.

1) Operating income adjusted for amortization of intangible assets identified in connection with business acquisitions and for restructuring costs and market valuation of derivatives.

Duni in the world

Austria
Australia
Belgium
Czech Republic
Denmark
Finland
France
Germany*
Hungary
Italy
Netherlands
New Zealand*
Norway
Poland*
Russia
Singapore
Spain
Sweden*
Switzerland
Thailand*
United Arab Emirates
United Kingdom
USA

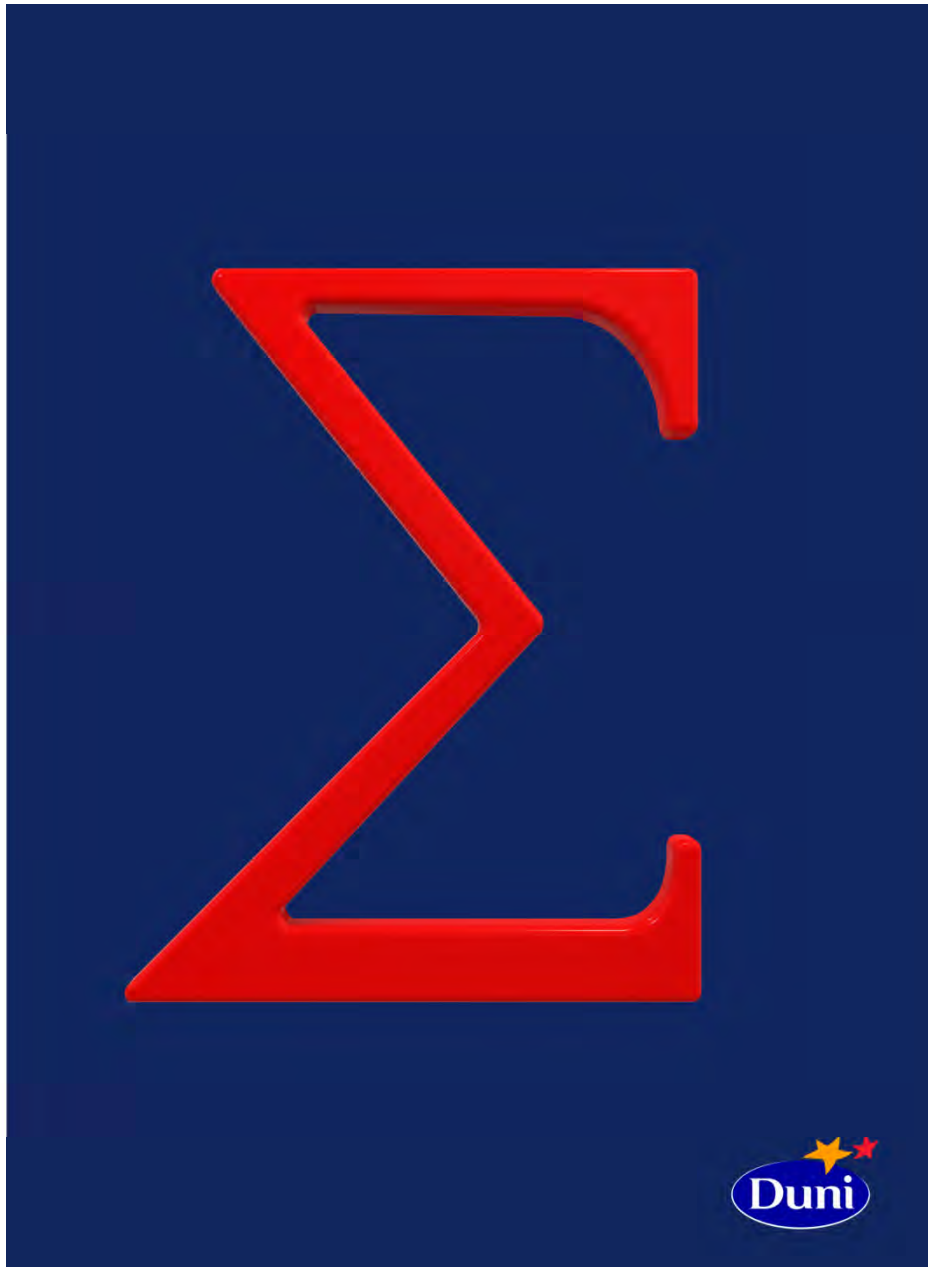
* Production

Status and challenges

- Centralization of shared functions
- Legacy in function distribution
  - Some local flavor remained
- People moving and changing roles
- Authorizations and Segregation of Duties a part of the audit
- SAP’s authorization concept
- Standard roles vs tailored roles
  - Granularity of roles
- High effort in role maintenance

Numbers

Active Users ~800
Active Roles ~570
Average 13 roles per user
Average 42 transactions per role
Average 825 transactions per user



How did we end up like this?

2003 SAP Nordic - MM, SD, FI/CO
- No experience
- Menu based roles

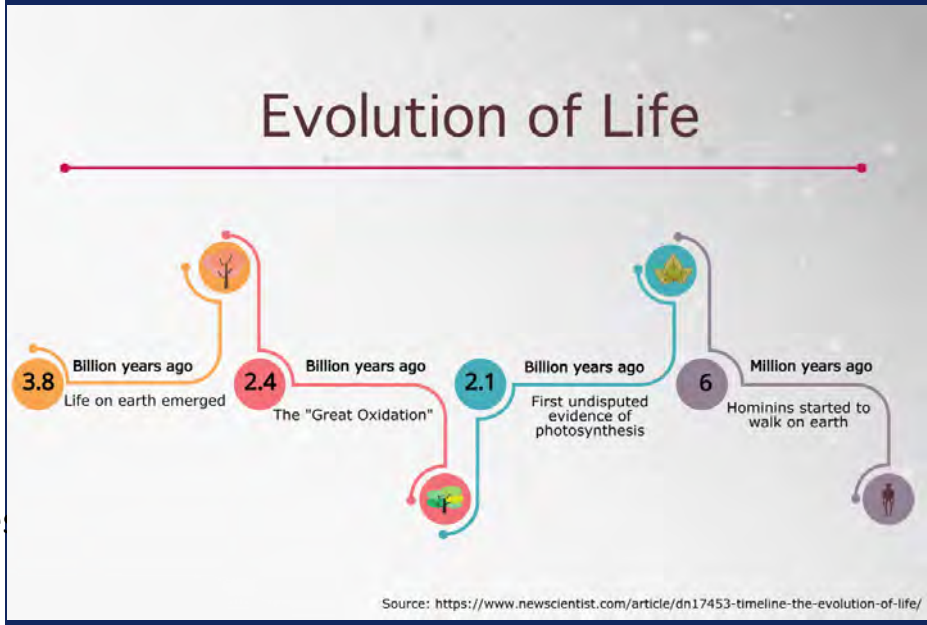
2005 Production site in Poland – MM, FI/CO, PP
- Organizational limitations

European Finance Function – FI/CO

2006 European roll starts… - MM, SD, FI/CO
- Menu based to wide
- What's needed role – local variants, individual add on roles
- Mixed roles in small BU's

2009 New concept – at EFF
- SOD function based roles
- Organisational level

2012 Merge SAP systems – MM, SD, FI/CO, PP
- Consider existing wide authorizations



What we want to achieve is

- No overhead of transactions assignment for end users
- Minimize or mitigate SOD conflicts
- Minimize the administration effort
  by having a clear structure and strategy

How to achieve this

1. Wave 1 – analyse and clean up
   - Remove not used own created roles
   - Remove not used transactions from user roles
   - Take care of all critical SOD conflicts

2. Wave 2 – Define the role creation strategy and process
   - Site & position based roles
   - Define decision makers and communication

3. Wave 3 – restructure
   - Minimize or mitigate SOD conflicts
   - **Only needed transactions for each user**
   - New naming convention based on the strategy

Actions

Remove not used own created roles
Remove not used transactions in roles/users
Remove critical transactions from end user roles
and define alternatives for the end users

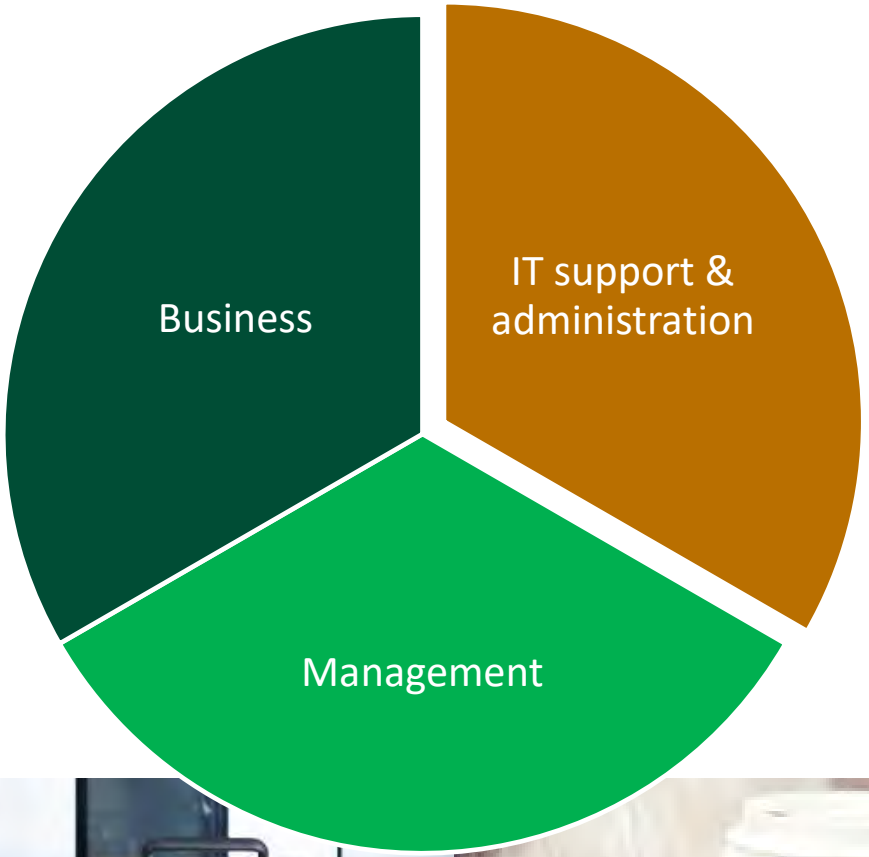
Define the strategy for roles together with the business
considering SOD conflicts

Recreate roles based on the strategy
minimize or mitigate SOD conflicts
only needed transactions per position and site

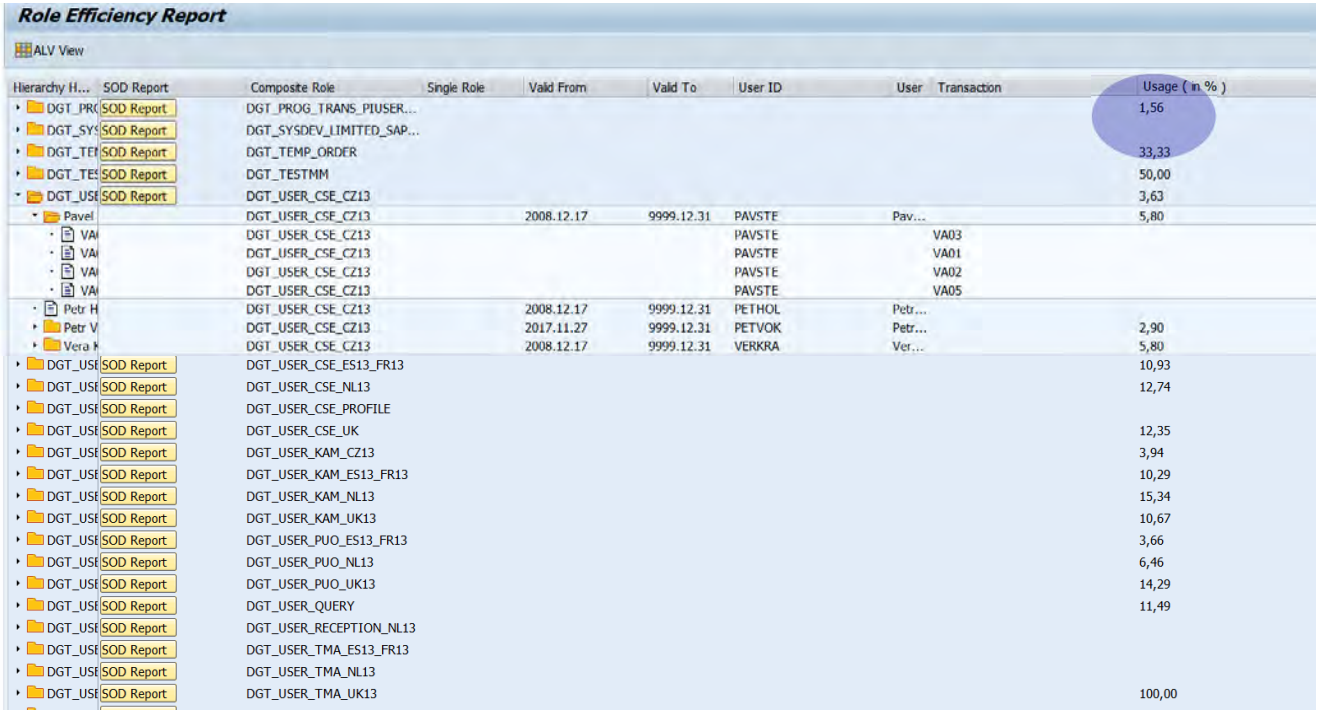
Set up a way of working for this so that it can be done by support organization

Find all users and roles with critical authorizations
and then decide how to limit this
Do the similar exercises for users and roles that has Critical SOD conflicts
Reduce “overhead” for users with a lot more authorization
than is actually being used.
Based on the above restructuring roles in general

Wave 1 – analyse and clean up



Remove not used own created roles



Role Efficiency Report

ALV View

Hierarchy H...	SOD Report	Composite Role	Single Role	Valid From	Valid To	User ID	User	Transaction	Usage (in %)
DGT_PR	SOD Report	DGT_PROG_TRANS_PIUSER...							1,56
DGT_SY	SOD Report	DGT_SYSDEV_LIMITED_SAP...							
DGT_TE	SOD Report	DGT_TEMP_ORDER							33,33
DGT_TE	SOD Report	DGT_TESTMM							50,00
DGT_US	SOD Report	DGT_USER_CSE_CZ13							3,63
Pavel		DGT_USER_CSE_CZ13		2008.12.17	9999.12.31	PAVSTE	Pav...		5,80
VA		DGT_USER_CSE_CZ13				PAVSTE		VA03	
VA		DGT_USER_CSE_CZ13				PAVSTE		VA01	
VA		DGT_USER_CSE_CZ13				PAVSTE		VA02	
VA		DGT_USER_CSE_CZ13				PAVSTE		VA05	
Petr H		DGT_USER_CSE_CZ13		2008.12.17	9999.12.31	PETHOL	Petr...		
Petr V		DGT_USER_CSE_CZ13		2017.11.27	9999.12.31	PETVOK	Petr...		2,90
Vera K		DGT_USER_CSE_CZ13		2008.12.17	9999.12.31	VERKRA	Ver...		5,80
DGT_US	SOD Report	DGT_USER_CSE_ES13_FR13							10,93
DGT_US	SOD Report	DGT_USER_CSE_NL13							12,74
DGT_US	SOD Report	DGT_USER_CSE_PROFILE							
DGT_US	SOD Report	DGT_USER_CSE_UK							12,35
DGT_US	SOD Report	DGT_USER_KAM_CZ13							3,94
DGT_US	SOD Report	DGT_USER_KAM_ES13_FR13							10,29
DGT_US	SOD Report	DGT_USER_KAM_NL13							15,34
DGT_US	SOD Report	DGT_USER_KAM_UK13							10,67
DGT_US	SOD Report	DGT_USER_PUO_ES13_FR13							3,66
DGT_US	SOD Report	DGT_USER_PUO_NL13							6,46
DGT_US	SOD Report	DGT_USER_PUO_UK13							14,29
DGT_US	SOD Report	DGT_USER_QUERY							11,49
DGT_US	SOD Report	DGT_USER_RECEPTION_NL13							
DGT_US	SOD Report	DGT_USER_TMA_ES13_FR13							
DGT_US	SOD Report	DGT_USER_TMA_NL13							
DGT_US	SOD Report	DGT_USER_TMA_UK13							100,00

- In this report we found that we have own created roles that is no longer assigned to any user.

Remove not used transactions in roles/users

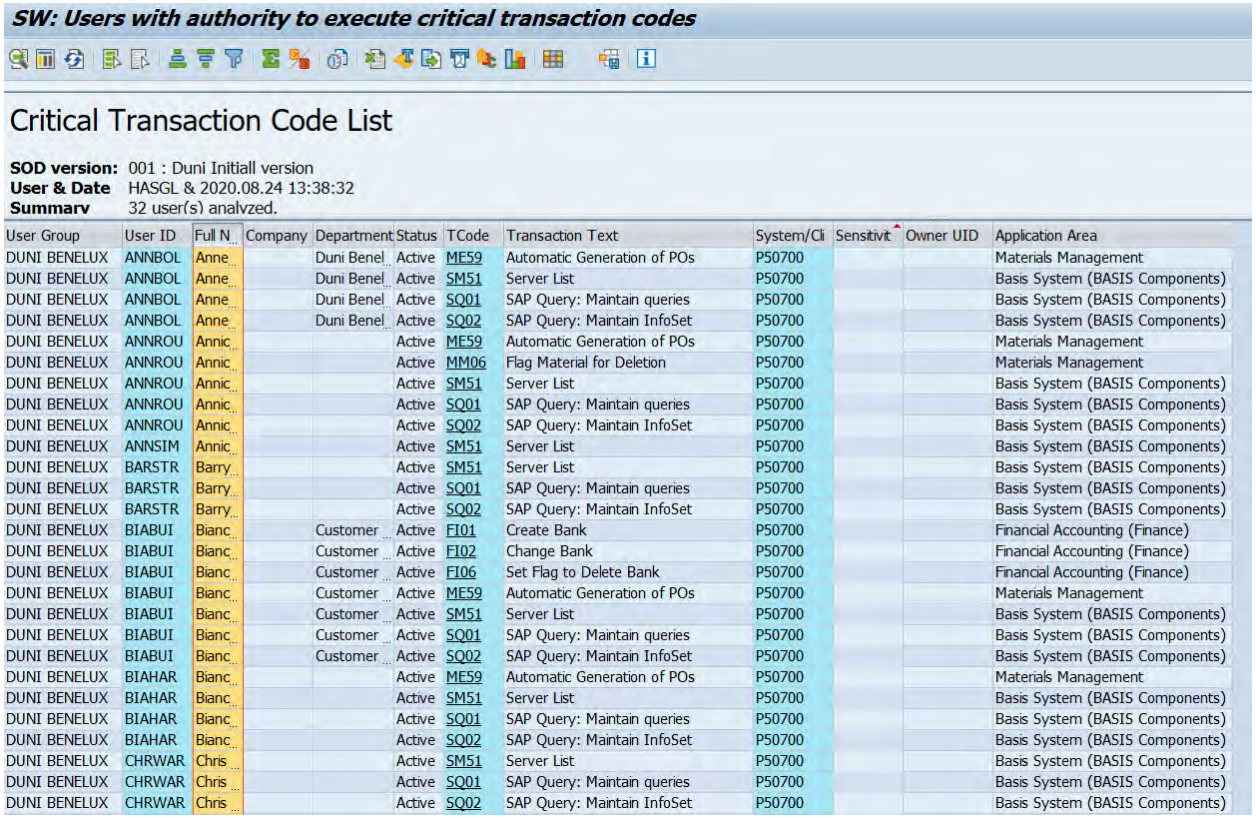
Ran Executable-Currently Authorized Tcod

User & Date on HASGL on 2020.08.24 13:30:40
1 user(s) analyzed.

User ID	Full N...	Execut...	TCode	Transaction Text
HEIDRU	Heiko ...	Y	MD04	Display Stock/Requirements Situation
HEIDRU	Heiko ...		MMBE	Stock Overview
HEIDRU	Heiko ...		SESSION_...	Session Manager Menu Tree Display
HEIDRU	Heiko ...		VA02	Change Sales Order
HEIDRU	Heiko ...		VA03	Display Sales Order
HEIDRU	Heiko ...		VL02N	Change Outbound Delivery
HEIDRU	Heiko ...		VL03N	Display Outbound Delivery
HEIDRU	Heiko ...		VL06I	Inbound Delivery Monitor
HEIDRU	Heiko ...		VL10A	Sales Orders Due for Delivery
HEIDRU	Heiko ...		ZETI	label printing program
HEIDRU	Heiko ...	N	CA03	Display Routing
HEIDRU	Heiko ...		CM01	Cap. planning, work center load
HEIDRU	Heiko ...		CM02	Capac. planning, work center orders
HEIDRU	Heiko ...		CM03	Capac. planning, work center pool
HEIDRU	Heiko ...		CM04	Capac. planning, work center backlog
HEIDRU	Heiko ...		CM05	Capacity plan.:Work center overload
HEIDRU	Heiko ...		CM10	Capacity leveling
HEIDRU	Heiko ...		CM21	Capacity leveling SFC planning table
HEIDRU	Heiko ...		CM25	Capacity leveling: Variable
HEIDRU	Heiko ...		CO01	Create production order
HEIDRU	Heiko ...		CO02	Change Production Order
HEIDRU	Heiko ...		CO03	Display Production Order
HEIDRU	Heiko ...		CO04	Print Production Orders
HEIDRU	Heiko ...		CO05	Collective Release of Prod. Orders
HEIDRU	Heiko ...		CO07	Create order without a material
HEIDRU	Heiko ...		CO09	Availability Overview
HEIDRU	Heiko ...		CO11	Enter Time Ticket
HEIDRU	Heiko ...		CO11N	Single Screen Entry of Confirmations
HEIDRU	Heiko ...		CO12	Collective Entry of Confirmations
HEIDRU	Heiko ...		CO13	Cancel confirmation of prod. order
HEIDRU	Heiko ...		CO14	Display confirmation of prod. order

- This is one example shows how much overhead there can be for one single user when it comes to available transactions.

Remove critical transactions from end user roles 1/2



SW: Users with authority to execute critical transaction codes

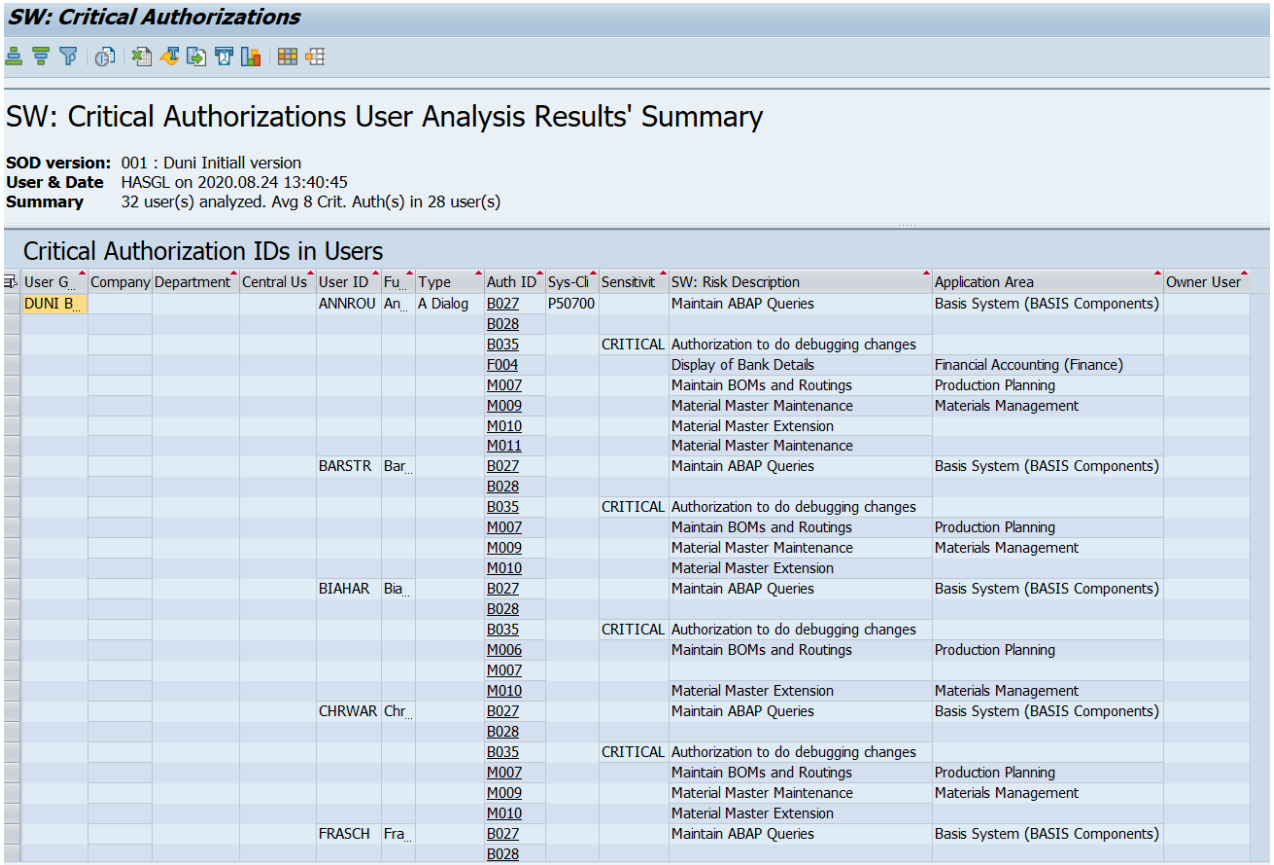
Critical Transaction Code List

SOD version: 001 : Duni Initiall version
User & Date HASGL & 2020.08.24 13:38:32
Summary 32 user(s) analyzed.

User Group	User ID	Full N	Company	Department	Status	TCode	Transaction Text	System/Cli	Sensitivit	Owner UID	Application Area
DUNI BENELUX	ANNBOL	Anne		Duni Benel	Active	ME59	Automatic Generation of POs	P50700			Materials Management
DUNI BENELUX	ANNBOL	Anne		Duni Benel	Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNBOL	Anne		Duni Benel	Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNBOL	Anne		Duni Benel	Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNROU	Annic			Active	ME59	Automatic Generation of POs	P50700			Materials Management
DUNI BENELUX	ANNROU	Annic			Active	MM06	Flag Material for Deletion	P50700			Materials Management
DUNI BENELUX	ANNROU	Annic			Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNROU	Annic			Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNROU	Annic			Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)
DUNI BENELUX	ANNSIM	Annic			Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	BARSTR	Barry			Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	BARSTR	Barry			Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	BARSTR	Barry			Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	FI01	Create Bank	P50700			Financial Accounting (Finance)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	FI02	Change Bank	P50700			Financial Accounting (Finance)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	FI06	Set Flag to Delete Bank	P50700			Financial Accounting (Finance)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	ME59	Automatic Generation of POs	P50700			Materials Management
DUNI BENELUX	BIABUI	Bianc		Customer	Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIABUI	Bianc		Customer	Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIAHAR	Bianc			Active	ME59	Automatic Generation of POs	P50700			Materials Management
DUNI BENELUX	BIAHAR	Bianc			Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIAHAR	Bianc			Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	BIAHAR	Bianc			Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)
DUNI BENELUX	CHRWAR	Chris			Active	SM51	Server List	P50700			Basis System (BASIS Components)
DUNI BENELUX	CHRWAR	Chris			Active	SQ01	SAP Query: Maintain queries	P50700			Basis System (BASIS Components)
DUNI BENELUX	CHRWAR	Chris			Active	SQ02	SAP Query: Maintain InfoSet	P50700			Basis System (BASIS Components)

- We can analyse the critical transactions to see to which users they are assigned.

Remove critical transactions from end user roles 2/2



SW: Critical Authorizations

SW: Critical Authorizations User Analysis Results' Summary

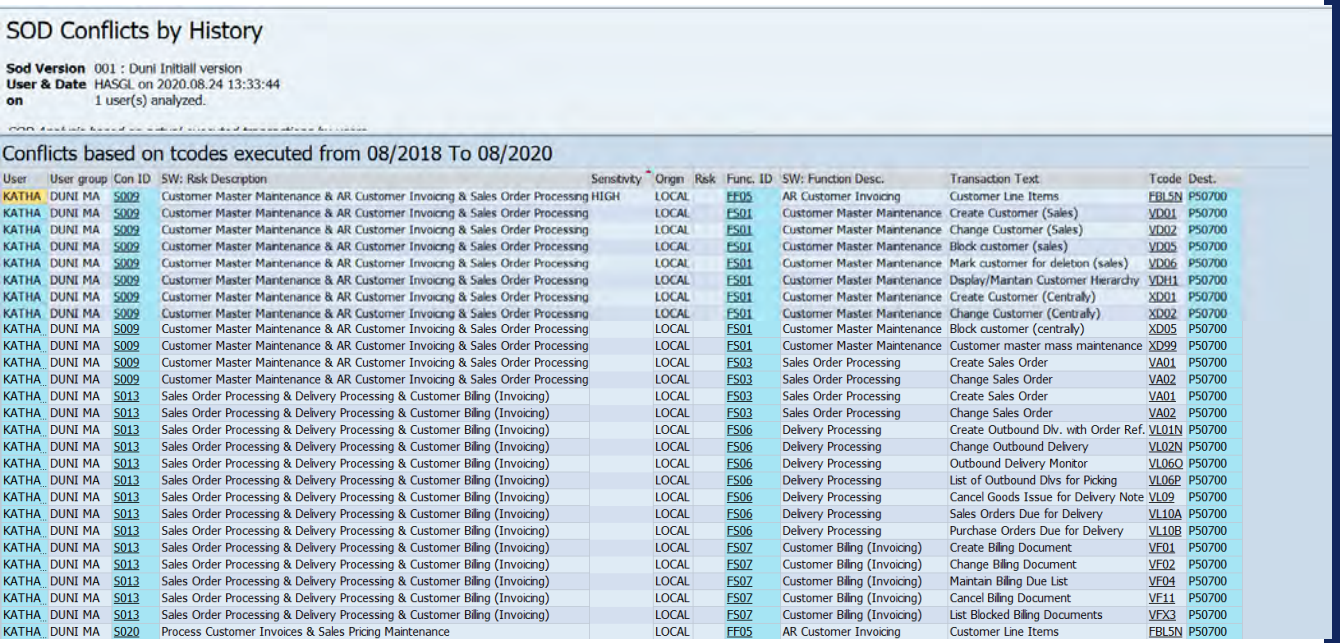
SOD version: 001 : Duni Initiall version
User & Date HASGL on 2020.08.24 13:40:45
Summary 32 user(s) analyzed. Avg 8 Crit. Auth(s) in 28 user(s)

Critical Authorization IDs in Users

User G...	Company	Department	Central Us	User ID	Fu...	Type	Auth ID	Sys-Cli	Sensitivit	SW: Risk Description	Application Area	Owner User
DUNI B...				ANNROU	An...	A Dialog	B027	P50700		Maintain ABAP Queries	Basis System (BASIS Components)	
							B028					
							B035		CRITICAL	Authorization to do debugging changes		
							F004			Display of Bank Details	Financial Accounting (Finance)	
							M007			Maintain BOMs and Routings	Production Planning	
							M009			Material Master Maintenance	Materials Management	
							M010			Material Master Extension		
							M011			Material Master Maintenance		
				BARSTR	Bar...		B027			Maintain ABAP Queries	Basis System (BASIS Components)	
							B028					
							B035		CRITICAL	Authorization to do debugging changes		
							M007			Maintain BOMs and Routings	Production Planning	
							M009			Material Master Maintenance	Materials Management	
							M010			Material Master Extension		
				BIAHAR	Bia...		B027			Maintain ABAP Queries	Basis System (BASIS Components)	
							B028					
							B035		CRITICAL	Authorization to do debugging changes		
							M006			Maintain BOMs and Routings	Production Planning	
							M007					
							M010			Material Master Extension	Materials Management	
				CHRWAR	Chr...		B027			Maintain ABAP Queries	Basis System (BASIS Components)	
							B028					
							B035		CRITICAL	Authorization to do debugging changes		
							M007			Maintain BOMs and Routings	Production Planning	
							M009			Material Master Maintenance	Materials Management	
							M010			Material Master Extension		
				FRASCH	Fra...		B027			Maintain ABAP Queries	Basis System (BASIS Components)	
							B028					

- We can also check for users which critical transaction they have access to.

Minimize or mitigate SOD conflicts 1/2



SOD Conflicts by History

Sod Version 001 : Duni Initiall version
User & Date on HASGL on 2020.08.24 13:33:44
1 user(s) analyzed.

Conflicts based on tcodes executed from 08/2018 To 08/2020

User	User group	Con ID	SW: Risk Description	Sensitivity	Origin	Risk	Func. ID	SW: Function Desc.	Transaction Text	Tcode	Dest.
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing	HIGH	LOCAL		FF05	AR Customer Invoicing	Customer Line Items	FBL5N	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Create Customer (Sales)	VD01	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Change Customer (Sales)	VD02	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Block customer (sales)	VD05	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Mark customer for deletion (sales)	VD06	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Display/Maintain Customer Hierarchy	VDH1	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Create Customer (Centrally)	XD01	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Change Customer (Centrally)	XD02	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Block customer (centrally)	XD05	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS01	Customer Master Maintenance	Customer master mass maintenance	XD99	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS03	Sales Order Processing	Create Sales Order	VA01	P50700
KATHA	DUNI MA	S009	Customer Master Maintenance & AR Customer Invoicing & Sales Order Processing		LOCAL		FS03	Sales Order Processing	Change Sales Order	VA02	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS03	Sales Order Processing	Create Sales Order	VA01	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS03	Sales Order Processing	Change Sales Order	VA02	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Create Outbound Dlv. with Order Ref.	VL01N	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Change Outbound Delivery	VL02N	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Outbound Delivery Monitor	VL06O	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	List of Outbound Dlvs for Picking	VL06P	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Cancel Goods Issue for Delivery Note	VL09	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Sales Orders Due for Delivery	VL10A	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS06	Delivery Processing	Purchase Orders Due for Delivery	VL10B	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS07	Customer Biling (Invoicing)	Create Biling Document	VF01	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS07	Customer Biling (Invoicing)	Change Biling Document	VF02	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS07	Customer Biling (Invoicing)	Maintain Biling Due List	VF04	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS07	Customer Biling (Invoicing)	Cancel Biling Document	VF11	P50700
KATHA	DUNI MA	S013	Sales Order Processing & Delivery Processing & Customer Biling (Invoicing)		LOCAL		FS07	Customer Biling (Invoicing)	List Blocked Biling Documents	VFX3	P50700
KATHA	DUNI MA	S020	Process Customer Invoices & Sales Pricing Maintenance		LOCAL		FF05	AR Customer Invoicing	Customer Line Items	FBL5N	P50700

- As a help to decide if we remove or just mitigate the risk we can use the report for see how a user has been using the SOD conflicting transactions.

Minimize or mitigate SOD conflicts 2/2

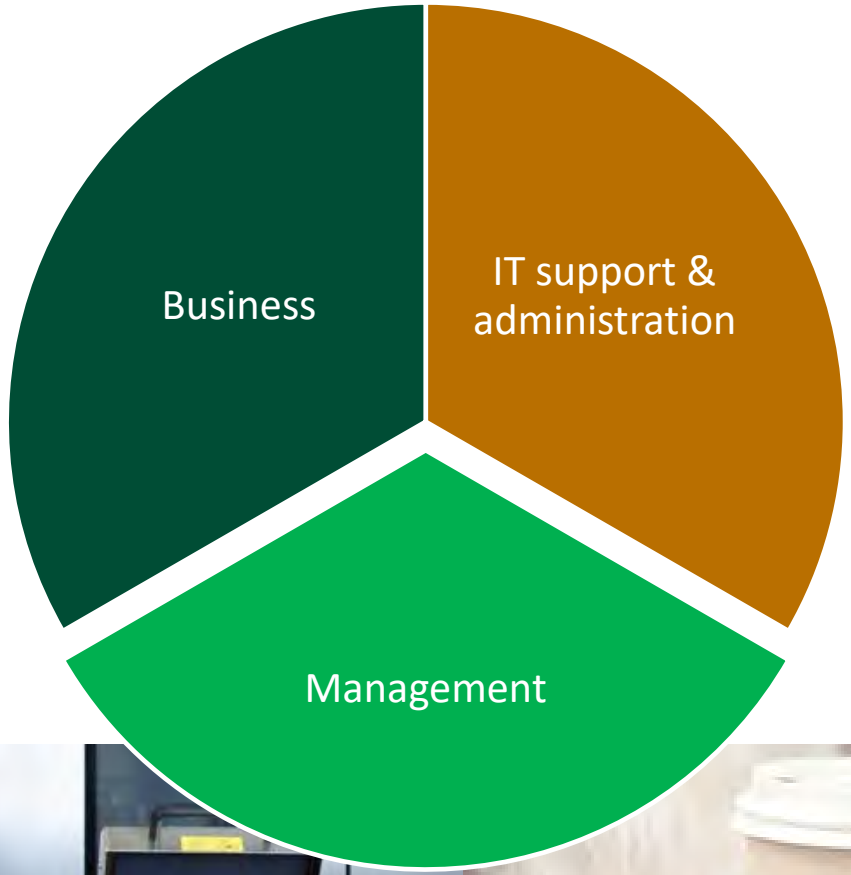
Segregation of Duties Summary Report

SOD version: 001 : Duni Initiall version
User & Date: HASGL on 2020.08.24 13:56:08
Summary: 25 user(s) analyzed. Avg 1 SOD Conflict(s) in 1 user(s)
Mitigation Summary: 1 conflicts of which 0 mitigated

User	Full ...	Con ID	Cont ID	Auditor	Mit Valid	Mit Valid	SW: Risk Description	Scan Date	# Conflict	Mit. Count
AGNKON	Agnie...								0	0
ANNFRA	Anna...								0	0
ANNJAN	Anna...								0	0
ANNKUR	Anna...	F029					Maintain Posting Period & Post Journal Entry	2020.02.11	1	0
ANNZAD	Anna...								0	0
BARWOJ	Barb...								0	0
EMIPAU	Emilia...								0	0
EWAPOL	Ewa ...								0	0
JOAZAC	Joan...								0	0
JULBER	Julie ...								0	0
KACJOZ	Kacp...								0	0
KARNOW	Karoli...								0	0
KAROLI	Karoli...								0	0
KRIGUL	Kriste...								0	0
LUKGAU	Luka...								0	0
MAGGOR	Magd...								0	0
MAGMAR	Magd...								0	0
MARPAW	Marci...								0	0
NATLEW	Natali...								0	0
PAWPAD	Pawel...								0	0
PETNIE	Peter...								0	0
PETWAL	Petra...								0	0
REIBRI	Reim...								0	0
SYLBUN	Sylvia...								0	0
TOMSWI	Tom...								0	0

- In the SOD summary report we get an overview of the conflicts within a selection of users.s
- The risk description comes from the SOD repository.

Wave 2 – Define the role creation strategy and process

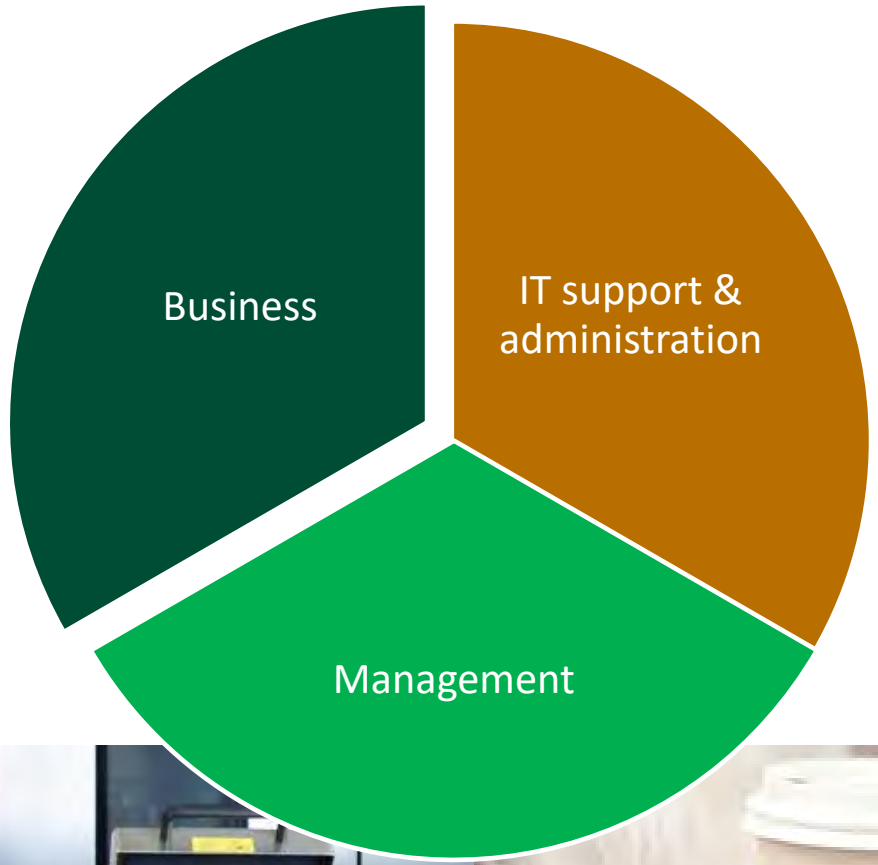


Our future approach for role design

- Position Based Approach
  - Makes it easier to understand and mitigate risk for “necessary” SOD conflicts.
  - Naming convention including Business Unit, Department, Position
- One Composite Role per Position (Job Title)
  - All User Role (The Role All Users are given with basic transactions)
  - Maintain Role
  - Display Role

- SoD Issues in the Composite Position Role are common
  - Unlikely to be caused by the All User Role
  - Unlikely to be caused by the Display Role
  - Most likely to be contained within the Maintain Role
  - Benefits of this situation
    - Simple to Remediate
    - Removing access does not affect users outside of the position
    - Simple to Mitigate and Monitor if required
    - Simple to Add Access
    - Adding access does not affect users outside of the position

Wave 3 – restructure



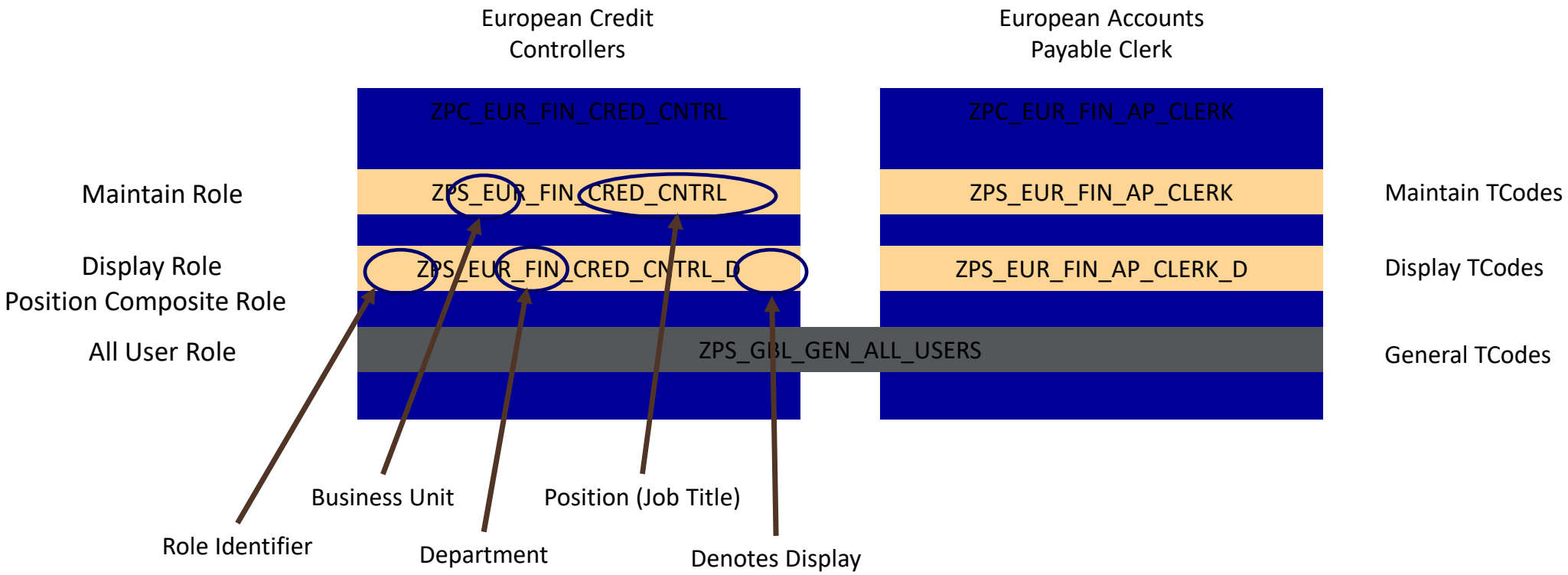
Together with the business

- Analyze
  - Departments
  - Positions
  - Tasks
- Define new roles
  - Maintenance transactions
  - Display transactions

Centrally we will

- Define the “All user role”
  - Transactions that everyone needs such as SU53, SP02, SMX, SBWP etc.
- Define a naming convention to clearly indicate the use of the role

Summary of Role Design



Questions?

sven-gunnar.linderson@duni.com

simone@securityweaver.com