

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

Bezpečnost dat v prostředí SAP

Leoš Černý

KPMG Česká republika





Proč je složité nastavit bezpečné prostředí v SAP?

Komplexní IT prostředí lze provozovat bezpečně pouze v případě, pokud jsou identifikována rizika a hrozby a přijata příslušná bezpečnostní opatření. Protože SAP řešení je velmi komplexní, lze narazit na potíže již při definování bezpečnostních pravidel. Tyto potíže mohou způsobit:

- **Různorodé požadavky na funkcionalitu** napříč všemi aspekty business procesů.
- **Požadavek na jednoduchý přístup** k informacím.
- **Požadavek na flexibilitu systému** vyvolává potřebu zahrnout právní, účetní a business požadavky ve více než 100 zemích světa (např. účtování, nákupní objednávky nebo zakázky).
- **Složitou organizační strukturu** mnoha společností a skupin, která vyvolává **potřebu oddělit přístup** na úrovni společnosti, divize či nákladového střediska.

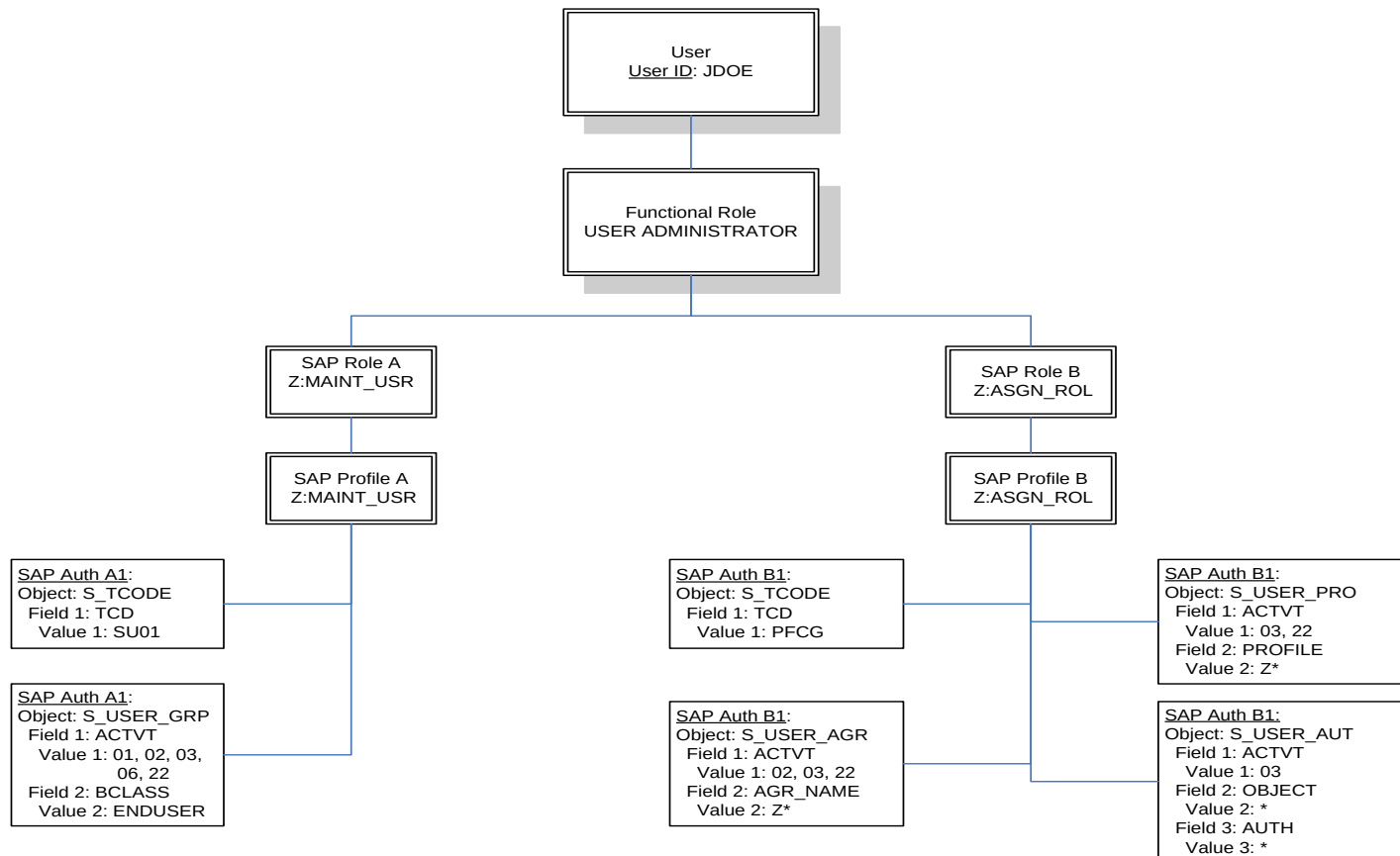
Dalšími důvody jsou:

- **Přizpůsobení organizační struktury** – bezpečnost v prostředí SAP je relativně složitá a v průběhu implementace je nutné zohlednit přizpůsobení SAP rolí potřebám organizace. **Většina společností selže právě v této fázi.**
- **Odpor ke změně** – manažeři často neberou vážně potřebu změny rolí a profilů a tím i odpovědností. Často ponechají silný přístup na úkor bezpečnosti svých vlastních dat.
- **IT oddělení vyžaduje neomezený přístup** – IT oddělení je většinou poměrně resistantní k vývoji specifických rolí a často přiděluje silný přístup, a to i v produkčním prostředí.
- **Jsou potřeba speciální nástroje a procesy** jako např. pro řízení oddělení pravomocí a odpovědností a jejich následnou kontrolu.
- **Komplexní prostředí** – jednoduché vysvětlení: V SAP pracujeme s cca < 10 000 transakcemi a objekty.

Proč je složité nastavit bezpečné prostředí v SAP?

Základní model řešení SAP bezpečnosti:

SAP využívá tzv. „**object-based**“ nastavení bezpečnosti. V SAP funkcionalitě je více jak **1000 kontrolních bodů**, které kontrolují autorizační objekty a jejich definici. **Interakce této funkcionality a business požadavků** se obecně nazývá **autorizační koncept**.





Základní oblasti SAP Bezpečnosti

SoD a
kompenzační
kontroly

Parametry
pro SAP
účty

Silné SAP
účty

Silné a citlivé
oprávnění
v SAP

Řízení
přístupu

SAP Role
a jejich
vývoj

Profiles by Complex Selection Criteria

Users by Complex Selection Criteria

Display Profile Parameter

Parameter Name	User-Defined Value	Sys
ApplianceType		
DIR_ATRA	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_AUDIT	F:\usr\sap\NL5\DVEBMGS00\log	F:\u
DIR_BINARY	F:\usr\sap\NL5\DVEBMGS00\exe	F:\u
DIR_CCMS	F:\usr\sap\CCMS	F:\u
DIR_CLIENT_ORAHOME		
DIR_CT_LOGGING	F:\usr\sap\NL5\SYS\global	F:\u
DIR_CT_RUN	F:\usr\sap\NL5\SYS\exe\uc\NTAMD64	F:\u
DIR_CT_SAPJVM	F:\usr\sap\NL5\SYS\exe\jvm\NTAMD64\sapjvm_	F:\u
DIR_DATA	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_DBMS	F:\usr\sap\NL5\SYS\SAPDB	F:\u
DIR_EPS_ROOT	\\NLACCAPP24\sapmnt\trans\EPS	\\N
DIR_EXECUTABLE	F:\usr\sap\NL5\DVEBMGS00\exe	F:\u
DIR_EXE_ROOT	F:\usr\sap\NL5\SYS\exe	F:\u
DIR_EXTRACT	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_GEN	F:\usr\sap\NL5\SYS\gen\dbg	F:\u



SoD a kompenzační kontroly

V rámci SoD a kompenzační kontroly je třeba se zaměřit na:

- **Definování matice SoD**
 - **Např. oprávnění** změnit kmenová data dodavatele a zároveň proplatit fakturu
 - Objednat zboží, přijmout a zaplatit fakturu
- **Analýzu** SoD na úrovni autorizačních objektů a kompenzačních kontrol
- **Aktualizaci seznamu** nově připravených transakcí (custom transakcí)
- **Kvalitu kompenzačních kontrol** v případě identifikovaného SoD konfliktu
- **Přípravu SAP rolí**, které akceptují SOD a jsou v souladu s organizační strukturou

- **Definovat procesy**, které umožní zhodnotit přiřazení rolí před tím, než jsou přiděleny uživatelům
- **Nastavení SAP bezpečnosti** zodpovídá IT a ostatní specializovaná oddělení – hranice není úplně přesná.

		AP Voucher Entry AP Payments AP Release Blocked Inv AP Clear Vendor Acct. Vendor Mast. Maint. FI Vendor Mast. Maint. MM Vendor Mast. Maint. CEN Bank Reconciliation AR Cash Application AR Clear Customer Acct. Material Master Maint. Service Master Maint. Requisitioning Release Requisition Process Requisition Purchase Order Entry Purchasing Agreement																
Task Group Description	Grp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	14A	15	16
AP Voucher Entry	1		X	X	X	X	X	X									X	X
AP Payments	2	X				X	X	X	X								X	X
AP Release Blocked Inv	3	X															X	X
AP Clear Vendor Acct.	4	X															X	
Vendor Mast. Maint. FI	5	X	X				X										X	X
Vendor Mast. Maint. MM	6	X	X			X											X	X
Vendor Mast. Maint. CEN	7	X	X														X	X
Bank Reconciliation	8		X							X								
AR Cash Application	9								X									
AR Clear Customer Acct.	10																	
Material Master Maint.	11													X			X	X
Service Master Maint.	12													X			X	X
Requisitioning	13											X	X		X		X	X
Release Requisition	14													X			X	X
Process Requisition	14A													X			X	X
Purchase Order Entry	15	X	X	X	X	X	X	X				X	X	X	X			
Purchasing Agreement	16																	



Parametry pro SAP účty

Pro nastavení parametrů SAP účtů je třeba zohlednit následující:

- Samozřejmostí je **správně nastavená politika hesel**
- **Nestandardní dialogové účty** – např. servisní, RFC či jiné technické účty
- **Temporary** – dočasně alokované účty jak z technických, tak z procesních důvodů
- Účty pro **vzdálený přístup** z jiné sítě
- Účty pro „**cestující**“ **uživatelé** a třetí strany
- **Základní bezpečnostní parametry** pro řízení uživatelských účtů v SAP – např. jmenná konvence, politika hesel, používané typy uživatelských účtů

- **Silné SAP účty** tzv. standardní – vždy zamčené
- Ponechání **hesla** pro uživatele SAP*, DDIC

The screenshot displays the SAP User Maintenance (SU01) interface for user TESTUSER. The 'Parameters' tab is selected, showing fields for Alias, User Type (Dialog), and Password. The Password section includes a warning that the password must be changed by the user and a checkbox for 'System Differentiates Between Upper- and Lower-Case'. The 'Initial password' and 'Repeat password' fields are filled with asterisks. The 'User Group for Authorization Check' section is also visible at the bottom.



Silné SAP účty

Silné SAP účty:

- Umožňují **nadstandardní operace v SAP** s omezenou možností monitoringu a kontroly
- účty jsou určeny jen pro **řešení závažných problémů**
- je **nutná kontrola** nad jejich užíváním a přidělováním
- Jedná se jednak o **standard** SAP účty, tak o **specifická oprávnění** navržená např. pro konverzi dat nebo customizaci systému
- Silné SAP účty – vždy zamčené
- Např. uživatelé SAP*, EarlyWatch a DDIC

The screenshot shows the SAP User Information System interface. The 'Structure' pane on the left highlights 'Users by Complex Selection Criteria'. The main window displays 'Users by Complex Selection Criteria' with a summary table and a detailed user list.

Number of Users Selected: 2

System	NL5	Client	200	Checked By	MFRTSCH	23.10.2012	18:38:10
Selection Criteria:							
User	I	EQ	DDIC				
	I	CP	SAP*				
	I	EQ	EARLYWATCH				

User	Full Name	Group	Account no	Locked	Reason	Valid from	Valid to	User Type	Ref. User
SAP*	SAP sap	SUPER						A Dialog	
SAPKPMG								A Dialog	



Silná SAP oprávnění a citlivé transakce v SAP

Silné SAP role a profily:

- **Vybrání uživatelé** (zejména IT) mají část přístupu, který umožňuje jak administraci systému, ale i vlastní práci, která je v gesci běžných zaměstnanců
 - **Vývoj** dostatečně silných rolí a vhodných kompenzačních kontrol
 - Zajistit, že IT uživatelé **nebudou mít přístup** k business transakcím
 - Zaměřit se na **přístupová oprávnění** těchto silných uživatelů
 - Zhodnotit **efektivitu kompenzačních kontrol**
 - **Kontrola** silných SAP oprávnění (silné SAP role a účty)
 - Profily SAP_ALL, S_A*, SAP_NEW
- **Kontrola oprávnění** k citlivým transakcím v SAP
 - Např. autorizace pro zúčtování a/nebo zrušení faktury
 - editace bankovních účtů, generování platebního příkazu
 - přístup k SAP reportům a jejich editace
 - přístup k SAP tabulkám

Parameter Name	User-Defined Value	Sys
ApplianceType		
DIR_ATRA	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_AUDIT	F:\usr\sap\NL5\DVEBMGS00\log	F:\u
DIR_BINARY	F:\usr\sap\NL5\DVEBMGS00\exe	F:\u
DIR_CCMS	F:\usr\sap\CCMS	F:\u
DIR_CLIENT_ORAHOME		
DIR_CT_LOGGING	F:\usr\sap\NL5\SYS\global	F:\u
DIR_CT_RUN	F:\usr\sap\NL5\SYS\exe\uc\NTAMD64	F:\u
DIR_CT_SAPJVM	F:\usr\sap\NL5\SYS\exe\jvm\NTAMD64\sapjvm	F:\u
DIR_DATA	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_DBMS	F:\usr\sap\NL5\SYS\SAPDB	F:\u
DIR_EPS_ROOT	\\NLACCAPP24\sapmnt\trans\EPS	\\N
DIR_EXECUTABLE	F:\usr\sap\NL5\DVEBMGS00\exe	F:\u
DIR_EXE_ROOT	F:\usr\sap\NL5\SYS\exe	F:\u
DIR_EXTRACT	F:\usr\sap\NL5\DVEBMGS00\data	F:\u
DIR_GEN	F:\usr\sap\NL5\SYS\gen\dbg	F:\u



Pro nastavení parametrů SAP účtů je třeba zohlednit následující:

- **Přidělování oprávnění a řízení změn** v přístupech v SAP – procesní zajištění
- **Definované role** nebo skupiny rolí na jednotlivé pozice
- Oprávnění poskytnutá non-Dialog účtům, například service účtům
- **Pravidelná revize citlivých oprávnění** – např. možnost přístupu do SAP tabulek, job scheduling nebo citlivé business transakce – např. platební příkaz, možnost měnit čísla bankovních účtů

- Dočasné / Temporary účty skutečně přidělovat na dobu omezenou
- SSO vs SAP GUI přístup a nastavení hesla pro přístup

User Maintenance: Initial Screen



User

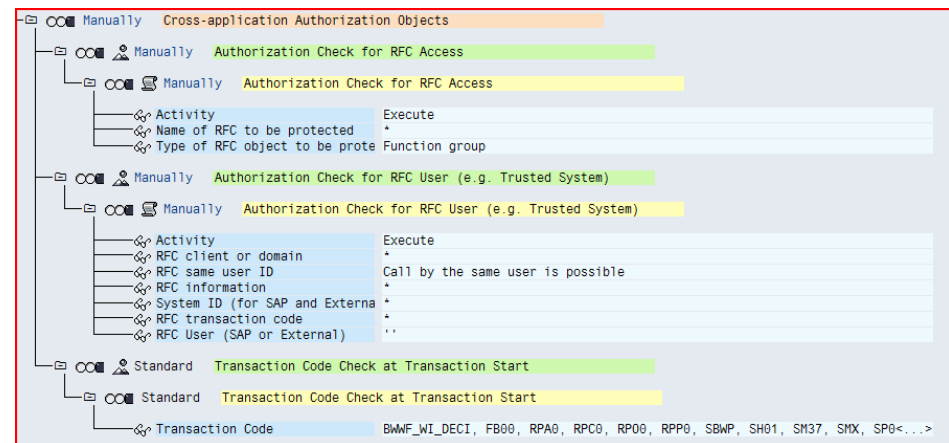
Alias



SAP Role a jejich vývoj

Při správě SAP rolí je třeba zohlednit následující:

- Kontrola nad procesem změn nebo vývojem SAP rolí je **základ pro bezpečnost dat** v SAP systému
- Nekontrolované změny v SAP rolích mohou způsobit **narušení celého autorizačního konceptu** i nastavení bezpečnosti SAP
- Změny a přidání SAP transakcí
- Nové **naprogramované transakce a autorizační objekty**
- Nové role by měly projít testem na citlivé transakce a testem na SOD
- **Kontrola firemních politik**, procedur a bezpečnostních standardů
- Nastavení **vnitřních bezpečnostních procesů** společnosti
- **Standardizované změnové řízení** vyžadující autorizaci změn před uvolněním do produkčního prostředí





Možnost analýzy dat v SAP

Vyšší efektivita

- Redukce duplicitních prací
- Širší možnost identifikovat a napravit chyby
- Užití automatizace

Korekce chyb

- Monitorování nedostatků a jejich předcházení či odstranění
- Automatická prevence podvodů

Včasné informace

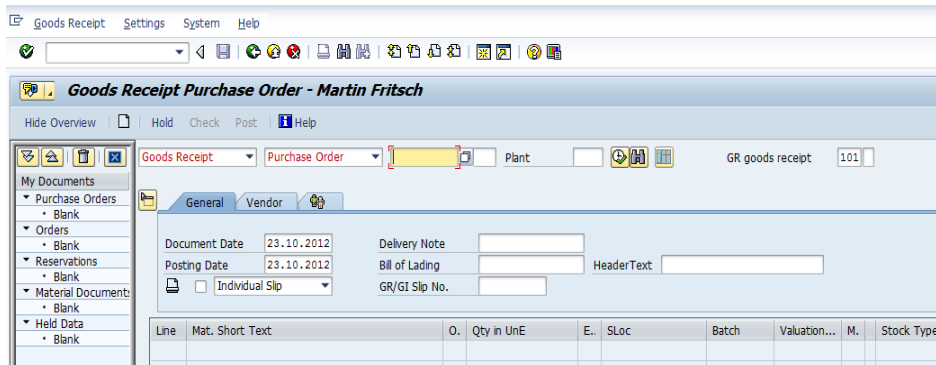
- Redukce překvapivých zjištění
- Zvýšená rychlost předání informací auditorům a businessu

Základní kroky analýzy dat

Příprava a definice KPI	Získání dat	Analýza a zpracování dat	Reporting
▪ Zahájení – Definice přístupu, rozsahu, harmonogramu, cílů a plánování ▪ Plán získání dat – Prověření SAP prostředí a rozsahu ▪ Technická příprava – Definice potřebných SAP tabulek a reportů	▪ Získání dat – Extrakce relevantních informací ze systému SAP ▪ Uložení dat na relevantním úložišti ▪ Spuštění dohodnutých reportů a metrik (podle stanovených KPI) ▪ Příprava reportů	▪ Analýza dat – Analýza a zhodnocení identifikovaných trendů – Ověření prvních výsledků s vedením společnosti ▪ Analýza procesů prostřednictvím interview s vlastníky procesů a vedením společnosti ▪ Identifikace prostoru pro zlepšení	▪ Sestavení reportu včetně výstupu z analýzy dat a doporučení pro zlepšení ▪ Ověření reportu s odpovědným managementem ▪ Finalizace reportu ▪ Vytvoření plánu dalších kroků

Možnost analýzy dat v SAP

- Manuální změny vystavených faktur
- Jednorázový zákazník
- Jednorázový dodavatel
- Manuální účtování do deníku
- Změny v skladové evidenci, analýza skladových pohybů
- Aging pohledávek
- Změna platebních podmínek
- Neaktivní účty hlavní knihy
- Analýza skladových pohybů prostřednictvím MIGO transakce



Goods Receipt Purchase Order - Martin Fritsch

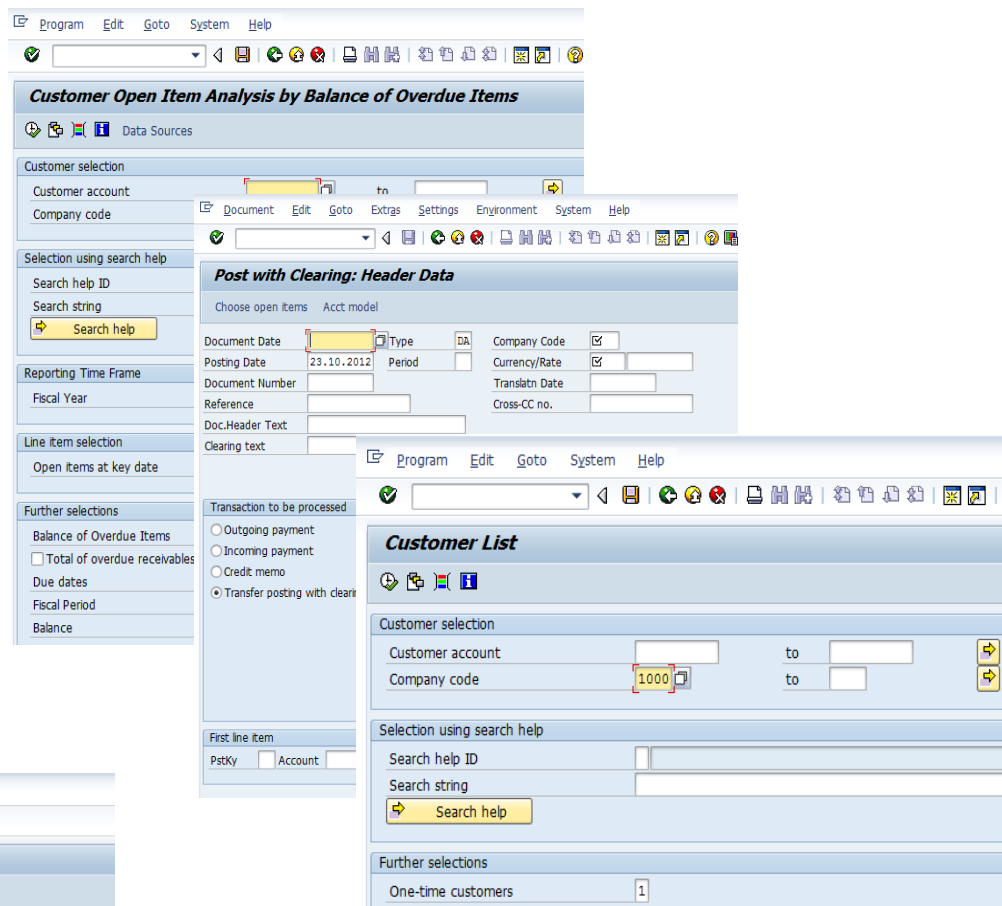
Hide Overview | Hold | Check | Post | Help

Goods Receipt | Purchase Order | Plant | GR goods receipt | 101

General | Vendor

Document Date: 23.10.2012 | Delivery Note | Posting Date: 23.10.2012 | Bill of Lading | HeaderText | GR/GI Slip No. | Individual Slip

Line	Mat. Short Text	O.	Qty in UnE	E.	SLoc	Batch	Valuation...	M.	Stock Type
------	-----------------	----	------------	----	------	-------	--------------	----	------------



Customer Open Item Analysis by Balance of Overdue Items

Customer selection

Customer account | Company code

Selection using search help

Search help ID | Search string | Search help

Reporting Time Frame

Fiscal Year

Line item selection

Open items at key date

Further selections

Balance of Overdue Items

☐ Total of overdue receivables

Due dates

Fiscal Period

Balance

Post with Clearing: Header Data

Choose open items | Acct model

Document Date | Type | DA | Company Code | Currency/Rate | Translatn Date | Cross-CC no.

Posting Date: 23.10.2012 | Period | Doc. Number | Reference | Doc. Header Text | Clearing text

Transaction to be processed

☐ Outgoing payment

☐ Incoming payment

☐ Credit memo

☒ Transfer posting with clearing

First line item

PstKy | Account

Customer List

Customer selection

Customer account | to | Company code | 1000 | to

Selection using search help

Search help ID | Search string | Search help

Further selections

One-time customers | 1



Bezpečnost systému SAP - shrnutí

Analýza SOD a kompenzačních kontrol

- Např. oprávnění změnit kmenová data dodavatele a zároveň proplatit fakturu
- Kvalita kompenzačních kontrol v případě identifikovaného SoD konfliktu

Základní bezpečnostní parametry pro řízení uživatelských účtů v SAP (např. jmenná konvence, politika hesel, používané typy uživatelských účtů)

- Ponechání hesla pro uživatele SAP*, DDIC
- Využívání non-Dialog účtů pro běžnou práci

Kontrola silných SAP oprávnění (silné SAP role a účty)

- Uživatelé SAP*, EarlyWatch a DDIC
- Profily SAP_ALL, S_A*, a SAP_NEW

Kontrola oprávnění k citlivým transakcím v SAP

- Např. autorizace pro zúčtování a/nebo zrušení faktury, editace bankovních účtů, generování platebního příkazu, přístup k SAP reportům a jejich editace, přístup k SAP tabulkám

Kontrola firemních politik, procedur a bezpečnostních standardů

- Nastavení vnitřních bezpečnostních procesů společnosti
- Standardizované změnové řízení vyžadující autorizaci změn před uvolněním do produkčního prostředí

The screenshot displays two SAP development tools side-by-side. The top window is the 'ABAP Editor: Initial Screen' with a menu bar (Program, Edit, Goto, Utilities(M), Environment, System, Help) and a toolbar. The 'Program' field contains 'RFDSLDD00' and a 'Create' button is visible. The 'Subobjects' list on the left includes 'Source Code', 'Variant', 'Attribute', 'Document', and 'Text'. The bottom window is the 'Data Browser: Initial Screen' with a menu bar (Table, Edit, Goto, Settings, Utilities(M), System, Help) and a toolbar. The 'Table Name' field contains 'KONTB1'.

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Leoš Černý
KPMG Česká republika
lcerny@kpmg.cz

