



Living a healthy life.

Upravljanje dostopov in avtorizacij v SAP okolju z uporabo SAP GRC Access Control

Robert Biličič

Junij 2008



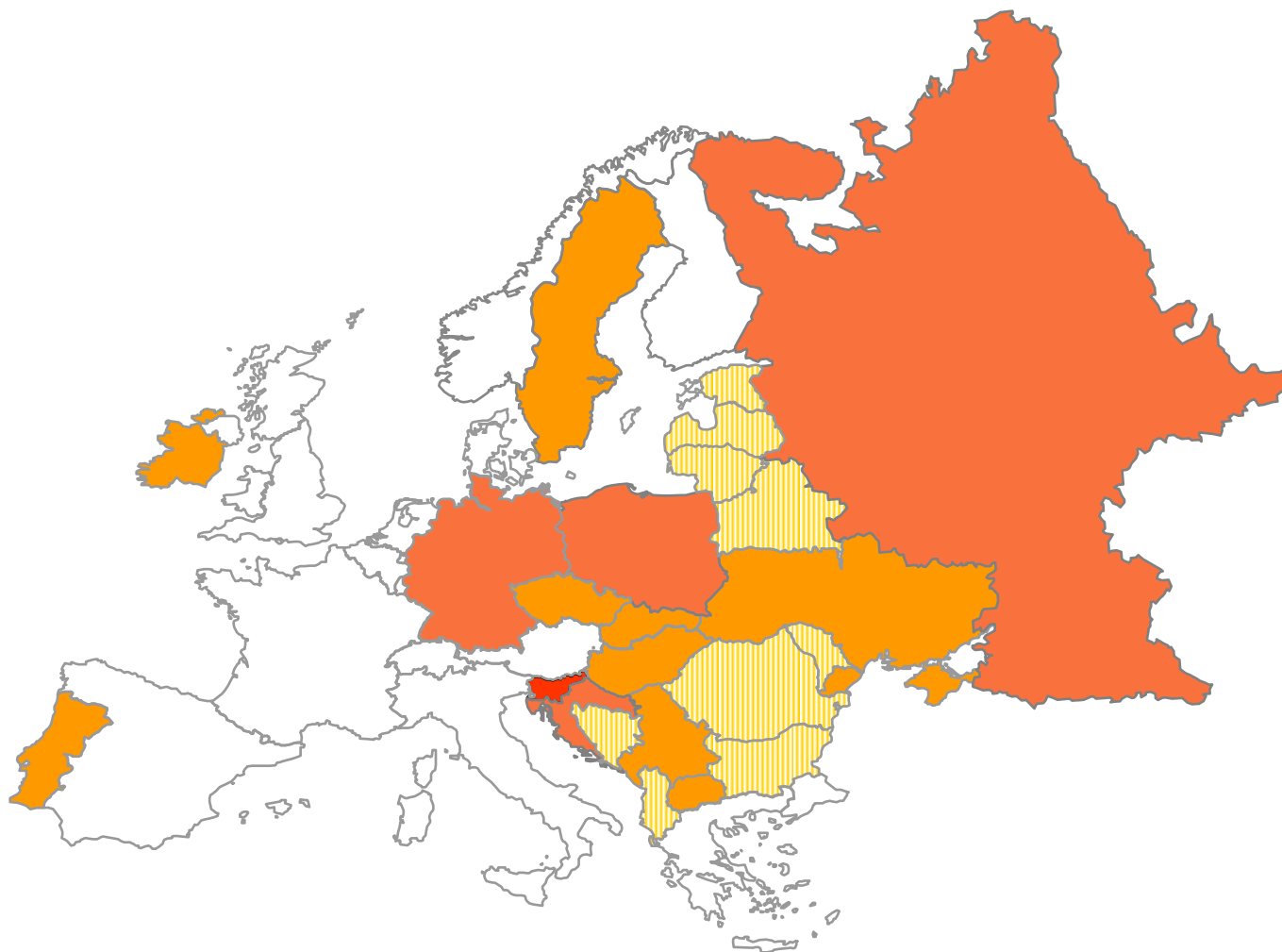
Covering the markets from Vladivostok to Lisbon

Subsidiaries abroad

GERMANY: TAD Pharma GmbH, Cuxhaven
 RUSSIAN FEDERATION: OOO KRKA - RUS, Moscow,
 OOO KRKA FARMA, Sergiev Posad
 POLAND: KRKA - POLSKA, Sp. z o.o., Warsaw
 UKRAINE: DP KRKA UKRAINA, Kiev
 CZECH REPUBLIC: KRKA ČR, s. r. o., Prague
 SLOVAKIA: KRKA Slovensko, s.r.o., Bratislava
 CROATIA: KRKA - FARMA, d.o.o., Zagreb
 HUNGARY: KRKA Magyarország Kft., Budapest
 SERBIA: KRKA - FARMA, d.o.o., Novi Sad
 IRELAND: Krka Pharma Dublin Limited., Dublin
 MACEDONIA: KRKA - FARMA DOOEL, Skopje
 SWEDEN: KRKA SVERIGE AB, Stockholm
 USA: KRKA USA LLC, Delaware
 PORTUGAL: KRKA Farmacêutica Lda., Estoril

Representative offices

Albania	Kosovo
Azerbaijan	Latvia
Belarus	Lithuania
Bosnia and Herzegovina	Moldova
Bulgaria	Romania
China	Russian Federation
Estonia	Serbia
Georgia	Slovakia
India	Ukraine
Kazakhstan	Uzbekistan



■ production subsidiaries
 ■ other subsidiaries
 representative offices



Upravljanje tveganj

- **Sarbanes-Oxley Act 2002** - zagotavljanje ažurnega finančnega poročanja (Enron, Artur Andersen, WorldCom) – velja tudi za Evropska podjetja, ki poslujejo na US tržišču – **SOX Compliant; COSO in ISO 17799** – enterprise risk management framework
- **Basel II** – access control, configuration control, user monitoring and management, ...(Society General, Bearings, UBS)
- Slovenija: finančna zakonodaja, dostop do notranjih informacij (pravila borze), varovanje osebnih podatkov, HR
- Farmacevtska industrija:GxP zahteve; CFR 21 Part 11
- **ISO 27001** – Information Security Management

SAPPHIRE 2008 Berlin



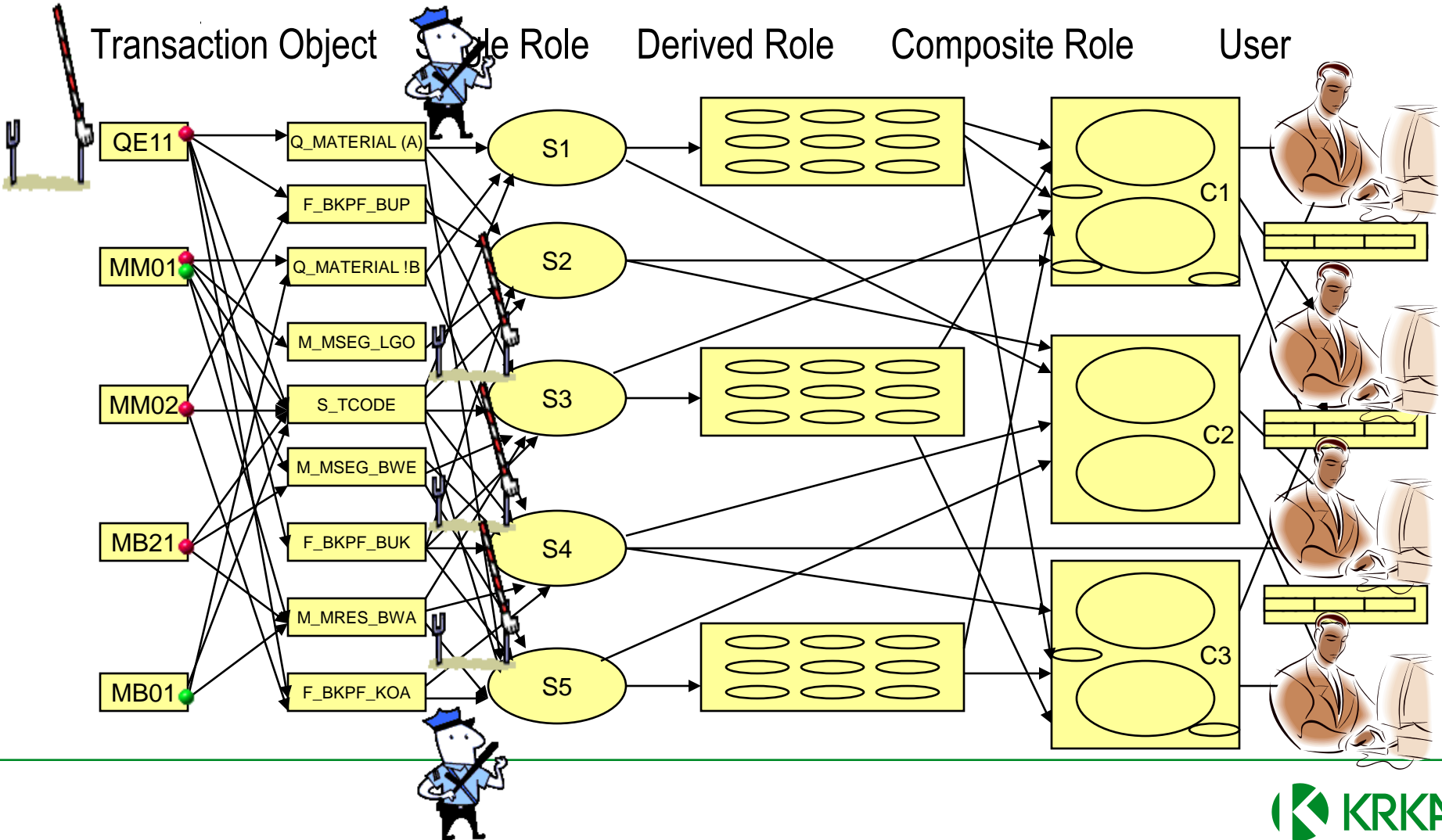
Cilji implementacije

- **Controlled Environment**
- **Transparent and Reliable End-User Provisioning**
 - Central System for all User Change Requests (R/3, BI, SCM)
 - “What-if” simulation / Proactive Risk Analysis
- **Reduced and Reliable Authorization Validation Testing**
- Easier Role Maintenance Support
- **Transaction Ownership – Business Process Owners responsibility**
- **Transparent and Accurate List of Users with Business- and GMP-Critical Transactions**
 - Alerts and Monitoring
 - Super-User Controlled Access for External and Internal Support
- Easier and Transparent Documentation of Business- and GMP-Critical Roles and Transactions
- **Enabling efficient environment, capable adopting quick changes in business process**

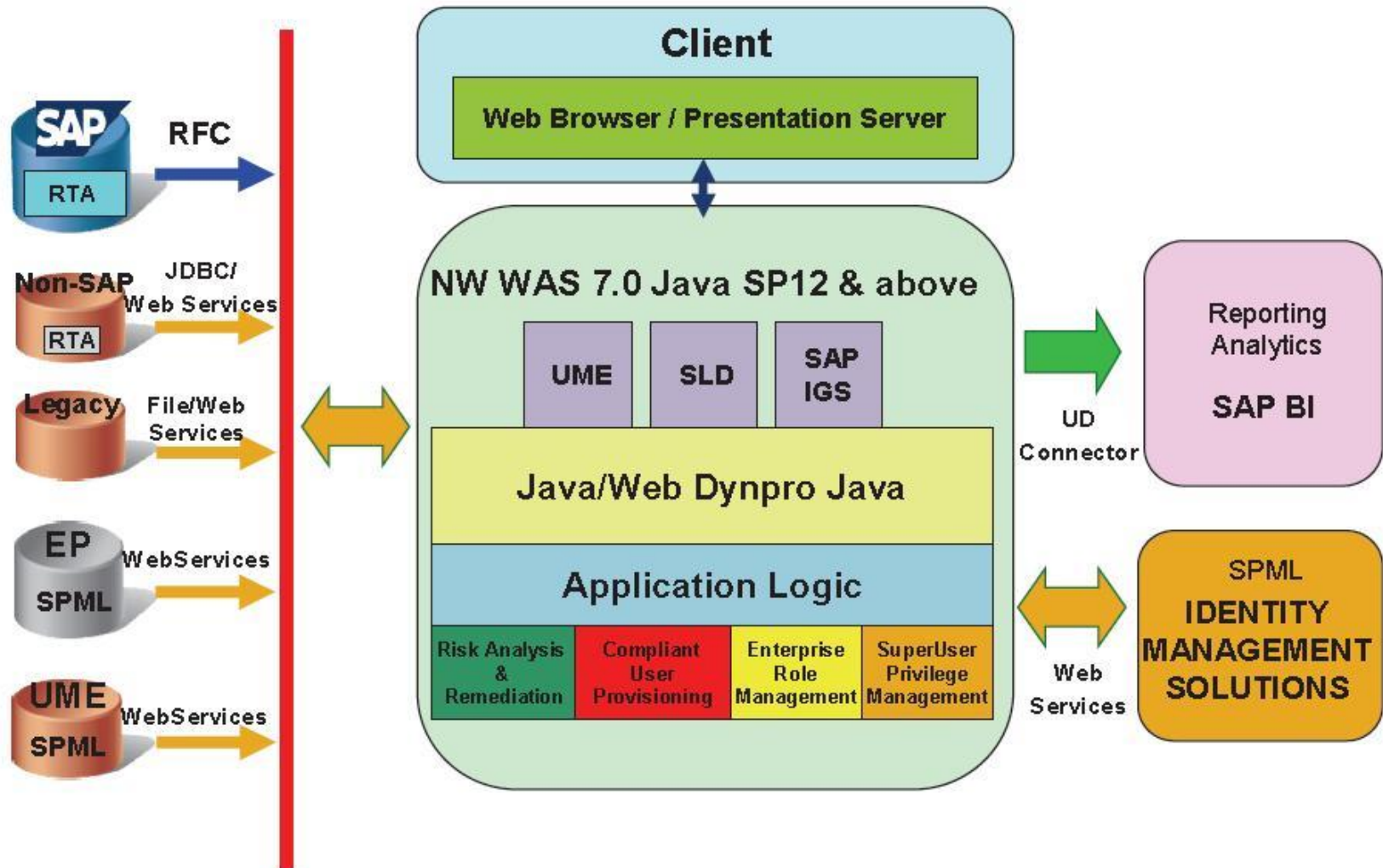
Tehnični izzivi

- 77.833 Transactions (276 /KRKA/...)
- 1.540 Authorization Objects
- 1500 Users
- 963 Roles
(701 Single Roles, 262 Composite Roles)
- Complex Matrix

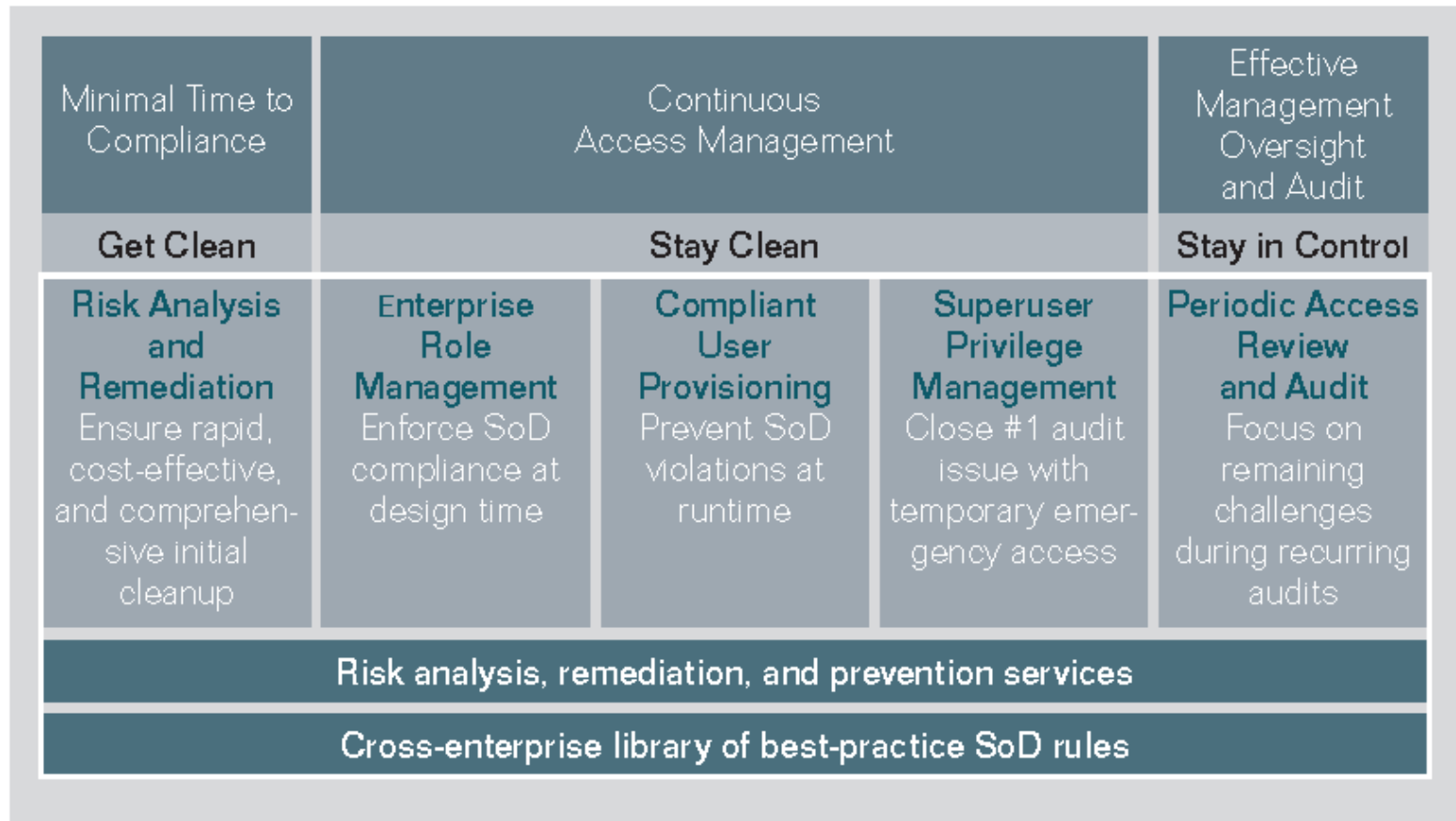
Real-time Compliance 24x7...



Access Control Component Architecture



SAP GRC Access Control



Implementation of SAP GRC Access Control Suite



- **Risk Analysis And Remediation**
(Compliance Calibrator)
- **Enterprise Role Management**
(Role Expert)
- **Superuser Privilege Manager**
(FireFighter)
- **Compliant User Provisioning**
(Access Enforcer)

Rezultati

- Maintenance and Documentation of Business- and GMP-Rules
- Implementation of Information Source Ownership (Transactions and Authorization Objects)
- Defined workflows for User-, Role and Risk-Change Requests including the usage of electronic signature according to the requirements of CFR 21 part 11

Produkcijske izkušnje

Reduced Maintenance Effort for User- and Role- Change Requests :

- Average time until request is processed and closed: 1 week before versus 1 day after Implementation
- No Interference by the Technical Team now versus min. half an hour before the Implementation
- Business is now responsible for Change Requests, not the Technical Team any more

FireFighter:

- Less Effort by Technical Team for Maintenance of Emergency-User
- Less Effort by Auditors to review the Audit Logs

Produksijske izkušnje - nadaljevanje

Reduced Auditing Effort for Risks in User and Role Access Rights:

- Average time per Audit: 2 weeks for collecting the information versus a couple of minutes to collect
- Risk Awareness was created: Risks were known before but Business Process Owners were not AWARE of risks

Ramp-Up 5.2 and 5.3 - Razlogi

Ramp-up 5.2

- Special Characters / Unicode Support
- Role Expert


Ramp-up 5.3

- All fields in SU01 are now fully supported
- UME / Portal Authorizations are now supported
- SSO to all GRC AC Applications - Launch-Pad
- Role Expert: Direct Connection to PFCG

Still Missing:

- All requests starts in AE (for risk, role, user, FF) change


Vnos zahtevka



SAP GRC Access Control
Compliant User Provisioning

Welcome Robert Biličič


[Help](#) | [About](#) | [Log Off](#)



Request Access:

Welcome to the Request Access page

Help is available for each link; click the link located on the top of this page



- **Change Account:** You can request changes to existing account using this link. You can request additional access and other changes to an account such as account validity etc. Sprememba pravic obstoječemu uporabniku.
- **NEW_HIRE:** Zahteva za kreiranje novega uporabnika v SAP sistemih - uporabnik še nima prijave za SAP sisteme.
- **Information:** Does not know which link to select from above? Simply click this link and provide information about what access you need.
- **Lock Account:** You can use this link to request locking of accounts in various systems. You can also request mass locking of accounts.
- **Unlock Account:** You can use link to request unlocking of accounts. You can also request mass unlocking of accounts.
- **ROLE CREATE/CHANGE:** Zahtevek za spremembo vloge
- **Superuser Access:** You can use a link to request Superuser Access
- **RISK_MITIGATION_CREATE_CHANGE:** Risk, Mitigation Create Change Request
- **Password Self-Service** Use this link to reset or request to change the password

Vnos zahtevka - nadaljevanje

Create Request

General Information

Request Type*

Priority*

Due Date

Employee Type

User ID

Last Name*

First Name*

E-Mail Address*

Telephone

Company

Functional Area

Requestor and Manager Information

Requestor Last Name*

Requestor First Name*

E-Mail Address*

Manager Last Name

Manager First Name

E-Mail Address

Application*

Type	Short Description	Category

[+ More](#)

Roles/Profiles
PD Profiles
Risk Violations
Mitigation
SuperUser Access
Comments
Request Justification
Attachments

System Type	System	Role/Profile Name	Type	Role/Profile Description	Valid From	Valid To	Approver	Action

Approve

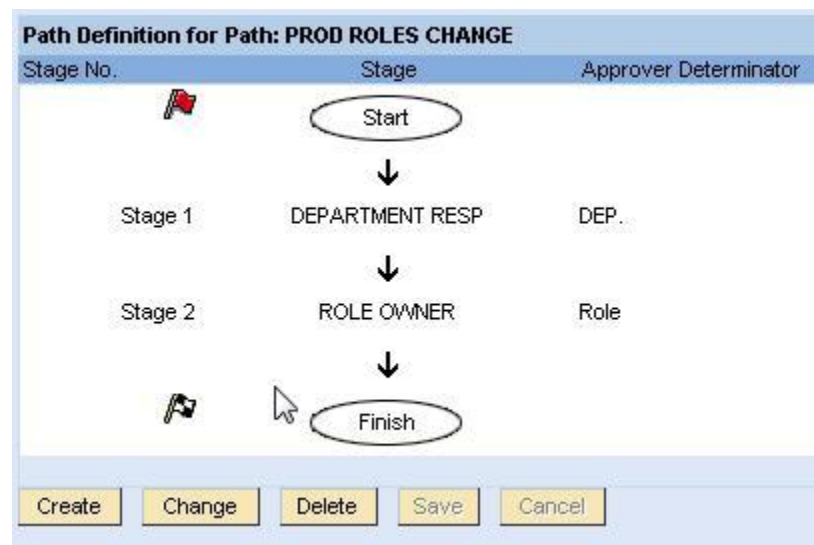
Risk Analysis

Select Roles

Select SuperUser Access

Select PD Profiles

Pot potrjevanja



Potrjevanje

Approval Path Status								
PROD CHANGE (Status : APPROVE)	1. DEPARTMENT RESP (Status : Approved)			2. ROLE OWNER (Status : Approved)				
	[Sonja Kermc(KERMCS)]			[Tomaž Mikec(MIKEC)]				
Request Status								
Request Number	3610		Status	Closed		Approval Due Date	12/31/9999	
General Information								
Request Type	Change Account		User Name	Viktorija Čatić(CATIC)				
Priority	Medium		E-mail address	Viktorija.Catic@krka.biz				
Employee Type	Enduser		Position					
Application	R3PCLNT400		Org. Unit					
Department	107216		Requestor	Tadej Grampovčan(GRAMPOVCAN)				
Business Process			E-mail address	tadej.grampovcan@krka.biz				
Company			Manager	Sonja Kermc(KERMCS)				
Valid From	04/16/2008		E-mail address	Sonja.Kermc@krka.biz				
Valid To	12/31/9999							
Additional information								
Job			Cost Center					
Personnel Number			Business Area					
Personnel Area			Request Category					
Location			Request Reason					
Telephone	2173		Functional Area					
Custom Fields								
Department1	107216							
Roles/Profiles								
<input checked="" type="checkbox"/>	System	Role/Profile Name	Type	Role/Profile Description	Valid From	Valid To	Approver	Action
<input checked="" type="checkbox"/>	R3PCLNT400	MM:A:REZERVACIJE:1000		Rezervacije 1000	04/16/2008	12/31/9999	Tomaž Mikec(MIKEC)	ADD

Upravljanje uporabnikov - poročila

Management Reports

Access Requests

Date From: 03/06/2006

To Date: 06/11/2008

System: All

Request Type: All

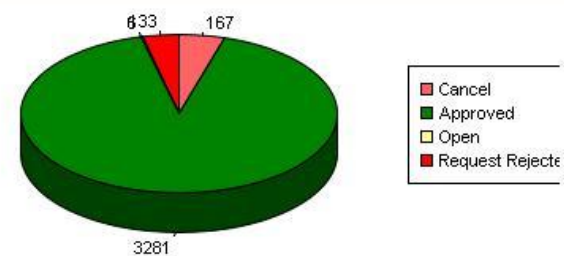
Priority: All

Functional Area: All

Workflow Type: Access Enforcer

Archived Requests:

Total Number of Requests: 3587



Request by Type

Date From: 03/06/2006

To Date: 06/11/2008

System: All

Status: All

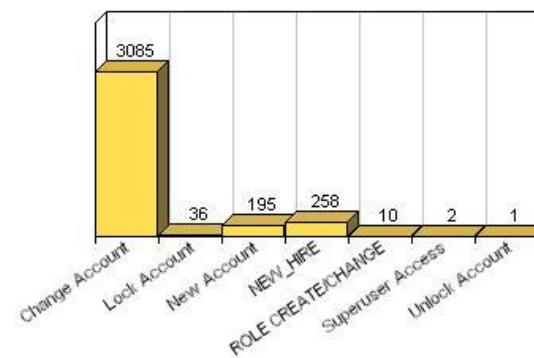
Priority: All

Functional Area: All

Workflow Type: Access Enforcer

Archived Requests:

Total Number of Requests: 3587



Risk Analiza - Poročila

Management View - Risk Violations

Summary as of 06-jun-2008

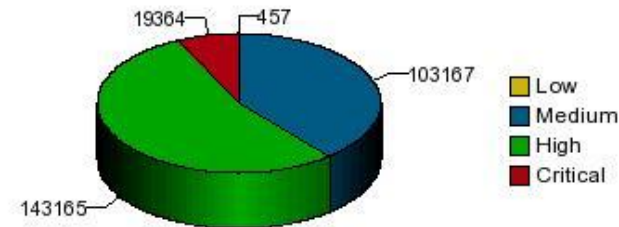
Risk Violations

Month/Year: 06/2008
 System: R3PCLNT400
 Analysis Type: User
 User Group: All
 Violation Count by: Permission

Go

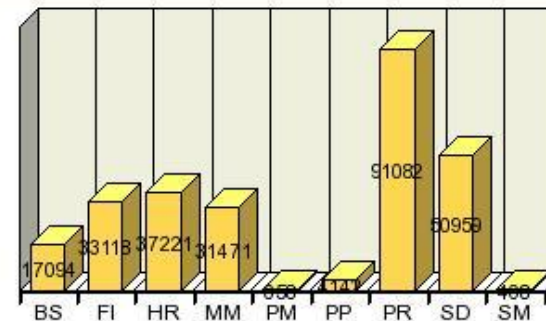
Number of Users Analyzed: 1,859

Total Number of Violations: 266,153



Risk Violations by Process

Process	Count	Percentage
Basis	17,094	6%
Finance	33,118	12%
HR and Payroll	37,221	14%
Materials Management	31,471	12%
PM - Vzdrzevanje	658	0%
PP - Production planning	4,142	2%
Procure to Pay	91,082	34%
Order to Cash	50,959	19%
Supply Chain Management	408	1%



Vprašanja ?

robert.bilicic@krka.biz

