

# SAP Governance, Risk & Compliance

## Implementation Challenges

Melissa Dielman – 07/09/2010



### Agenda

Why GRC?

SAP GRC Access Control

Success factors and pitfalls

Deloitte Implementation Approach

Q&A

## Agenda

### Why GRC?

SAP GRC Access Control

Success factors and pitfalls

Deloitte Implementation Approach

Q&A

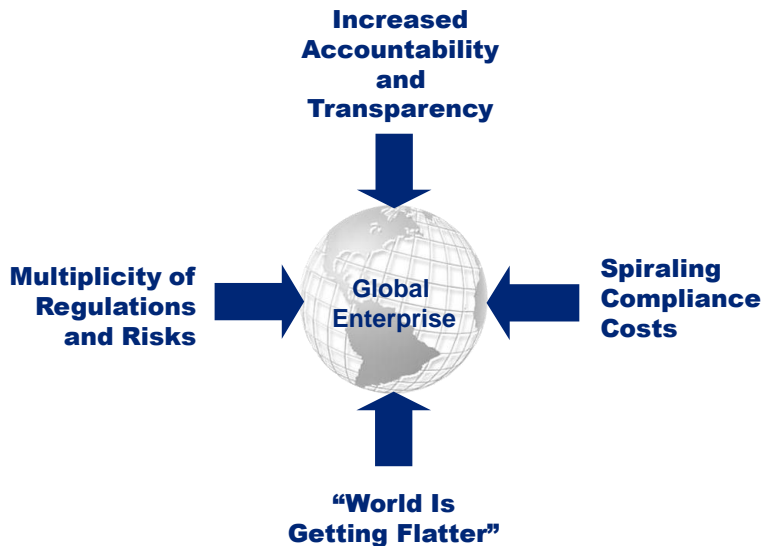
## Define Governance, Risk & Compliance

**G**overnance: ensuring complete & accurate management information & providing controls on the execution of management strategies

**C**ompliance with financial & trade regulations, data privacy legislation, contractual agreements

**R**isk related to strategic choices, your economic environment, injury & loss, data leakage, external factors,... that may jeopardize the realization of the organization's business objectives

## Pressures On Businesses Today



5

## Why do we care about Access Control?

### Common detected issues:

- **Expanding functionalities** and SAP platforms increase the need for proper access management
- **Growing companies** require an organization of access to local data vs central data
- User access and authorization controls for SAP and non-SAP systems is a **recurring Audit Item**
- User life cycle and authorization management **process is manual, error-prone** and not embedded in the organization (including lack of tooling)
- **Poor communication** between Business & IT results in "best-guess" approval of requests
- Segregation of Duties (SoD) **violations remain undetected** and uncorrected (shift of responsibilities, personnel moves, changes in organization...)
- Request for emergency access (super user) is ad hoc and **insufficiently monitored and controlled**

© 2010 Deloitte Belgium

## Objectives of Implementing a GRC strategy

- Reduce the potential of fraud and problems around financial reporting and business critical information
- Reduce the risk of asset or resource losses
- Comply with laws and regulations including those related to corporate governance, internal controls, risk management and data privacy
- Optimize business decisions by providing trustworthy information with high quality
- Improve operating efficiency

©2010 Deloitte Belgium

## Objectives for integrating SAP GRC Access Control

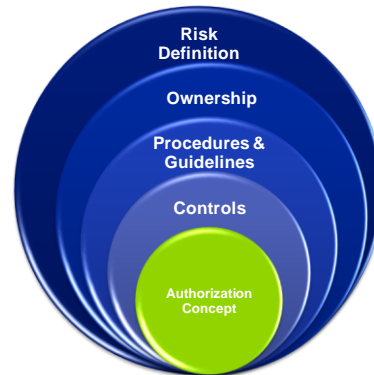
- Gain confidence that audit and compliance requirements are met
- Report on critical access violations: data, system maintenance & Segregation of Duties
- Provide visibility and control on access across business applications
- Establish a consistent, documented & possibly automated process for access management
- Achieve & maintain compliance at a lower cost

©2010 Deloitte Belgium

## Governance, Risk & Compliance

A comprehensive Governance, Risk & Compliance Approach is required to manage SAP Access Risk

- Risk Definition & Security Policy
- Ownership model
- User provisioning procedures
- Role management guidelines
- Internal Control Framework
- Solid, Flexible, SOD-conflict free authorization (role) structure



© 2010 Deloitte Belgium

## Agenda

### Why GRC?

### SAP GRC Access Control

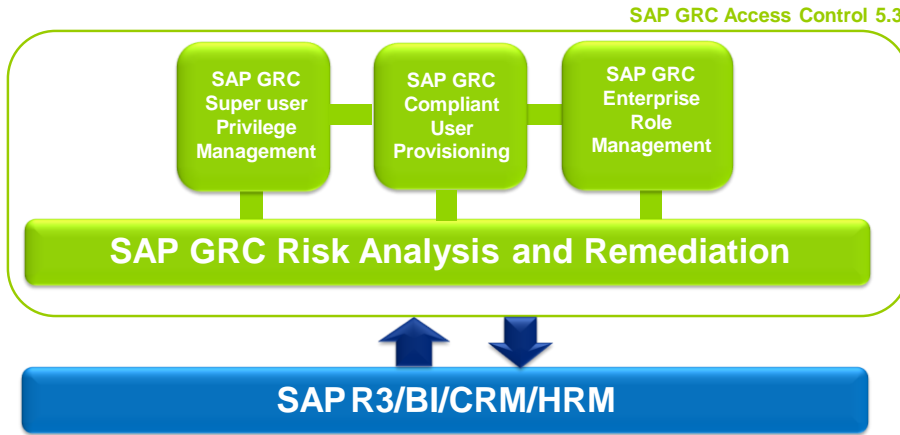
### Success factors and pitfalls

### Deloitte Implementation Approach

### Q&A

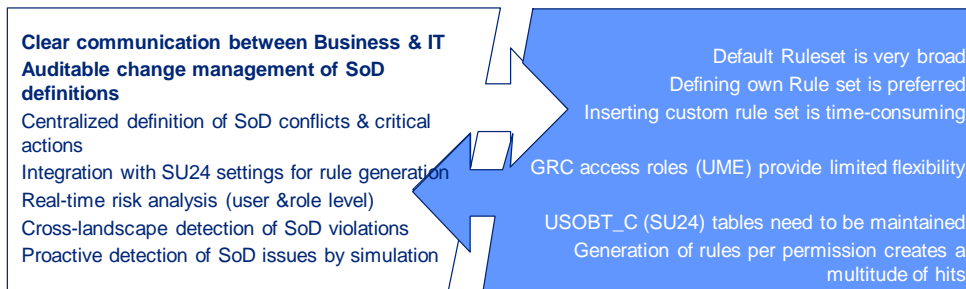
© 2010 Deloitte Belgium

## SAP GRC Access Control – 4 interacting modules



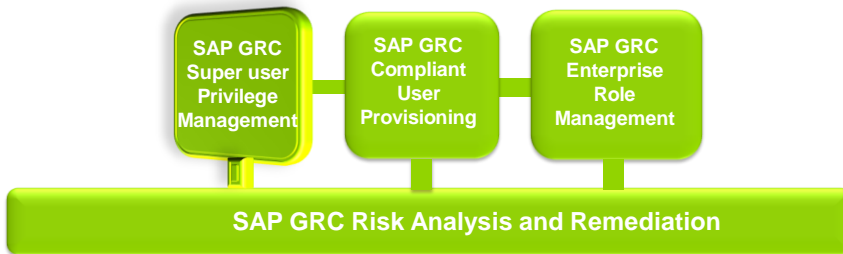
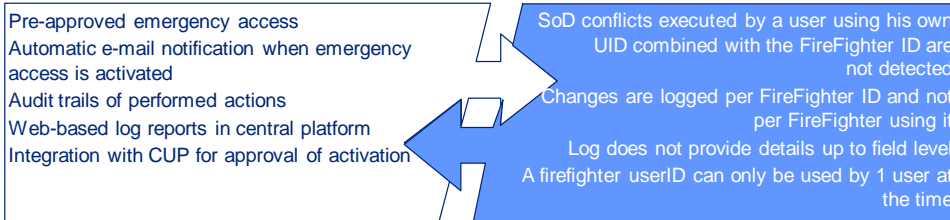
© 2010 Deloitte Belgium

## Risk Analysis & Remediation (RAR): Detect & Report Risk



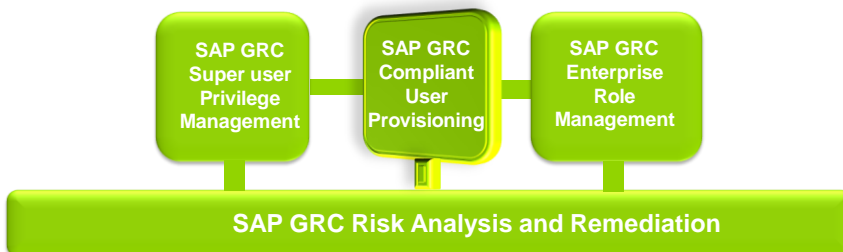
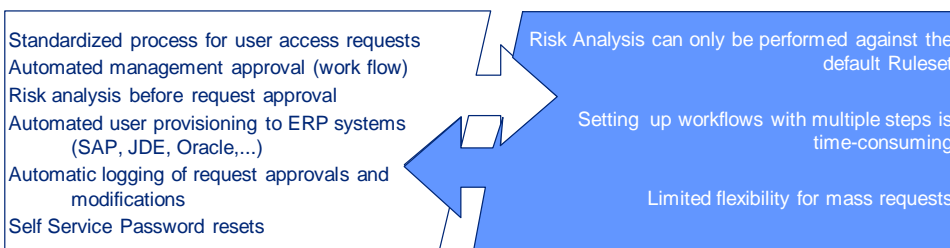
© 2010 Deloitte Belgium

## Super User Privilege Management (SPM): remove (Z)SAP\_ALL



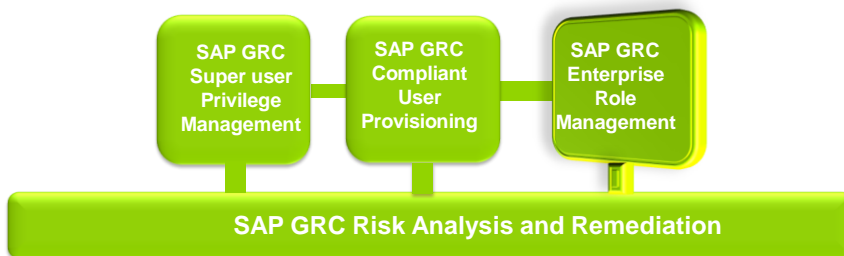
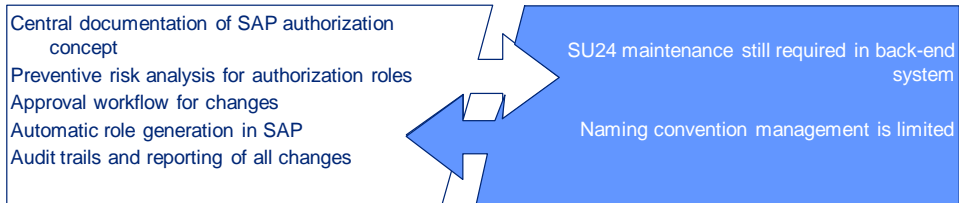
© 2010 Deloitte Belgium

## Compliant User Provisioning (CUP): automate, control & document



© 2010 Deloitte Belgium

## Enterprise Role Management (ERM): Enforce Concept Rules



© 2010 Deloitte Belgium

## Agenda

### Why GRC?

### SAP GRC Access Control

### Succes factors and pitfalls

### Deloitte Implementation Approach

### Q&A

© 2010 Deloitte Belgium

## Implementing SAP GRC Access Control

### *Critical Success Factors & pitfalls*

#### **Avoid the “Big Bang”**

- building out the GRC solution component by component allows to effectively absorb all parts of a sustainable solution.
- starting the monitoring & remediation with a limited number of high priority risks will ensure the results are manageable and tackle the most urgent issues.

#### **Business Challenges**

- shift of responsibility/ownership from the IT team to the BU's
- ownership of risks by business persons will increase awareness and effectiveness of the processes & tool
- support from appropriate levels of the organization will assist in addressing points of resistance

#### **Objectives**

- understanding the organization's key business objectives & goals is critical, since the GRC process needs to align and integrate with the overall business plan.

© 2010 Deloitte Belgium

## Implementing SAP GRC Access Control

### *Critical Success Factors & pitfalls*

#### **Expectation Management & ownership**

- make sure business understands the objectives and how the GRC process & tool supports this
- define key stakeholders & include them in requirement definitions
- project sponsor should be key business person (e.g. CFO, CRO)

#### **Timing**

- it is key that the business has achieved a certain level of maturity in both its SAP environment and the Risk awareness to ensure successful implementation, acceptance & ownership
- small successes are replicated & gradually extended across the organization, so the timing of when & where the organization begins to address key requirements will be important

#### **Ownership will have to grow - communication & involvement is key**

© 2010 Deloitte Belgium

## Implementing SAP GRC Access Control

### *Critical Success Factors & pitfalls*

#### **Resources**

- understanding the organization's key business initiatives will be critical, since multiple initiatives often compete for the same (business) resources
- SOD project team should integrate with business and IT organizations
- resources should include a mix of IT to run the tool and update authorizations and from the business to help evaluate exceptions and identify mitigating controls

#### **Solid foundations: Authorization Role concept**

- a solid authorization structure facilitates Access management substantially – any efforts to accomplish such a structure is to be a first priority activity.
- work sequentially: tackle your roles first, then you users
- don't make this a technical exercise: balance security with efficiency

© 2010 Deloitte Belgium

## Implementing SAP GRC Access Control

### *Critical Success Factors & pitfalls*

#### **Installation vs. Integration**

- installation and configuration of SAP GRC Access Control is the “easy” part; a successful integration in the organization requires a tailored definition & set-up of Risk ,Controls & Processes, which requires time and business & risk

## Agenda

### Why GRC?

### SAP GRC Access Control

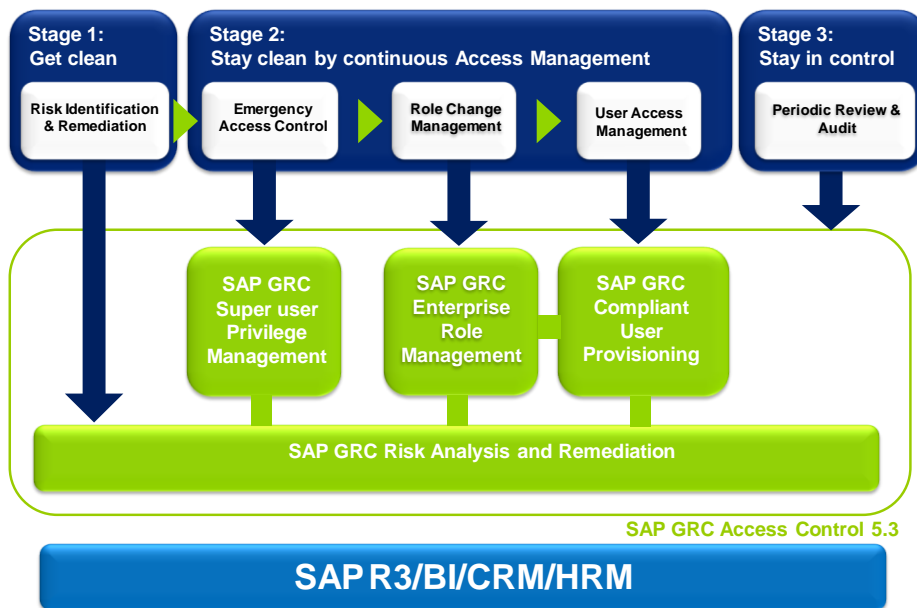
### Success factors and pitfalls

### Deloitte Implementation Approach

### Q&A

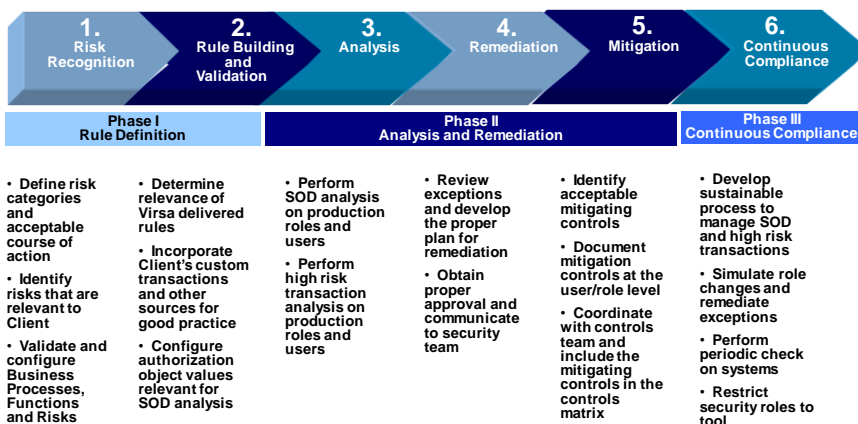
© 2010 Deloitte Belgium

### SAP GRC Access Control implementation



© 2010 Deloitte Belgium

## Access Risk Remediation Process: Get Clean



## Preparatory actions for Access Controls Implementations

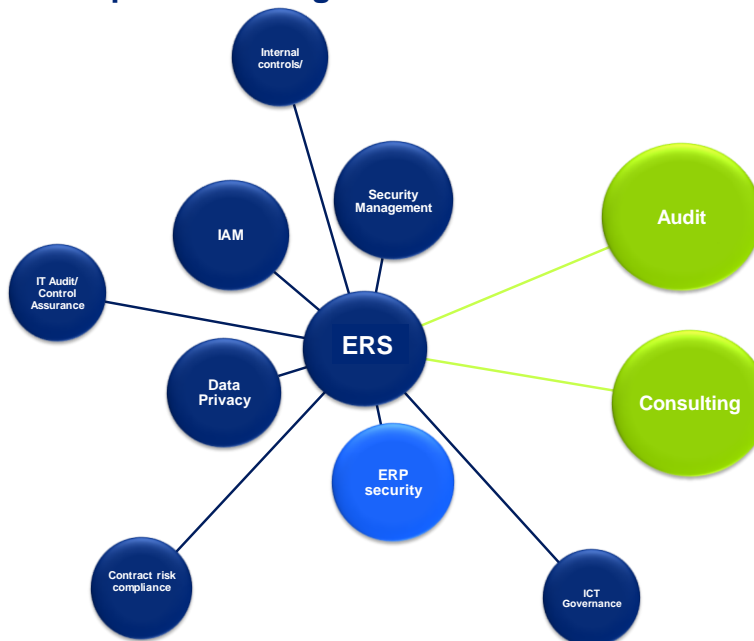


## Deloitte Value Proposition

|   |  |
|---|--|
| <p><b>Governance, Risk &amp; Compliance (GRC) is in our DNA</b></p> | <p>We are a consistent leader in Governance, Risk and Compliance, an area where selecting a strategic partner who has a deep understanding of Risk &amp; Security is fundamental. Deloitte can help creating a Governance, Risk and Compliance vision that is sustainable &amp; fits into to Company's mission statement</p> |
| <p><b>Deloitte SAP GRC initiative in Belgium</b></p>                | <p>Deloitte Belgium has built and invested in SAP GRC competence centres, including SAP GRC Risk Management, Access Control, Process Controls and Global Trade Services (GTS).</p>   |
| <p><b>Strong SAP Authorizations and SoD Expertise</b></p>           | <p>Our team includes people who have long-standing experience with implementing SAP authorizations, Segregation of Duties and internal controls in SAP environments, which will ensure a pragmatic approach and recommendations.</p>   |
| <p><b>Deloitte and SAP are global partners</b></p>                  | <p>Deloitte is the only traditional SAP implementation partner working collaboratively to develop and execute the GRC and CPM (Corporate Performance Management) program. This is thanks to our deep accounting, tax, compliance, risk and controls expertise</p>  |

© 2010 Deloitte Belgium

## Deloitte provides Integrated Services



© 2010 Deloitte Belgium

# Agenda

## Why GRC?

### SAP GRC Access Control

### Success factors and pitfalls

### Deloitte Implementation Approach

## Q&A

© 2010 Deloitte Belgium

Thank You

**Deloitte.**

**Melissa Dielman**  
Senior Manager

Deloitte Enterprise Risk Services  
Berkenlaan 8 b  
B-1831 Diegem  
België

Tel: +32 2 800 24 38  
Mobile: +32 470 56 20 63  
mdielman@deloitte.com

Member of  
Deloitte Touche Tohmatsu

**Deloitte.**

**Kris Wauters**  
Senior Consultant

Deloitte Enterprise Risk Services  
Berkenlaan 8 b  
B-1831 Diegem  
België

Tel: +32 2 800 27 33  
Mobile: +32 475 59 06 51  
kwauters@deloitte.com

Member of  
Deloitte Touche Tohmatsu

Deloitte Touche Tohmatsu  
Belgium

indiennin@deloitte.com  
Tel: +32 2 800 24 38  
Fax: +32 2 800 54 88

Senior Manager  
Melissa Dielman  
Berkenlaan 8 b  
B-1831 Diegem  
Belgium

**DELOITTE**

Deloitte Touche Tohmatsu  
Belgium

kwauters@deloitte.com  
Tel: +32 2 800 27 33  
Fax: +32 2 800 54 88

Senior Consultant  
Kris Wauters  
Berkenlaan 8 b  
B-1831 Diegem  
Belgium

**DELOITTE**

© 2010 Deloitte Belgium