

axl & trax

be you. we care.

LOSEC
LEADERS IN SECURITY

*Facing today's challenges
in
**SAP Security
and
GRC***

Wouter Janssen
<wouter.janssen@axl-trax.com>

March 24th, 2011

axl & trax



axl & trax
the name...



be you. we care.

© axl & trax. all rights reserved.

axl & trax

Agenda

- Securing SAP, what is the problem?
- Risk orientation
- Securing SAP
- Trends
- User security
- Governance, Risk & Compliance (GRC)
- Identity Management

be you. we care.

© axl & trax. all rights reserved.

axl & trax

1. Securing SAP

What is SAP?

- SAP is usually used to refer to the company SAP AG, its range of products (SAP ERP, R/3, ..)
- SAP products facilitate business processes and information flows within and between organizations
- Valuable assets are worth protecting



Define "SAP"

Define "valuable assets"

Assess risk

Decide on action

Action!



be you. we care.

© axl & trax. all rights reserved.

axl & trax

2. So what's the problem?

- Security is a means to safeguard company assets against threats
- Things that make SAP security a worthy challenge
 - Thousands of users world-wide
 - Business-critical system & process operation
 - Different processes and configuration in different sites
 - Multi-dimensional roles and responsibilities
 - Standard is a concept, not practice
 - Multi-layer, multi-component security
 - Interconnectivity, customizing and custom developments
 - Integrated systems, non-integrated organizations

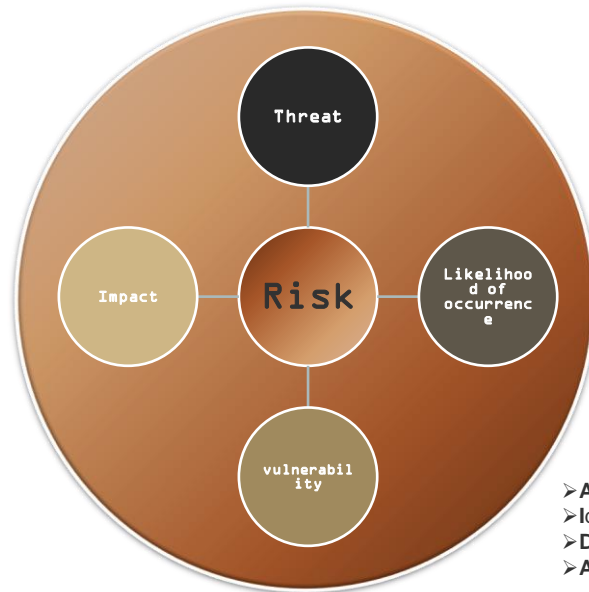
"Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security" - John Allen Paulos

be you. we care.

© axl & trax. all rights reserved.

axl & trax

3. Risk-based ↔ solution-based



- Assess risk
- Identify alternatives
- Decide on action
- Act

be you. we care.

© axl & trax. all rights reserved.

axl & trax

4. Securing SAP

What's your wish-list?

- ▮ Data protection
- ▮ Reliable process execution
- ▮ Availability of correct and complete data
- ▮ Secure & available applications, databases and servers
- ▮ Restricted user access
- ▮ Company policy or external (regulatory) compliance
- ▮ Enforcement of good practices
- ▮ Control and/or Cost-effectiveness



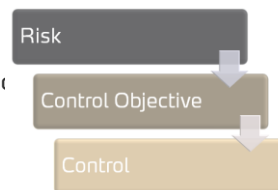
be you. we care.

© axl & trax. all rights reserved.

axl & trax

5. Trends

- User access rights to **protect**, not just **grant** access
- External **compliance** as a business driver
- Lower risk **appetite**
- Increased attention for **governance**
- Control through **automation**
- Prioritization of **fashionable** controls



be you. we care.

© axl & trax. all rights reserved.

axl & trax

6. User security

- User provisioning of authorization roles in SAP
- Building a good role is easy, building a good role **concept** is complex
- **Transparency** and **manageability** of roles are key for sustainable control
- Enterprises tend to define access rights by
 - Functionality (transactions)
 - Enterprise structure (organizational levels)
 - Detailed restrictions (document types, movement t ...)
 - Business function (sales, procurement, HR)
 - Position/function (sales manager)
 - individual

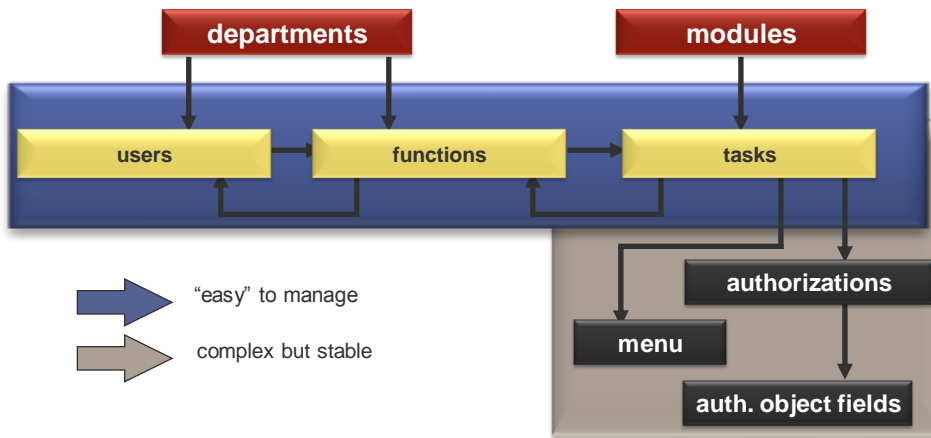


be you. we care.

© axl & trax. all rights reserved.

axl & trax

6ⁱ. User security: RBAC through functions & tasks



be you. we care.

© axl & trax. all rights reserved.

axl & trax

6ⁱⁱ. Maturity in user security

- **Enable** authorized staff and **protect** assets against misuse, error or fraud
- **Balance** between IT and business requirements
- Maintain **efficient** and **controlled** IT security processes
- Guarantee a consistent and transparent **security model**
- Ensure **compliance** with internal/external requirements
- Establish clear **ownership** and **responsibility**
- Stick to the **standards** (e.g., ITIL SO, COBIT, ISO27002, RBAC)
- Differentiate between **tactical** and **operational** user management



be you. we care.

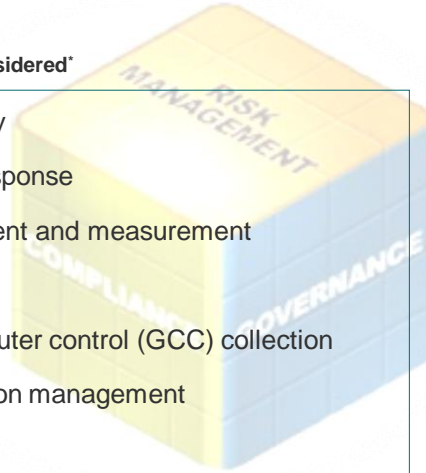
© axl & trax. all rights reserved.

axl & trax

7. Governance, Risk & Compliance

GRC areas/capabilities to be considered*

- Controls and policy library
- Policy distribution and response
- IT Controls self-assessment and measurement
- IT Asset repository
- Automated general computer control (GCC) collection
- Remediation and exception management
- Reporting
- Advanced IT risk evaluation and compliance dashboards



* Source: Gartner

be you. we care.

© axl & trax. all rights reserved.

axl & trax

7i. GRC - Segregation of duties

- **Segregation of duties** is the division of roles and responsibilities to reduce the possibility for a single individual to compromise a critical process
- An **organizational control** measure to reduce the chance of fraud and/or error whilst improving control
- Ensures that **at least two individuals** are involved in critical activities or in completion of a process
- Combinations of incompatible functions are usually referred to as “**SoD Conflicts**”
- Differentiate between **SoD Conflicts** and **Critical functionality**

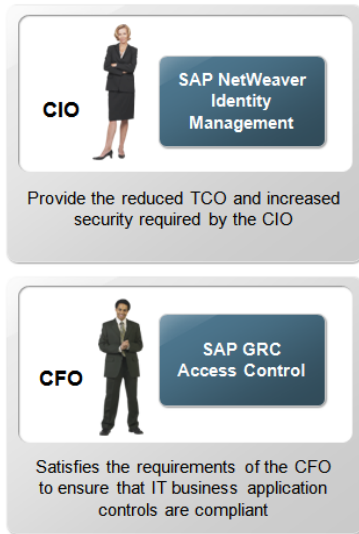


be you. we care.

© axl & trax. all rights reserved.

axl & trax

(SAP) Compliance breakdown



Compliant Identity Management

- Provides compliant Identity Management across SAP and heterogeneous landscape in one integrated solution
- Standards based integration creates tightly aligned, loosely coupled solution from complementary components
- Gives a consistent view on current and historic access rights, approvals and policy violations

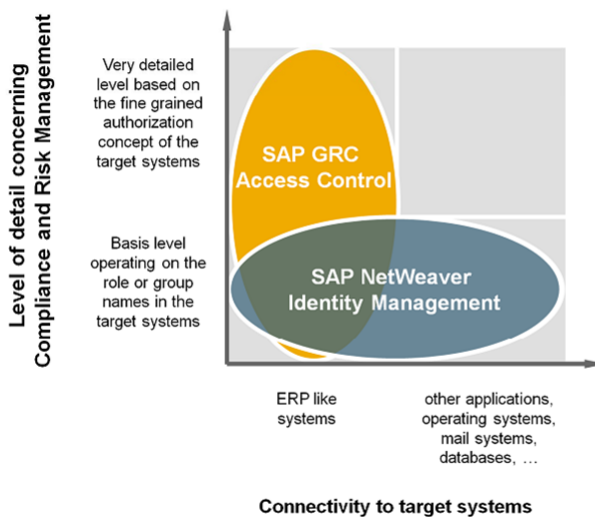
be you. we care.

© axl & trax. all rights reserved.

© SAP AG - all rights reserved

axl & trax

Scope SAP GRC vs. SAP IdM



Compliant Identity Management

- NetWeaver Identity Management provides:
 - Heterogeneous connectivity
 - Powerful business role mapping
 - Identity lifecycle management
- GRC Access Control provides:
 - Pre-defined business rules
 - "Informed" segregation of duty checking
 - ERP role creation & management
 - Business risk controls and mitigation

be you. we care.

© axl & trax. all rights reserved.

© SAP AG - all rights reserved

axl & trax

8. Identity Management

- ❖ Cross-platform **access management process** automation and enforcement
- ❖ Capabilities allowing identity/role **lifecycle management**
- ❖ **Control** through standardization, policy enforcement, automation, self-service and delegation
- ❖ Moving from **technology-centric** silo's to **organization-centric** and **policy driven** provisioning
- ❖ **Workflows** and cross-platform **reporting** increase effectiveness of detective control



be you. we care.

© axl & trax. all rights reserved.

axl & trax

8i. Facing Identity Management challenges

- ❖ Prepare for “**business “readiness”**”
 - ❖ Allocated operational responsibilities
 - ❖ Redesigned processes
 - ❖ Meta-processes
 - ❖ Anticipate future change
 - ❖ Establish & agree on control requirements
- ❖ Defining **rules...prepare for exceptions**, but try to avoid them
- ❖ Audit ability and reports are capabilities/features, make sure to use them if compliance or control were **project drivers**
- ❖ Don't **control** because you can to avoid the creation of a paper tiger



be you. we care.

© axl & trax. all rights reserved.

axl & trax

9. Food for thought

- Tool ≠ compliance
- SoD rules ≠ the holy grail
- Risks are specific, solutions generic
- “A fool with a tool is a bigger fool”
- “It is cost effective to automate repetitive tasks; it is expensive and complicated to automate everything.”
- Compliance may be the result of good governance
- Security improvement is a program, not a project

CAPABILITY ≠ COMPLIANCE

be you. we care.

© axl & trax. all rights reserved.

axl & trax

Questions?



be you. we care.

© axl & trax. all rights reserved.

axl & trax

Thank you for your attention

axl & trax

be you.. we care.

wouter janssen \ director
wouter.janssen@axl-trax.com

CISA CISSP CISM CGEIT CFE
Certified SAP NetWeaver Security Consultant

geldenaaksebaan 329 \ b-3001 heverlee \ belgium
tel. +32 16 311 000 \ mobile +32 494 51 51 26
www.axl-trax.com