

axl & trax

be you. we care.

**LOSEC**  
LEADERS IN SECURITY

*Governance, Risk  
and  
Compliance*

*Willing to take a risk?*

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

*June 6<sup>th</sup>, 2011*

axl & trax



**axl & trax**  
the name...



be you. we care.  
© axl & trax. all rights reserved.

**axl & trax**

**axl & trax**  
the global reference in the SAP security market

**fact sheet:**

- ❑ formerly CSI Belgium ° 1997
- ❑ 2008 rebranded to axl & trax
- ❑ over 20 dedicated SAP security, GRC, IAM, authorization experts
- ❑ more than 200 customers served

**our partnerships:**



be you. we care.  
© axl & trax. all rights reserved.

**axl & trax**

## why are we successful?

- 14 years experience in SAP security, audit & control
- we focus 100% on internal controls
  - GRC / SAP security is our core business
- our experts are certified in the area of
  - auditing: CISA; CIA; ...
  - security: CISM; CISSP; CGEIT...
  - various SAP certifications
- we represent the bridge between business & IT
  - combine theoretical with in the field experience
  - sound knowledge of business processes and data flows
  - ability to communicate in business language
- our vision & principles
  - KISS - Keep It Stupidly Simple
  - GRC is a business issue - IT is the enabler

be you. we care. think before you act

© axl & trax. all rights reserved.

axl & trax

## Agenda

- Risk in today's reality
- Scoping GRC and its stakeholders
- GRC challenges with SAP environments
- An approach for risk management with SAP ECC
- Closing the gap of control: continuity

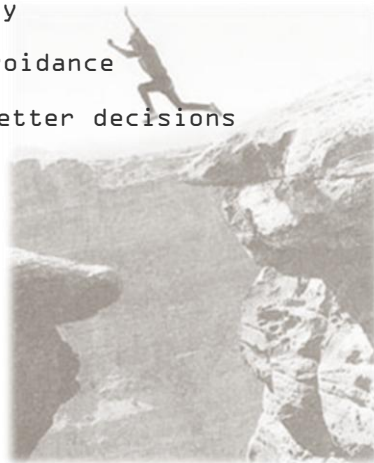
be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Willing to take a risk?

- companies face risk everyday
- risk management vs. risk avoidance
- knowledge → awareness → better decisions
- project vs. process
- solo vs. team



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Governance Risk & Compliance

- **Governance**
  - strategy execution
  - measurable performance
  - direct & stay in control
- **Risk**
  - balancing risk and opportunities
  - identifying threat, likelihood & impact
  - continuously assuring control effectiveness
- **Compliance**
  - upkeeping actual requirements
  - performance measurement
  - demonstrating compliance posture
  - managing conformance in changing times

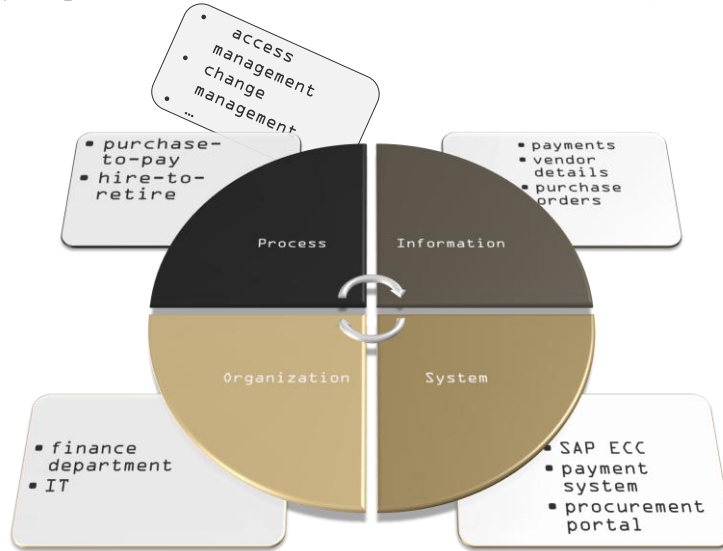


be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Scoping: where to start?

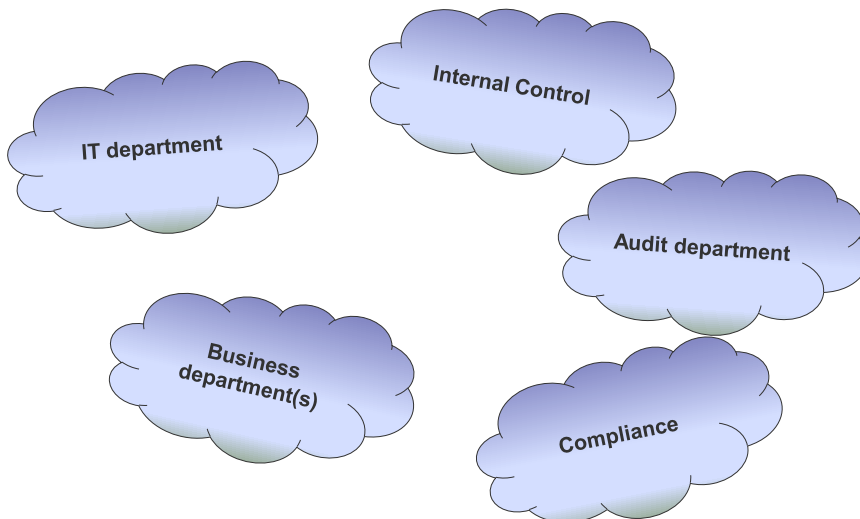


be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Scoping: Who will take the lead?



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

### Risk specificity

- how to attribute & select risk
  - process - inherent
  - industry-specific
  - company-specific
  - regulatory/legal
- ... and how to assess its criticality?
  - risk appetite
  - vulnerability (company posture?)
  - existing controls in place (relevance?)
  - competitive advantages / financial g
  - cost / inability to mitigate



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## risk vs. control measures

### how to relate risk to control measures?

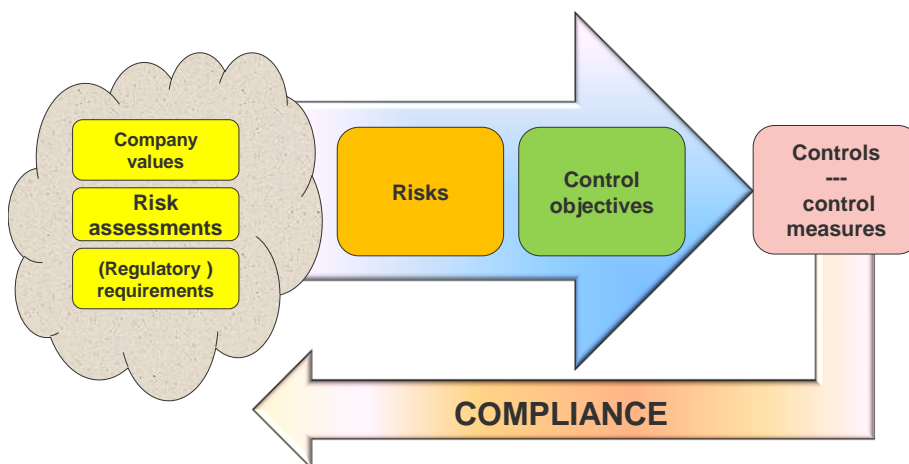
- good process design
- application (SAP) configuration
- master data management
- critical access rights
- segregation of duties
- training & clear work instructions
- reports and reporting
- workflows

be you. we care.

© axl & trax. all rights reserved.

axl & trax

## From risks to compliance



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## SAP ECC systems and GRC

### different types of controls

- **inherent controls**
- **business processes controls**
  - process design / configured controls
  - process execution → master data management
- **access controls**
  - critical access rights
  - segregation of duties
  - emergency / temporary access
- **system controls**
  - logging & trailing
  - development & customizing settings
  - ...

be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Challenges in SAP environments

- process-integration usually implies **control integration**
- **shared data** means shared stakes, risks and dependencies
- system integration requires **control harmonization**
- **system-centric** governance & control fails in heterogeneous landscapes
- the **configurability** of SAP environments requires good control over change processes and project

be you. we care.

governance  
© axl & trax. all rights reserved.

axl & trax

## segmentation of solutions

- integrated GRC (multi-governance, enterprise wide)
- domain-specific GRC
- point solutions to GRC

### *question:*

*how to ensure good governance across the enterprise, IT, processes and solutions?*



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## SAP BusinessObjects GRC suite



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## risk, control automation & risk owners

- control automation improves timeliness & reduces effort, but still requires
  - ownership
  - exception handling
  - maintenance
  - periodic review of effectiveness
- who does what in the control environment and what can be automated?
  - reporting
  - reviewing reports and/or exceptions
  - escalation
  - exception approval
  - assurance of effective process execution
  - periodic review of risk & mitigation accuracy
  - project embedding



be you. we care.

© axl & trax. all rights reserved.

axl & trax

## Governance Risk & Compliance

- GRC is an holistic **umbrella** for "G", "R" and "C"
- no generally accepted integrated approach, standards or common body exist
- vertical and horizontal standards and good practices do exist
- an **integrated approach** is key for effectiveness, buy-in and success
- automated controls require periodic **"maintenance"** → validity, effectiveness, tuning and relevance

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

**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](http://www.axl-trax.com)