ROADMAP TO SAP SECURITY

The NORM Definition whitepaper

Version 1.1 – July 2010

© 2010 axl & trax

1. Background
2. Roadmap to compliance
   2.1. risk management
   2.2. solving risks
   2.3. monitoring compliance
3. The norm definition process
   3.1. ownership
   3.2. initial analysis
   3.3. norm identification
   3.4. post-norm analysis
   3.5. monitoring
1. Background

The objective of this document is to provide guidance on the key steps leading to proper control over SAP access rights and the authorization concept.

This document describes:
- a risk approach for the SAP authorization concept
- the axl & trax roadmap to compliance in an SAP environment
- one particular roadmap step in detail: the norm definition

The axl & trax roadmap steps are explained in various white papers, each describing one of the key steps. The current white paper presents the norm method that allows companies to identify authorization access rights requirements and map them with the current state in the SAP system. This approach is to identify and remediate the existing gap between the desired state (business requirements) and the actual state (implementation). This is done to get in control over the user access rights.

2. Roadmap to compliance

Thanks to more than 14 years of experience in SAP audit, security and control and more specifically on authorizations and user access rights, axl & trax has developed an effective approach to design, implement and control user security in SAP systems. This approach is described in the axl & trax roadmap for SAP compliance outlined below.

The purpose of this roadmap is to define consecutive steps leading to an adequate level of security in SAP systems and moreover to identify risk posture and maturity of the company with the purpose to identify actions for improvement of the overall security posture.

This paragraph outlines the axl & trax roadmap to compliance. This roadmap is used to identify the company’s maturity level per item in order to define actions for improvement to achieve the desired state of control.
The roadmap can be split into 3 phases, each of which further described below:

- Risk management
- Solving risk
- Monitoring

2.1. Risk management

In the Risk management phase we identify the current state of the user access rights and compare this to good practice in order to identify weaknesses. Why compare it to best practices? Because often companies do not have clear security policy or extensive knowledge about security backdoors existing in any SAP system or a clear view of what the risk is of the currently granted access rights. So what is the existing risk exposure?

The first step is thus the identification of the as is situation. This is usually done through an audit or a conceptual review. The conceptual review (review of the authorization concept) digs into the authorization design/model to perform root cause analysis of identified problems. Understanding the root cause attributes to understanding of risk exposure.

Ownership must be defined by identifying the persons responsible to decide on:

- **Rules** – which company rules or policies must be enforced (e.g., Nobody should be able to do development in a production system)
- **Roles** – which roles and responsibilities exist today and what is the content of each as defined in the SAP system (e.g., the role “Display financial accounting” should only be given to finance staff and may not contain maintenance activity)
- **Norm** – what is the norm for the granted access rights? What are the business requirements as to which users get access to what? (e.g., employee Johan should be able to do the “payment run” but Jack should not).
2.2. solving risks

Solving issues & risks is the implementation of the defined rules. This is done through remediation activities or redesign of the authorization concept. This, depending on the identified root causes in the conceptual review.

Remediation of the existing issues can be done through changing user assignments or adjusting existing role content. Each scenario implies that the existing authorization concept is transparent and maintainable.

Remediation of risk through authorizations can also be done by implementing compensating controls. This happens usually when authorizations cannot solve the issue or when the users require the access rights despite the risk.

Remediation of the existing authorization concept is sometimes difficult due to:
- Lack of transparency – content of role is unclear
- Lack of consistency – content of role is not correct anymore
- No existing authorization concept or model

When an existing concept has proven ineffective and unmanageable, it is better to redesign the authorization concept. This new concept is then developed following a strict methodology and linked to the defined rules and business requirements.

2.3. monitoring compliance

Monitoring ensures that business/security rules are properly implemented and respected over time. It is important that the monitoring rules are aligned with the actual business requirements. If the safety net implemented is not reporting correctly the current risks exposure, it may give false confidence and increase the risk of security breaches. Enduring control must be enforced to avoid security erosion and assure that any new risk exposure is reported in time.

3. The norm definition process

Defining business requirements related to the SAP authorization process and segregation of duties is difficult. Unclear business requirements and lack of ownership can undermine the decision process and may lead to inappropriate SAP role content and user-role assignments.

This may have the following adverse effects:
- higher risk of undesired access rights or inadequate role decomposition
- increased maintenance effort for the authorization team (increasing cost)
- more frustration by the user-id community
- unavailability of the required SAP functionality
- mismatched business expectations
axl & trax uses the norm methodology to identify the business requirements, ease the decision process and reduce the effort put into adjustment of the authorization concept.

The norm methodology helps in identifying:
- which users can do specific/critical SAP functionalities or can have SoD conflicts
- which users did perform specific/critical SAP functionalities or SoD conflicts
- which users should (not) execute specific/critical SAP functionalities or SoD conflicts
- the gap between what users can do, what they should do and what they actually did

This approach allows defining appropriate remediation action while limiting the impact on the user community.

The methodology considers different types of actions (compensating controls, adapt role content, adapt user assignment or adjust business responsibilities...). It also creates a benchmark for future monitoring to ensure business requirements are enforced over time.

**Norm methodology**

The norm methodology allows measuring the actual state and comparing it to the desired one.

- trace who executed which transaction to assist the business in defining the desired state and to monitor the correctness of the desired state
- define the desired state to design first before changing or removing roles and identify remediation actions

This approach allows thinking before doing, to make business management back responsible for access rights and to identify when access rights or compensating controls are best deployed.

### 3.1. ownership

Ownership is a key element in the norm project. It is the basis for the approval flow and allows the definition of which access rights are allowed. Ownership can be defined on different levels: user, SAP roles, process, SAP functionality, segregation of duties conflicts and more.

For a norm project, ownership must be defined at least on SAP process level and on the segregation of duties matrix. Defining ownership is a business activity.

### 3.2. initial analysis

The purpose of the initial analysis is to assess and report on the granted access rights and segregation of duties conflicts. The initial report will serve as a basis to identify the norm and contains details of granted access rights per user (can), executed transaction codes per user (did) and SoD conflicts per user-Id.

A set of SoD conflicts and relevant queries (SAP critical functionalities) is selected and analyzed. The results are reviewed using CSI Authorization Auditor® and are reported in easy-to-handle Excel sheets.

### 3.3. norm identification

When defining the norm, the company defines what a user should or should not be able to do. This is the first step to define the desired state.

The report resulting from the initial analysis is discussed with the defined owners and responsible staff from business who will then verify if the granted access rights are in line with the business requirements.
The following categorization is used in this step:

- **Required (R)** – the user should have access to the functionality (daily job)
- **Allowed (A)** – the user can have access to the functionality
- **Not allowed (N)** – the user should not have access to the functionality
- **Unknown (UT)** – no decision yet taken

When the norm details are known, a new analysis can be performed. At this stage no action is taken within SAP roles because there is a risk that the decisions taken do not fully reflect the current 'life' situation.

### 3.4. post-norm analysis

A new analysis run is performed ++ three months after the initial analysis to capture further transaction code usage. This analysis provides insight into the granted and executed access rights (actual state) versus the defined norm (desired state) and is the basis for remediation.

The following combination of norm items will be found in the segregation of duties analysis.

- **required – required**: both conflicting activities are part of the user’s daily job
  - transaction code execution attest that the user is using both activities
  - the conflict can’t be resolved and compensating controls must be considered
  - transaction code execution shows that one or more activities are not used
  - check if the not executed activities are required and possibly adapt access rights

- **allowed**: user can do the activity but is not required to
  - check transaction code execution to assess if the conflict is executed and validate business need
  - remove access if not executed or monitor its use on a regular basis
  - set the norm to ‘required’ if the transaction codes were executed and required

- **Not allowed**: the user should not have access to the functionality
  - Check transaction code execution to validate ‘not allowed’ status
  - If no execution the access rights should be adapted
  - If executed, the status ‘not allowed’ should be re-validated

- **Unknown**: no decision yet taken
  - Check transaction code execution and re-validate with business to set the correct norm

The analysis steps described above correspond to paths in the remediation tree depicted below:
3.5. monitoring

The defined and documented norm can be use as a baseline for monitoring with CSI Authorization Auditor®. A regular analysis on the current state and periodic assessment of the norm allow enduring enforcement of the established business requirements and related security policies.