Access Control Applications for SAP

Ivan Spruit, Jasper Schutte and Sander van der Zon

Many organizations want to get a better grip on the management of SAP authorizations in order to get rid of their "authorization issues." This has stimulated an increased use of integrated Access Control applications over the last few years. This article elaborates upon the advantages of using integrated Access Control applications, and lists a number of factors that can improve the success in implementing these applications.

I. Spruit MSc
is manager at KPMG IT Advisory.
spruit.ivan@kpmg.nl

J.G. Schutte MSc
is consultant at KPMG IT Advisory.
schutte.jasper@kpmg.nl

A.M. van der Zon MSc
is consultant at KPMG IT Advisory.
vanderzon.sander@kpmg.nl

Introduction

In the last decade, organizations have come to pay more attention to internal control and risk management in ERP systems such as SAP. This increased attention is partly but not solely the result of stricter legislation. Actual daily practice has shown that authorization related controls – as a part of internal control – are still not functionally sound. Users have been assigned undesirable combinations of authorizations, and a relatively high number of users are authorized to access critical functional transactions or system functionality. In the past, management frequently initiated efforts to reconfigure their authorization processes and procedures. Unfortunately, it often turned out that problems with the assigned authorizations resurfaced after some years, which allows for undesirable segregation of duty conflicts to show up again, while the costs of control remain high.

Over the past few years, the market has responded to these issues, and a number of different integrated Access Control applications have been launched. These offer extensive opportunities for managing (emergency) users, authorization roles and facilitate the (automatic) assignment of authorization roles to users. In addition, all these applications provide support with controls, such as preventative and detective checks on segregation of duty conflicts. In addition, these applications make it easy to see a clearer picture of the actual access risks, by means of reports and dashboards.

This article focuses on the functionality of Access Control applications (hereafter called "AC applications") and the preconditions for a successful implementation of these applications.

Why are authorizations so important?

To describe authorization management, this article adopts the definition of Fijneman et al. ([Fijn01]), which is based on the IT management process:

"... All activities related to defining, maintaining, assigning, removing and monitoring authorizations in the system"

The authorization management process can subsequently be divided into the following sub-processes:

- *User management:* all activities, including controls, related to assigning and withdrawing authorizations, as well as the registration in the system. In a practical context, the term "provisioning" is commonly used. User registration takes place on the basis of source data: for

> *Many organizations find that managing authorizations within SAP is a major challenge*

example, as recorded in an HR system. One part of user management is issuing passwords and managing special users, such as system and emergency users.[1] Recurring assessments and checks of the assigned authorizations also form a major part of user management.

- *Role management:* all activities, including controls, required for the definition and maintenance of authorizations within the system. There is a strong relationship between the role-management process and the change-management process. Here too, recurring checks of the authorization roles are essential.

Authorizing access to a person or object in any SAP system is usually based on arrangements made beforehand: a policy is established for granting access, for example. These arrangements are made by the management, as a rule, and in virtually all cases they aim to ensure that risks or threats to an organization remain on an acceptable level.

Authorizations are an integral part of the internal control system of an organization. "Segregation of duties" is based on the principle of avoiding conflicting interests within an organization. The aim is to ensure that, within a business process, a person cannot carry out several successive (critical) tasks that may result in irregularities – accidentally or on purpose – that are not discovered in time or during the normal course of the process ([ISAC01]). It is essential to an organization to identify any issues related to segregation of duties and take appropriate action. The causes of segregation of duty conflictsare discussed in the next section.

Authorization issues

Many organizations find that managing authorizations within SAP is a major challenge, and that assigning authorization roles and preventing segregation of duty conflicts are time-consuming matters that result in high administration costs. Common problems in this context are:

- a large number of unknown and unmitigated risks related to segregation of duty violations
- authorizations that are not in line with the users' role and responsibilities in the organization (business model)
- excessive authorizations for system administrators and other "special" users.

Overall, these issues have their origins in the following causes:

- insufficient insight into SAP authorization roles, in the business as well as the IT organization
- insufficient insight into the assigned authorizations
- insufficient insight into the impact of organizational changes on existing authorizations
- lack of attention to update authorizations in times of organizational change
- insufficient insight into potential issues related to the segregation of duties
- lack of control ownership
- unclear responsibilities within the organization, so that it is not clear who is allowed to do what
- unable to resolve authorization issues due to the complexity and lack of knowledge of the SAP Authorization concept
- non-compliance with procedures;

AC applications can solve the majority of the issues that concern user and role management. In the case of role assignments, functionality exists to configure approval workflows. In addition, the workflow can include a preventative control that in case of segregation of duties violations the related risks must be approved by the financial manager beforehand. Workflows can likewise be configured for changes within authorization roles; in such cases, similar approval is required before the changes become effective. At the same time, the applications offer support when it comes to the periodic or ad-hoc checks and evaluations of the assigned authorizations in the system.

Access Control applications

In the past, AC applications were primarily used by IT auditors who developed these applications themselves. This arose from the need to carry out audits on the logical access security of SAP in a more effective and efficient manner. This functionality predominantly involved the offline identification and detection of assigned authorizations and segregation of duty conflicts. Examples of these kind of applications are the KPMG Security Explorer and the CSI Authorization Auditor, which can be used for the periodic evaluation of the assigned authorizations. However, there is an increased need of management and the

[1] System users are users that are used by (another) system to establish an interface between systems or are required for batch purposes. An emergency user is a user which is used in cases of disaster, and often has more access rights.

IT organization to manage the authorizations more efficiently. Within organizations, it has given rise to the goal of using "integrated" AC applications within the context of managing user roles. This will also enable preventative checks in an efficient manner.

There are various solutions on the market in the field of integrated AC applications for SAP. Table 1 provides a short description of three well-known AC applications.

Integrated Access Control functionality vs. controls

To stay in control over SAP authorizations, it is necessary to implement and embed certain controls in the organization and system. These controls can be identified with the help of a generally accepted information security standard. AC applications can offer support in this context by providing functionality that enable:

1. Insight in access risks related to segregation of duties violations and assignment of critical authorizations. This enables organizations to monitor and evaluate the assigned authorizations on a continuous basis.
2. Controlled assignment of authorizations to users, including the documentation of mitigating controls in case segregation of duty violations are breached.
3. Controlled authorization role changes.
4. Controlled use and review of "super users".
5. Controlled password self-service reset functionality.
6. Documentation of the risks and rules related to critical access and segregation of duties.

Process efficiency and cost reduction

Apart from more "control-related" reasons to use AC applications, organizations also apply them for reasons of cost reduction and process optimization. Organizations can, for example, automate large parts of the user management process. Workflows and mobile apps enables the business to request, approve and assign authorizations without the involvement of user administrators.

Integrated AC application also contains a password self-service functionality, which enables a staff member to restore his or her password him-/herself, without involving the helpdesk.

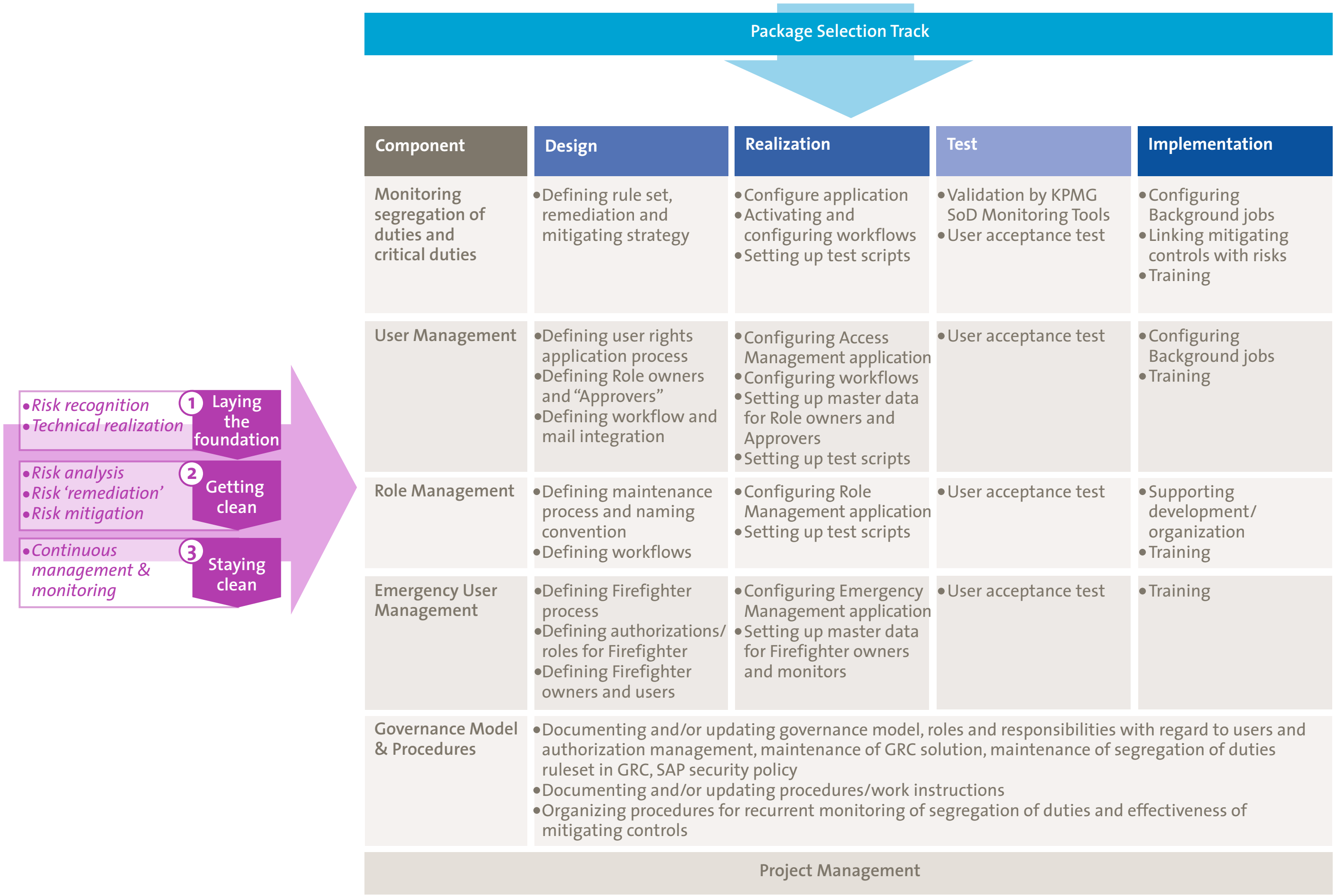
	Supplier	Product	Background
1	SAP AG	SAP Access Control SAP Identity Management	SAP Access Control is based on the former Virsa, which was taken over by SAP AG in 2006. SAP also allows integration with Identity Management solutions.
2	SymSoft	ControlPanel GRC	SymSoft is based in the USA and supplies AC applications for SAP. In addition, it provides applications for batch management ([CON01]).
3	Security Weaver	Security Weaver	Security Weaver is specifically directed toward Access Control software for SAP. It also provides products aiming to analyze transactional data

Table 1. **Examples of Access Control applications.**

Implement AC Applications

Figure 1 represents our recommended approach to implement AC applications. It is important to note in this context that an implementation is not limited to the technical implementation itself. Typically the aim of a project is to resolve issues in the existing authorization concept, as well as improving the related governance and processes. Our method is based on the following stages:

- *Laying the foundation – Risk Identification and Definition* In this stage, the desired segregation of duties and critical activities are defined, as well as the policy for dealing with a segregation of duty violations and user of emergency users.
- *Laying the foundation – Technical Realization* In this stage, the rules defined in the previous stage are translated into authorization objects and transaction codes. The AC Application is configured to monitor the segregation of duties and critical activities in the system and the "emergency user" functionality is implemented to allow quick wins in the *Get Clean* stage.
- *Getting Clean – Risk Analysis* In this stage the defined rules are used to analyze to what extend the desired segregation of duties are in place. Identified segregation of duty violations or users with access to critical activities will be reported.
- *Getting Clean – Risk Remediation* In this stage, the aim is to remove identified risks by making changes in the assigned authorizations or in the roles itself. Quick wins can be realized by using advanced data analysis techniques from the KPMG F2V methodology. These analyses extend beyond the determination of whether or not a user has executed a transaction, as they also determine whether or not an actual change or entry has been made in the system.



Component	Design	Realization	Test	Implementation
Monitoring segregation of duties and critical duties	• Defining rule set, remediation and mitigating strategy	• Configure application • Activating and configuring workflows • Setting up test scripts	• Validation by KPMG SoD Monitoring Tools • User acceptance test	• Configuring Background jobs • Linking mitigating controls with risks • Training
User Management	• Defining user rights application process • Defining Role owners and "Approvers" • Defining workflow and mail integration	• Configuring Access Management application • Configuring workflows • Setting up master data for Role owners and Approvers • Setting up test scripts	• User acceptance test	• Configuring Background jobs • Training
Role Management	• Defining maintenance process and naming convention • Defining workflows	• Configuring Role Management application • Setting up test scripts	• User acceptance test	• Supporting development/ organization • Training
Emergency User Management	• Defining Firefighter process • Defining authorizations/ roles for Firefighter • Defining Firefighter owners and users	• Configuring Emergency Management application • Setting up master data for Firefighter owners and monitors	• User acceptance test	• Training
Governance Model & Procedures	• Documenting and/or updating governance model, roles and responsibilities with regard to users and authorization management, maintenance of GRC solution, maintenance of segregation of duties ruleset in GRC, SAP security policy • Documenting and/or updating procedures/work instructions • Organizing procedures for recurrent monitoring of segregation of duties and effectiveness of mitigating controls			
Project Management				

Figure 1. **Recommended method for implementing Access Control.**

- *Getting Clean – Risk Mitigation* In this stage, the aim is to mitigate the remaining risks, by the implementation of mitigating controls in the organization and the documentation of these controls in the AC application.
- *Staying Clean – Continuous Management* The aim of this stage is to optimize user management and role management processes by utilizing the functionality of AC applications
- *Staying Clean – Continuous Monitoring* This stage involves the definition and implementation of procedures for ongoing monitoring of assigned authorizations and segregation of duty conflicts.

Workflows can likewise be configured for changes within authorization roles

Integration with other Continuous Control Monitoring applications

A number of AC applications are compatible with Continuous Control Monitoring (CCM) applications. SAP Access Control can be integrated with for example SAP Process Control which makes it possible to determine the effectiveness of the mitigating controls assigned in SAP Access Control via the "test of effectiveness" functionality of SAP Process Control. In addition, workflows from Process Control can be configured to review the logical access security, where reports from SAP Access Control are shown. Security Weaver and ControlPanelGRC also offer integration opportunities with their Process Auditor and Process Controls Suite.

Access Control and the IT auditor

Companies and organizations that implemented integrated AC applications prefer that the (external) auditor rely on the controls and reports of the AC application. Reasons are the desire to reduce the audit fee, but also using one and the same set of rules is also considered as a

Organizations also apply AC applications for reasons of cost reduction and process optimization

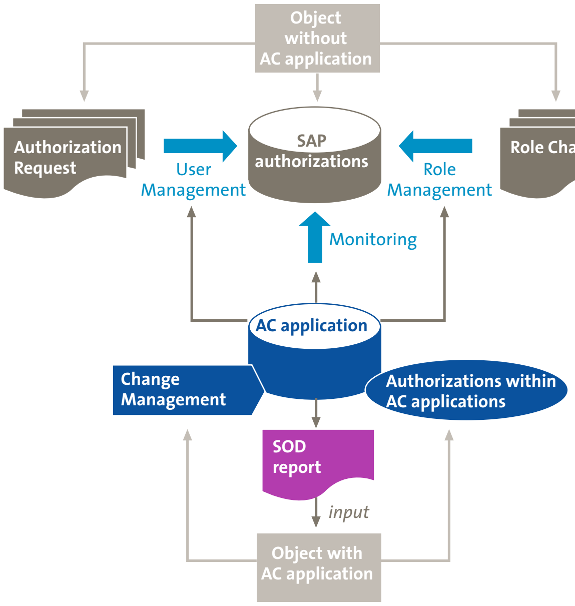


Figure 2. **Shift in the audit object.**

benefit. Auditors cannot simply depend on the functionality and reports of the AC applications, but first need to gain a certain degree of assurance with regard to the accuracy and completeness of the reports and the setup of the AC application, which slightly changes the audit object. This is represented in diagram form in Figure 2.

Conditions for relying on AC application functionality and reports

Before depending on the reports and another functionality of AC, an auditor wants the organization to meet a number of requirements:

1. Segregation of duties
- All conflicts with regard to the segregation of duties that are relevant to the auditor and accountant have been incorporated into the segregation of duty matrix used by the application.
- The defined segregation of duty conflicts need to be translated correctly and completely into transaction codes, authorization objects with fields and values, in order to prevent false negatives, as described earlier by Hallemeesch and Vreeke ([Hall02]).

2. The AC application has been configured to guarantee that:
- Approvals are provided by the right approvers (e.g. users are not able to approve requests for themselves)
- the segregation of duties check is performed on up-to-date data
- change logs are activated to enable an audit-trail.

3. Procedures
- The actual usage of super-user authorizations is reviewed
- Controls are in place to ensure that the AC application is not by-passed
- Exceptions for by-passing the AC application have been defined and documented
- Change management procedures for configuration and segregation of duty matrix changes have been defined and implemented

4. Authorizations
- Authorizations within the AC application are assigned based on the roles and responsibilities of the organization.

Control activities

If an auditor has been able to determine that his or her conditions are met, the auditor can make use of a process-driven audit approach instead of a data-driven one.

After the first review, there will typically be no need for an auditor to assess the segregation of duties matrix year after year. However, subsequent review will focus on the change-management. In such cases, the auditor should carry out the following actions:

- check the change-management process of the segregation of duties matrix
- assess the changes and "change log" of the segregation of duties matrix.

Lessons learned

In terms of functionality the integrated AC applications offer adequate controls to realize the control objectives and are therefore a good option to help achieve these objectives. At the same time, they also offer opportunities in terms of process optimization and improve efficiency.

To succeed in getting and staying in control over SAP Authorizations with the support of an AC organization the organization would do well to:

- set clear objectives. The potential implications of an Access Control implementation are often far-reaching. It is important, therefore, that clear goals are set at the start of the project and that, on the basis of these objectives, a decision is taken to determine which components of the AC application are within the project's scope. Realizing the project should be supported by a step-by-step approach.
- clean the authorizations beforehand, where possible, by implementing quick wins. With the help of "SAP statistics" and data analysis, unused authorizations can be deleted beforehand, and super-user functionality can be replaced by an "emergency" account. This will greatly reduce the amount of work during the Access Control project.
- pay ongoing attention to the "human factor" whenever the AC application is being used – even though the applications contain controls to reduce the number of "errors" due to known risks or user mistakes in the field of authorizations. Devoting attention to this "human factor" will guarantee the acceptance and correct use of the application, even after project completion.
- carefully define the "golden rules" that are aligned with the business processes and the setup of the SAP system. The rules that define the desired segregation of duties and critical authorizations are crucial to a successful implementation.
- remain vigilant with respect to breaches on segregation of duties and the use of "super-user" functionality. Execute periodic evaluations to avoid a false sense of being in control. Also establish processes that validate the effectiveness of mitigating controls.

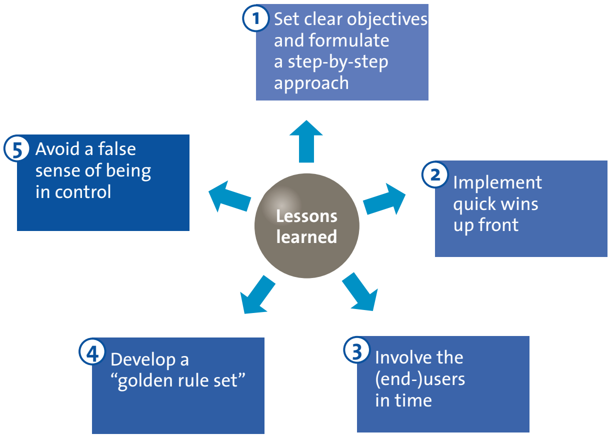

1 Set clear objectives and formulate a step-by-step approach
2 Implement quick wins up front
3 Involve the (end-)users in time
4 Develop a "golden rule set"
5 Avoid a false sense of being in control
Lessons learned

Figure 3. **lessons learned in using AC applications.**

To avoid surprises at the end of an Access Control implementation project, an organization would do well to enable a role for the auditor during the project, so that it is possible to capitalize on the auditor's findings during the implementation.

Next steps

The current AC applications offer no solutions for advanced data analyses of actual usage by users. There is limited functionality that shows whether a user has executed an activity, but there is no functionality that actually analyze whether a user entered or changed certain transaction or master records. It is therefore impossible, for example, to determine whether users have processed invoices for orders they have placed. For this type of analysis, one still has to depend on transaction monitoring applications, as used in audits or with relative new solutions like SAP Fraud Management.

References

[ALE01] http://www.alertenterprise.com; 2010.

[Bien01] Bienen, Noordenbos and Van der Pijl, *IT-auditing Aangeduid (IT Auditing Defined): NOREA Geschrift nr. 1 (NOREA Document no 1)*, NOREA 1998.

[CON01] http://www.controlpanelgrc.com/; 2010.

[Fijn01] Fijneman, Roos Lindgreen and Veltman, *Grondslagen IT Auditing (Foundations of IT Auditing)*, p. 66ff, 2005.

[Hall02] Hallemeesch, Vreeke, *De schijnzekerheid van SAP Authorizationtools (The False Security of Authorization Tools)*, 2008.

[ISAC01] ISACA, *CISA Review Manual 2008*, 2008.

[SAP01] http://www.sap.com/solutions/sapbusinessobjects/governance-risk-compliance/accessandauthorization/index.epx; 2010.

[SCW01] http://www.securityweaver.com; 2010.

About the authors

I. Spruit MSc is manager at KPMG IT Advisory. He has acquired extensive experience with the SAP authorization concept and its design. He has been involved in eight different Access Control implementations. He is also engaged in the implementation of CCM applications such as SAP Process Control.

J.G. Schutte MSc is consultant at KPMG IT Advisory. In the past few years he has been involved in a variety of SAP authorization implementation projects, as well as two Access Control implementations.

A.M. van der ZonMSc is consultant at KPMG IT Advisory. His daily work activities are devoted to assessing the assigned authorization roles and the execution of segregation of duty analysis within SAP.