5 GOLDEN RULES FOR SECURE USER MANAGEMENT

Use these tricks and get back control over your SAP authorizations

WHITE PAPER

VOQUZ
IT SOLUTIONS

5 GOLDEN RULES FOR SECURE USER MANAGEMENT

Use these tricks and get back control over your SAP authorizations

Summary

Does the following sound familiar? Historic growth of an organization's SAP user roles creates risk and management challenges that are rarely remediated without large-scale efforts or negative impacts on day-to-day operations. A clear picture about who currently has (and should have) which authorizations tends to become fuzzier with every passing year of SAP usage. One contributor to this challenge is a common workaround: employees and developers request and are provided more access than they require to perform job duties.

A particular danger with SAP authorization management is that unauthorized access to sensitive data in the SAP system can occur. However, certified security standards require a restrictive allocation of critical authorizations and a regular review of the existing role and authorization concept. Especially in terms of security and GDPR you have to be cautious!

This white paper shows you how to manage your SAP authorizations in a secure and compliant way. With our five rules for secure user management, you are protected against all dangers!

VOQUZ
IT SOLUTIONS

5 GOLDEN RULES FOR SECURE USER MANAGEMENT

Use these tricks and get back control over your SAP authorizations

Content

1. Everyone only gets the permissions that he really needs 4
1.1 Avoid power users! 4
1.2 Check your authorizations regularly. 4
2. Define critical activities and ensure an adequate monitoring 5
2.1 Monitor developers and development processes. 5
2.2 Avoid inactive accounts 5
3. Avoid mistakes – Automate the process of creating and deleting users 5
4. Document each decision 6
5. Action instead of reaction 6
6. SAP Authorization Management – Easy as 1-2-3 7
7. About VOQUZ 9
8. Contact 9

VOQUZ
IT SOLUTIONS

5 GOLDEN RULES FOR SECURE USER MANAGEMENT

1. Everyone only gets the permissions that he really needs

When assigning rights, you should always pay attention to whether the rights are really necessary at the relevant workplace. Otherwise, a large number of different authorizations or roles will inevitably result. It is then the task of the SAP Basis to manage these roles reliably and efficiently. The use of technical aids such as setQ is strongly recommended for this.

The responsibility for assigning rights lies with the respective departments. Only the responsible department can assess the necessity for the rights applied for. It should be noted, however, that specialist departments are generally not SAP specialists. They therefore need an easy-to-use user interface and help or advice on what individual authorizations or roles mean.

1.1 Avoid power users!

Power users have enormous permissions in your system - thus they represent a great risk for your security and compliance.

We therefore recommend the use of “Fire Fighters”. These are users who only have special permissions in an emergency for a certain period of time. These permissions are fully documented during use. You define these authorizations in advance so that they can be quickly implemented in an emergency.

With setQ this process is completely automated.

1.2 Check your authorizations regularly

Rights granted in the past should be questioned periodically. Such re-certifications help to avoid conflicts, for example when employees change departments.

The check should be carried out workflow-supported by the respective responsible departments. This process must be fully documented, as auditors, or in some industries also regulatory authorities, check this documentation.

However, the control of the authorizations can hardly be mastered manually. In addition, it is extremely expensive. The right tool does the work for you and controls the authorizations fully automatically and in compliance.

The corresponding setQ modules will help you:

Reduction Manager
Filters and revises existing SAP authorizations automatically. A cockpit shows up optimizing suggestions.

Recertification Manager
Recurring decisions get monitored and analyzed in a system overlapping cockpit.

VOQUZ
IT SOLUTIONS

2. Define critical activities and ensure an adequate monitoring

A well thought-out authorization concept is the be-all and end-all. Right from the start, you should take care to ensure that the combination of authorizations does not create any risks for the company. Critical authorizations should therefore only be assigned if absolutely necessary. An internal control system is also advantageous.

You should keep an eye on particularly critical processes, even if they are running under correct approvals. With the Alert Manager, you determine the focus of these checks and define a set of rules for reporting and alerting. You should focus on the essential processes and rules, so they don't get lost in a flood of unimportant messages.

2.1 Monitor developers and development processes

During the go-live phase, developers often have extreme privileges even in production systems. With a good development and test concept, you can avoid them as far as possible, but possibly not completely. Make sure that these authorizations are revoked as quickly as possible and that the activities in productive systems are closely monitored.

2.2 Avoid inactive accounts

Inactive accounts are an easy target for hackers and therefore pose a high risk. Be careful to close inactive accounts and only reopen them when needed.

3. Avoid mistakes – Automate the process of creating and deleting users

The SAP authorization assignment can hardly be handled manually. If you take the "need-to-know" principle seriously, the complexity of your authorization concept increases. This makes it much easier for errors to occur in manual processes, which in turn can become a security risk.

The setQ **Role Manager** follows a matrix concept for the administration of roles. Roles are divided into functions (What?) and packages (Where?). This enables efficient management of a large number of detailed roles.

With the setQ Authorization Manager for SAP Software, the approval process for granting SAP authorizations is automated and implemented as a transparent process. The allocation takes place from a central point - so you always have an overview of your SAP authorizations. Operation is also simplified: Administrators use the familiar SAP user interface, while business managers benefit from an easy-to-use Web interface that warns them in real time of unintentional SOD conflicts.

With the **Compliance Manager**, the assignment of new authorizations and their effects can be simulated in advance of going live. This software solution can also be used to define different approval procedures for conflicts. This also takes into account the four- or six-eyes principle. The **Compliance Reference Manager** has over 500 automated test queries that can be individually extended. This enables you to automatically find typical conflicts and resolve them quickly.
A manually systematic control of the authorization system can only be realized with a great deal of effort.

The corresponding modules in setQ:

Role Manager
Create new authorizations easily and implement them simultaneously in all systems.

Compliance Manager
Analysis of weaknesses, risks and law violations, and permanent display offline or in the running system.

Compliance Reference Manager
More than 500 prefabricated audit queries that are customizable to fit your requirements.

4. Document each decision

When the accountant examines your SAP system and your authorization concept, it is important that the changes are documented and, of course, correspond to the changes in the system.

There you can often find the problem: Various evaluations within SAP, e-mails, handmade notes in folders and similar more, must then be searched with an enormous amount of labor and time. This not only costs time, but also money.

But there's an easier way! You can automatically document changes – completely and comprehensibly. You just have to complete your SAP authorization management with functions such as those we offer with setQ.

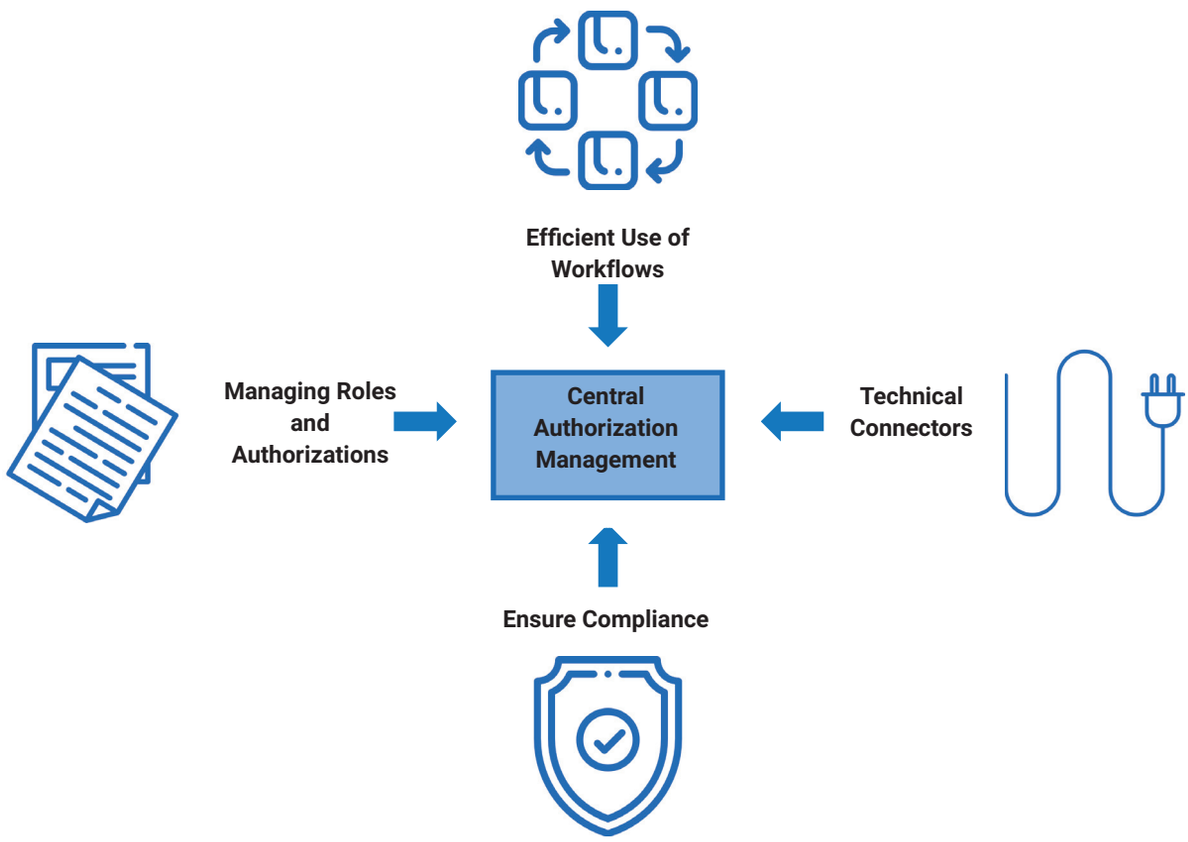
5. Action instead of reaction

There's the same rule for SAP authorization management as for SAP license optimization: Action instead of reaction! Don't wait until the account is standing on your doorstep! Ensure central SAP authorization management at an early stage and thus maximize your data protection and audit security.

VOQUZ
IT SOLUTIONS

5 GOLDEN RULES FOR SECURE USER MANAGEMENT

Lowering Cost by Knowing the Right Combination:



6. SAP Authorization Management – Easy as 1-2-3

With the help of the setQ Authorization Manager for SAP Software role approval and assignment processes are automated while making all related processes fully transparent for the business. Assignments are managed from a central dashboard – ensuring you have complete control over all connected systems. Operation is also simplified: Administrators use the familiar SAP user interface, while business managers benefit from an easy-to-use Web interface that warns them in real time of unintentional SOD conflicts.

Compliance and Security – setQ keeps you save on many levels

Especially when it comes to Security and GDPR, authorization management requires a tool you can rely on. setQ ensures that access to SAP is assigned reliably and securely. The contents of org-wide authorizations objects and roles are made transparent and traceable, allowing you to build a compliant end-to-end process for the SAP landscape at large.

5 GOLDEN RULES FOR SECURE USER MANAGEMENT

Lose your fear of threatening audits!

Design and migrate to a new role concept on the fly

setQ employs a reference model that drastically accelerates initial Role-Design and Re-Design using a modular architecture. Hundreds of templates simplify the functional aspects of designing, maintaining and reducing access of a best-practice authorization concept, without requiring large-scale efforts or the help of external consultants.

Even during the plug-and-play creation of new roles and concepts, setQ runs real-time checks for critical SOD conflicts in the background and can prevent them from being pushed to production automatically.

The deployment of your new roles follows a transparent ruleset and does not require complicated tinkering to get started. While legacy Identity Management for SAP requires complex knowledge and months of setup and refinement, a setQ install is fast and simple.

Reduce costs and simplify your SAP

It is difficult to maintain an overview within your SAP systems. In addition, there are regular changes that further complicate licensing and authorization assignment and raise up prices.

Benefit from a perfectly combined Identity Management in SAP. Results from our SAP license management tool samQ, e.g. unused transactions in roles, can be processed automatically.

Historically, SAP's contractual user definitions were written to be assigned based on **performed activities** (executed functions and transactions codes)

⟶ **i.e. low-cost license for low SAP usage**

SAP's new approach: Current and future contracts are reworded to force license assignments based on the potential access a user has (regardless of whether it's used or not)

⟶ **risk of unexpected ballooning costs following an SAP audit + an opportunity to clean up your role concept in anticipation of SAP's upcoming changes.**

Advantages at-a-glance

- Quick installation and unparalleled usability
- Reduction of costs and management efforts through automation
- Compliance & Security assurance
- GDPR-compliant authorization management
- Centralized and simple control mechanisms for roles and authorizations
- SOX -Compliant Authorization Management
- Automatic prevention of critical combinations and SOD conflicts
- Dramatic workload reduction for Basis and Security Teams
- Request, approval and assignment processes for authorizations are accelerated significantly for new and existing SAP users

VOQUZ
IT SOLUTIONS

About VOQUZ

The VOQUZ Group is a solution provider and systems integrator in the field of information technology. VOQUZ is a one-stop shop for the implementation of complex IT projects and provides customers with intelligent solutions in the areas of compliance and IT security.

The company's flagship compliance product is the samQ software solution, which it developed in-house. The solution delivers continual, automatic optimization of SAP licenses on the basis of actual use in order to minimize the number of unused licenses. In addition, engine use is calculated and 'indirect access' to SAP data is identified.

Contact

VOQUZ Labs GmbH
Kurfuerstendamm 11
10719 Berlin

Phone: +49 30 364188 - 31
Fax: +49 30 364188 - 32
E-Mail: labs@voquz.com

http://www.voquz.com

Download of the white paper:
https://www.voquz.com/news/downloads/

VOQUZ
IT SOLUTIONS

Germany
P +49 89 925191-0

Austria
P +43 1 5222015 -10

Romania
P +40 264704320

USA
P +1 917 818-2932

contact@voquz.com
www.voquz.com

VOQUZ

IT SOLUTIONS