SAP Access & Authorizations

How to manage your SAP
GRC Authorizations

VOQUZ
Labs

SAP Access & Authorizations
How to manage your SAP GRC Authorizations

S U M M A R Y

You might know this scenario - the number of real and perceived IT threats is growing rapidly in companies. This danger also affects Access & Authorizations in SAP GRC. These risks are not only caused by people acting not compliantly, but often caused by negligence or the wrong behavior of your own employees. Both are usually based on authorizations that are too far-reaching – which is not surprising with approximately 150,000 SAP transaction codes.

The abundance of transaction codes gives rise to uncertainties, which in the past were optimally compensated by manual work in the area of SAP GRC authorizations. Although manual handling of requirements with SAP on-board resources is possible in principle, massive human resources are required for this. This inevitably leads to an increase in effort and process costs, as well as the risks associated with inadequate authorization assignment.

In this white paper we have compiled the most important aspects of SAP GRC authorization management for you, so you don't fall into the 'authorization trap'.

SAP Access & Authorizations
How to manage your SAP GRC Authorizations

CONTENT

SAP Access & Authorizations
How to manage your SAP GRC Authorizations

Why manual solutions won't help you

The sheer number of approx. 150,000 transaction codes alone is enough to scare some people away. Where SAP GRC authorization management used to be achieved by manual work in former times, the whole thing is now more complex. Manual processing requires a large number of employees, which results in high costs and increases the risk of insufficient authorization assignment due to errors.

In order to manage authorizations properly, auditors must examine the SAP systems more and more extensively. Sooner or later, IT will have to hand over responsibilities to the business departments in order to share workflows and decisions about authorizations and risks. This becomes necessary when the classic approach no longer meets current requirements. This is where the sensible use of SAP on-board resources ends.

In the past, only so-called "historically grown monster roles" with innumerable T codes were criticized by the auditors, which were also constantly extended by the IT support. Today, much more attention should be paid to the topic as a whole.

For example, not only must the roles be "lean" - i.e. as few rights as possible, only that which is necessary - but also the corresponding workflow and the changes must be saved via versioning for the revision.

Segregation of Duty

The topic of so-called SOD (Segregation of Duty), paralyzes many companies in manual processes. Despite the effort involved, the view is always backward facing, i.e. the manual

VOQUZ Labs

process have to be run through again and again in order not to fall back directly on outdated information. With setQ users have the possibility to automate the requirements and manage them from a central location. Thus, the desired security for the company is easily established and errors in day-to-day business are avoided.

The handling of SOD can also be automated. In order to save process costs, possible SOD can be simulated at runtime during role construction or allocation, without colleagues in the workflow having to process or reject them. This means that, for example, it can be determined before a user applies for a role whether SODs could occur or whether the change to a role would create SODs. By workflow supported application and approval processes the corresponding Compliance is guaranteed at the same time. This is an On-Line Audit.

The revision of the role concept can create a large unexpected cost in any organization . Not only the construction of the roles or the workplace is extremely time consuming, but also the department interviews. In many Implementation Projects the aim is to contain all requests as far as possible without having to shut down the IT support hotline the day after the Go Live due to overload. This is a common occurrence and is "death by a thousand cuts" for any new SAP Implementation, as the business cannot operate with multiple authorization failures across many departments and not enough IT staff to resolve all the authorization issues.

The setQ reference models for roles and SOD support the revision of roles with countless templates and offer SOD freedom from the outset. With over 20 years of know-how of the well-known company codes, organizational units, etc., we can almost ensure that every user gets the right role and the support and

therefore the project go live is smooth and uneventful.

Special Cases and z-Transactions

What if special cases or z-transactions are involved? In this case setQ offers the possibility to work with the so-called SAP Reference User. Put simply: You set up the new roles, but have the old roles in parallel operation for a certain time period. The setQ Extension Manager recognizes the best roles to be added via the delta from old to new and suggests them. If there is no delta anymore, the old roles are switched off and nobody notices that the roles were ever revised. The classic alternative would be complex, permanent iterations until the concept finally fits - and that requires a significant amount of IT support.

During daily operation, the roles are repeatedly subject to mass changes across the various target systems. With the SAP on-board resources, the manual effort is also very high leading to errors. With setQ, every mass change can be executed from a central location, with workflow-support at the push of a button.

Substitute Cases / Fire Fighter roles

The topic Compliance also contains issues as the monitoring of users with temporarily extended authorizations. These are so-called emergency or special users. If, for example, a colleague goes on vacation or parental leave, it must be possible to continue working without interruption for the duration of the substitution. In the past, many screenshots could be found in folders that logged the assignments. The SAP_ALL was taken out of the safe.

VOQUZ
Labs

Today solutions like setQ Emergency Manager facilitate this task and assign specific authorizations on a visa or ticket basis. Subsequently, the deployment can be checked and confirmed according to the four-eyes principle. Simple solutions make it possible to record activities, but only provide a retrospective view of past activities. The setQ Emergency Manager offers the possibility to recognize and prevent critical activities at runtime. A new access has to be requested via workflow.

Workflows

Precise workflows should be part of any SAP GRC Authorizations solution. Almost all setQ Managers support the daily business with targeted e-mail requests and also remind of open workflow steps. On the other hand, unnecessary workflows can be avoided. With setQ, for example, a user created in HR Org. Management can automatically receive his roles in SAP via the position.

SAP GRC Authorization Management with setQ 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 solution 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. Reduce the ongoing escalating costs of your yearly audits, auditors now need less time than before.

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.

Depending on the requirements of the company, it can be decided which setQ Manager should be used. The range of A&A modules includes:

- **Role construction in interaction with approx. 1000 role templates**
- **User administration**
- **SOD and Compliance with over 500 SOD templates**
- **Monitoring tools**
- **Additional tools such as Password Reset or GDPR Reports etc.**

Various connectors e.g. to AD, BI, HR etc. optimally connect the existing systems.

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
Labs

About VOQUZ

VOQUZ Labs is a sub-division of the larger VOQUZ Group and the leading provider of Software Asset Management (SAM) and Authorization Management (GRC) add-ons for SAP, with bases in Berlin, Amsterdam, Cluj-Napoca, Cape Town, London, Mexico City and New York. VOQUZ Labs combine best-in-class SAP User Management solutions and a strong Consulting Expertise in License Advisory, Compliance, Security, Access Control and Efficient User Management.

About our SAP Solutions

With its software products samQ and setQ, VOQUZ Labs has specialized in the optimization of license costs and authorization concepts for SAP applications. These self-developed SAP solutions reduce the manual administration effort and cut costs by optimizing usage of the existing software inventory. In addition to the SAP license management tool samQ, setQ enables the automation of SAP authorization assignment. This way, authorization processes become revision-safe and compliant.

VOQUZ Labs

HEADQUARTER CONTACT

VOQUZ Labs AG
Kurfuerstendamm 11, 10719 Berlin , Germany
Phone: +49 30 36418- 833
Email: labs@voquzlabs.com
www.voquzlabs.com