

White Paper

daccord - Focused software to control and monitor access rights

100% IT compliance through practical access governance

Corporate data is a sensitive commodity. Regardless of the size of the company. No ifs, ands or buts. With progressive digitalization, protecting this commodity against data espionage from the outside is surely important, however, it is only one part of the solution. **Monitoring and documentation** of the access rights on the inside of the company are essential.

And who wants utter chaos when it comes to access rights, cumbersome or time-consuming analyses and cleanup processes or even unnecessary costs caused by excessive license fees? In addition, it is last but not least crucial to prevent IT security issues. Because in the end, this is very painful, but can be avoided with the right approach.

If the actual situation is analyzed without reservations, it quickly becomes evident that organizational changes in day-to-day business happen in an undetected or unnoticed manner. Often, it simply also takes too long to implement the resulting access rights changes.

We could give you numerous examples. An employee is transferred to a different department, another leaves the company, a colleague goes on maternity leave. An external employee becomes an internal one. Often, the IT department is the last link in the chain to know about these changes.

What remains are the access rights and permissions. The former external colleague continues to be able to frequently access internal data even after completion of a project. In the worst case, a serious security risk grows out of this lax approach.

The situation, generally mocked and poked fun at, of the intern having by far the most access rights within the company at the end of training is no coincidence.

So if deficits and a bad initial situation are assumed - which way is then the path to success? Who will handle finding the excess access rights or forgotten permissions, the cleanup and the withdrawal of said rights and permissions? Our software daccord will guarantee this. In a quick and continuous fashion and in the long run. And the result: accurate permissions - every time! In the end, you will gain time to do a comprehensive and diligent analysis and will prevent the causes for the dilemma.

This is the goal we pursue with our software **daccord**. We want to achieve **sustainable success** when it comes to **control, monitoring and cleanup of access rights** and convince with clearly defined principles independent of individual functionalities.

Our promise to you:

- ✓ Quick and easy implementation
- ✓ Direct results without lengthy preparatory work
- ✓ Applicable independent of manufacturer
- ✓ Optimized and complementary to the existing environments
- ✓ Tried-and-tested functionalities
- ✓ Resource-efficient and fully scalable
- ✓ Highest degree of flexibility thanks to a modular architecture
- ✓ Industry-independent use

The software daccord supports you in an accurate fashion with a multitude of functionalities in four typical challenges, confirmed to us in numerous customer projects:

1. Different systems and data
2. Data structure
3. Responsibilities
4. Sustainable control

“For us, daccord is a strategic application to which all systems are connected in order to achieve continuous control of all granted access rights and permissions.”

Patrick Baumann, IT application manager and project lead,
Reisebank AG

The daccord 4-phase model is the sustainable path to success.

The daccord 4-phase model:

First phase: Collect and aggregate	-> comprehensive data collection, permanent
Second phase: Prepare and structure	-> structured data, twice as valuable
Third phase: Assign and present	-> the right data for the right persons
Fourth phase: Review, inform and enforce	-> guaranteed control and verified results

Challenge no. 1 - Different systems and data

daccord collects, aggregates and delivers everything at a glance.

Who wouldn't want that? A **continuous analysis of all assigned rights and permissions** within the IT systems. Company-wide. Independent of the manufacturer. Without a software such as daccord, IT departments are forced to read out current access rights in a cumbersome and time-consuming fashion, and to analyze, reconcile and update such rights. All that in addition to the normal daily business activities.

To make matters worse, the granting of access rights is an ever-changing structure. Because there is constant change in companies. Such changes - barely recorded and updated by the IT department - are already obsolete again. And in companies with decentralized structures, different locations and IT systems, uniform and current reporting cannot be mastered without an adequate software solution in all reality. The software daccord is made for this.

daccord collects, aggregates and:

- delivers a current data set on a continuous basis
- consistently documents the current status of access permissions
- collects data of different IT systems in a uniform, analyzable format
- allows the simple and comprehensive review of all user and access data

Your concrete benefits:

- ✓ Access to the most current rights and permissions status of all systems at any time
- ✓ significant cost and time savings
- ✓ independent of the manufacturer
- ✓ uniform, comprehensible reports

Challenge no. 2 - Data structure

daccord prepares and structures data.

What good is data if it cannot be analyzed easily or only with extreme difficulties? **Structuring makes for the added value.** But is it really that hard? Persons work for companies. Persons have user accounts. User accounts have access rights and permissions. daccord will give you this structure and also quick, comprehensive insight for critical questions. Which user accounts and access rights does an employee in my complete IT landscape have? Which persons currently have a specific access right?

When it comes to software, not only the technical potential in the backend is important but also its user-friendly frontend. daccord is easy to use and delivers all relevant information in a personalized and comprehensible manner. No IT gibberish, no confusing analyses, but clear reports. This way, daccord users can see at a glance which accounts are not used or which accounts are orphaned, because for example a colleague has recently (or not so recently) retired. With daccord, an orphaned account is impossible. Especially those orphaned accounts cause unnecessary **financial burden**. Because usually, license fees have to be paid for those. There is an enormous potential for savings. daccord allows for system-wide and clearly structured analyses.

In addition, daccord offers the option of identifying an individual parameter - a target access rights model - and thus enables the analysis of deviations from the desired and agreed upon access rights and permissions.

“daccord is very flexible and adaptable to existing IT landscapes. Open interfaces can be requested and developed for all systems.”

Arnim Schmid, Head of IT-Department Network and Services

This is a tremendously valuable way to evaluate the rights and permissions granted to one person, for example in view of the job description or even in comparison to the colleague who should in reality have the same rights and permissions.

daccord prepares, structures and:

- makes access rights analyzable across the entire IT landscape
- allows the analysis of unwanted access rights constellations
- identifies orphaned user accounts or unused permissions
- compares granted permissions with the assigned target model

Your concrete benefits:

- ✓ A simple, structured view of all access rights and permissions
- ✓ Reduction of costs via deletion of orphaned accounts
- ✓ Identification and cleanup of unauthorized access rights and permissions

Challenge no. 3 - Responsibilities

daccord assigns and presents.

The larger the company, the less likely it is that the colleagues in the IT department know in detail the access profiles of the individual employees. During day-to-day business, the IT department merely implements requirements, does not know the circumstances and is only informed about changes after the fact. Now what? The responsible department should be in the spotlight.

Because it is only there that the current requirement profile of IT rights and permissions is known to the full extent. Today, this is done, but in a cumbersome way, manually and surely not consistently.

Implementing daccord does not only enormously reduce the work load of the colleagues in the IT department; in addition, the professional

assessment of access rights and permissions is in the right hands for the first time - it is now where it should be: with the responsible department.

Responsibility can be set up for other persons in the company or for certain, crucial access rights and permissions. But also responsibility for complete systems with all user accounts and permissions can be individually assigned to certain persons.

Because each and every responsible person knows best who should and should not have what types of access rights. True control, substantiated by professional experience, can only be effected from within the respective department. And such a department has to have the possibility to easily communicate results. daccord paves the way!

daccord assigns, presents and:

- delegates the control away from the IT department and to the specialized department
- enables the professional review of all access rights and permissions
- covers a multitude of types of responsibilities
- allows the import of allocations from

Your concrete benefits:

- ✓ Transfer of responsibility to the right position
- ✓ Sound control and cleanup
- ✓ Regulatory compliance

Challenge no. 4 - Sustainable control

daccord reviews, informs and enforces.

Why react only in hindsight? Compliance of access rights concepts can be reviewed. On a continuous basis and not just selectively. Control without suspicion. Because daccord will sound the alarm if a predetermined rule is violated, an access profile of a person/role does not correspond to the defined rights or if there are permissions in areas that are clearly not authorized. That is when our software will warn the responsible person - and only then.

To the regret of those involved, albeit legally prescribed, the periodic professional review - the so-called **recertification** - has been mandatory for some time now in sensitive sectors such as the financial or pharmaceutical industry. In theory, this method leads to the potential enhancement of the situation on the one hand, but the result in reality is debatable. After all, who maintains diligence if complicated lists of user accounts and access rights have to be signed every six months? Usually under pressure and without a clear understanding for what is going on in the

background. Then it seems obvious to just confirm the granted access rights and permissions. Done! In the hopes that later on everything will still function. Should a cleanup nevertheless be necessary, the IT department has to deal with it again, on short notice and with a significantly increased work load.

The law is the law and inevitable. That's why daccord offers all this and much more. Besides initiating periodic recertification processes for the respective responsible persons, daccord provides continuous review and monitoring of access rights and permissions - so-called **continuous auditing**. At any time, responsible persons can confirm access rights and permissions for a freely selectable or predetermined period of time and initiate a multitude of activities if required.

During this process, merely the changes have to be confirmed. This also works in the day-to-day business. For the responsible person as well as for the IT department.

daccord reviews, enforces and:

- actively warns in case of unauthorized access rights constellations
- initiates periodic recertification and control processes
- allows the continuous review and certification - continuous auditing
- reconciles predetermined rules
- informs via automated reports
- actively informs in regard to changes to access rights and prevents violations of rules

Your concrete benefits:

- ✓ Active control of the environment
- ✓ Guaranteed cleanup
- ✓ Equalization of the labor-intense recertification processes
- ✓ Regulatory compliance

daccord convinces.

Numerous customers confirm this.

Independent of the IT landscape and organizational framework conditions, daccord offers a comprehensive solution for the **sustainable control, monitoring and cleanup of access rights and permissions of your entire environment.**

Many of our customers are already using daccord successfully. Select references confirm the efficiencies reached in such a way in day-to-day business activities.



More about  daccord

www.daccord.de



info@daccord.de