CARO-Suite Best Practices

For effective cleansing of your access rights

With the CARO-Suite, you can analyse and automatically correct authorisation errors and access rights risks. Save time and money with clean authorisation structures with risk assessment by the CARO expert system for your IT security.

Best Practices

CARO-Suite - Access rights securely under control!

Historically grown access rights structures are a thing of the past with CARO. Security gaps are eliminated and automatically reduced. CARO brings order to your IT structures!

CARO-Risk Assess© - *For a clear overview*

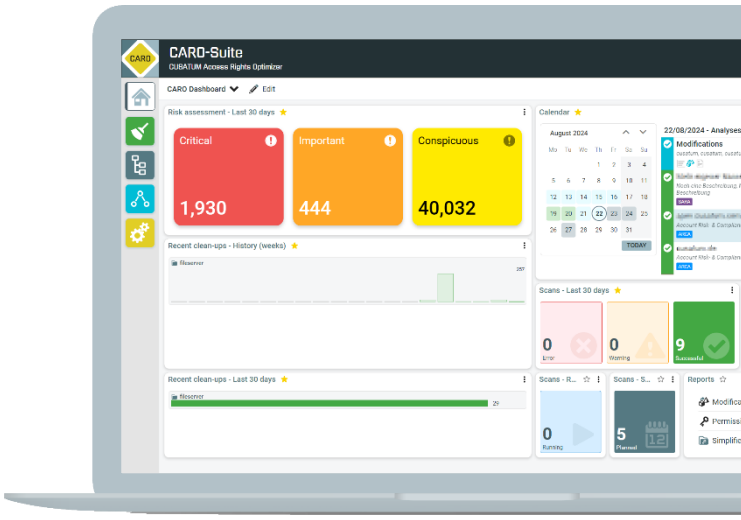
Overview through expert risk assessment and comprehensive permission analyses.

CARO-Automate© - *For your relief*

Efficiency through detailed recommendations for action and automated cleaning.

CARO-Secure© - *For your control*

You have your permissions under control; With compliance-conform reports and audit-proof logging.



CARO-SUITE IN DETAIL

- Risk assessment with expert knowledge
- Detailed analyses for permission errors
- Detailed recommendations for remediation
- For file system, Active Directory and Entra ID
- High-performance scans and in-depth analyses for changing your problematic access rights
- Scans and changes can be scheduled for any point in time
- Global resource view of access rights with group memberships
- Integration into other systems via Rest API
- Automation of employee workflow processes with the C-MAN add-on module
- Reports in PDF format, easily customizable to your own corporate identity using Word Office report templates
- Audit-proof logging of all changes made
- Multilingual web client with multiuser support
- Data storage in MS SQL database
- Simple license model

Best Practices

It makes sense to start certain analyses one after the other when cleaning up. The following overview shows a recommended **order** of CARO analyses for efficient clean-up.

Clean-up steps

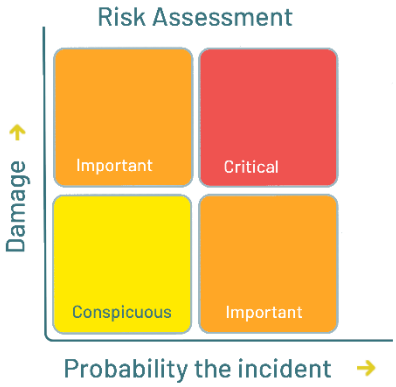
Order	Analysis modules	Technology	Useful settings in the CARO-Suite
1 Domain scan as a basic requirement	ARCA	AD, Entra ID	Scan daily, Search for at least inactive users
2 Check share permissions	SARA	FS	At least once a week
3 Find and remove dead SIDs	TEUS	FS, AD	At least once a week
4 Correct owner	BAKS	AD, FS	*So that the direct permissions created by CREATOR_ONWER are retained by subsequent ERBE clean-ups.
5 Create order for direct permissions	DARS	FS	
6 Correct problematic creator owners	BAKS DARS ERBE	FS	*May run if has been run BAKS **OR** a group concept is used on the system **AND** DARS does not provide any information, i.e. no permission groups are missing.
7 Remove direct unwanted permissions	DUKE	FS, AD	
8 Eliminate redundant permissions	RAPA	FS	

Best Practices

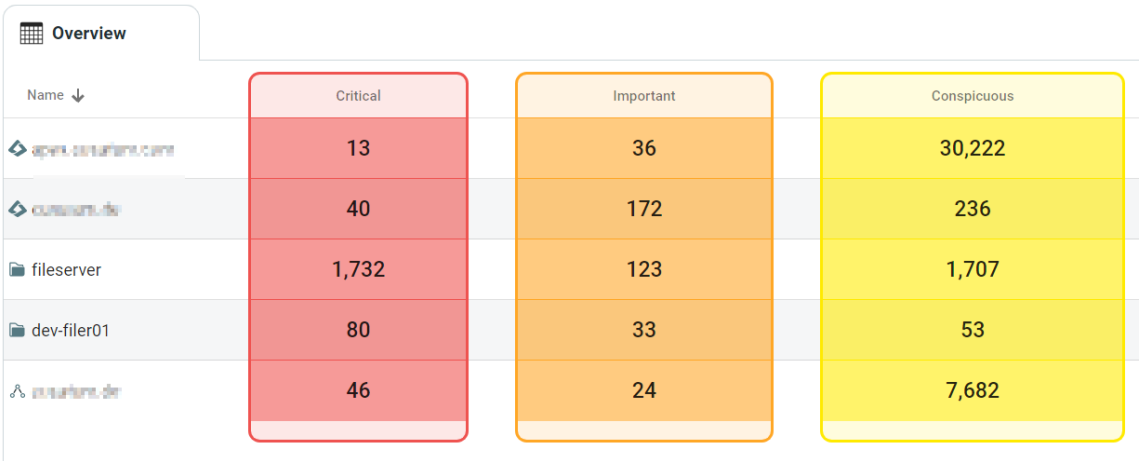
9	Check and correct minimum permissions	MARS	FS	
10	Find and eliminate interrupted inheritances, Finding and correcting moved directories	VASS	FS	Always perform at the end of the clean-up processes.
	Check list folder permissions	LARS	FS 👁	Always perform at the end of the clean-up processes.

👁 - is currently only offered as an audit module

Risk assessment by experts



With the **risk assessment dashboard**, you can see at a glance exactly where your biggest access rights problems are and how you can automatically correct them with just a few clicks.



Best Practices

CARO analyses and use cases

DARS

DUKE

BAKS

VASS

DARS

Direct access to analysis and restructuring software

- Identifies direct permissions of users
- Corrects these entries efficiently

Use case: Wilma Gucken is a member of the Finance department group and also has direct access to business data. Now that Wilma is no longer in the finance department, she still has access! DARS quickly finds all group and direct user accesses and effectively deletes these superfluous access rights. Notifications are generated for other users with direct access rights.

Check direct permissions

DUKE

Remove direct access rights for unwanted accounts

- Identifies all access rights of the configured unwanted accounts and removes them
- Reduces security risks by removing unknown and uncontrollable access rights

Use case: Administrators are granted full access by the UAC. DUKE removes these direct entries and restores group membership via the Administrators group.

Remove direct unwanted permissions

BAKS

Owner analysis and correction software

- Ensures authorised owners so that administrative accounts retain their permissions, e.g. so that backup tools work
- Analyses security risks by removing unauthorised and uncontrollable access rights

Use case: By creating directories and files, "normal" users gain ownership. This enables these users to change the authorisation themselves. In the worst case, administrators, service accounts and users are locked out. Best practice is to replace these users with the local file server administrators.

Correct owner

VASS

Inheritance analysis and sanitisation software

- Identifies changed authorisations in folder hierarchies
- Finds moved directories
- Alignment of permissions through inheritance or other system-specific tools

Use case: Breaking inheritance below the directory levels to be administered is often unintentional and results in users no longer being able to access these levels. Best practice is that all authorisations are inherited after the administration level. CUSATUM recommends a maximum of 4 levels.

Restore broken inheritances

Moved directories Find

Best Practices

CARO analyses and use cases

TEUS

LARS

ERBE

MARS

TEUS

Tool for removing unknown SIDs

- Removes dead SIDs and makes the documentation of your permissions easier to read and understand again
- Reduces the number of enquiries from your auditors and documents that you have full control
- Provides more security, as less attack surface for SID history injection

Use case: After deleting users and groups in the Active Directory, they are not automatically removed from the authorised resource ACLs. The orphaned or dead SID remains on the resources. These entries make necessary audit reports difficult to read and are also categorised as a security problem.

Remove unknown SIDs

LARS

List groups Analysis and restructuring software

- Analysing permissions in folder hierarchies
- Manage list permissions in parent folders

Use case: Users should be able to navigate to the "work directories". Best practice provides for list authorisation for this, which is controlled via Active Directory groups. Directories are often moved, created, renamed or deleted in the course of daily work. The list authorisations must be corrected so that users can continue to access the directories without any problems. Neither the administrators nor the software available on the market, e.g. SolarWinds-ARM, Tenfold or IDM/IAM systems, correct these problems in the long term.

Errors in list groups analyse

ERBE

Remove creator owner on file systems

- Removes the creator owner and prevents the creation of new dead SIDs
- Allows a clean migration, e.g. to the cloud

Use case: Microsoft's default setting when integrating new hard drives is to assign the creator-owner authorisation with full access. This creates direct authorisations that lead to an orphaned SID if the user is deleted. In addition, the user can lock out administrators, service accounts and users. CUSATUM's best practice is to remove this entry and work with a group authorisation.

Remove creator-owner

MARS

Minimum permissions analysis and restructuring software

- Checks all documents and folders for required access rights for accounts, considering both direct and indirect access rights
- Sets missing permissions

Use case: You want to check the minimum authorization for a user, e.g. whether a user or a service account has the minimum Modify everywhere. Often either no permissions are assigned, or the permissions are too low.

Minimum permissions check

Best Practices

CARO analyses and use cases

RAPA

SARA

RAPA

Redundant Account Permission Analysis

- Identifies redundant permissions
- Checking group memberships with simultaneous direct permissions

Use case: If a user has been assigned a direct authorization and an equivalent or higher group authorization, the direct authorization is redundant. In this case, the direct authorization can be removed. This also avoids the orphaned SID problem and makes the leaver process simpler and more effective.

Redundant permissions eliminate

SARA

Share Access Rights Analysis

Analysing share access rights

- Check for inherited NTFS access rights
- Search for **open shares** for authenticated accounts
- Searching for any-full-access shares
- Check for the existence of non-administrative share permissions

Use cases:

(1) The inheritance of NTFS access rights to shares should be deactivated. Changing inherited NTFS permissions remotely deletes all access rights and renders the share unusable.

(2) Shares are checked to see whether authenticated accounts (AD and local) have at least read access rights. These shares are then considered **open shares**. This can result in an uncontrolled outflow of data.

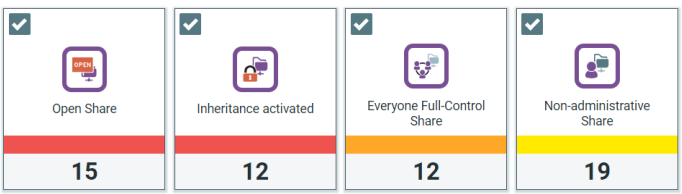
(3) The Everyone account should have maximum Modify access rights to the share. With full access, there is a risk that users could unknowingly cause damage with extended NTFS access rights.

(4) Your servers are checked for the existence of non-administrative shares. Administrative shares (C$, etc.) are ignored. Shares can allow uncontrolled access to critical information.

Check share permissions

SARA

CARO checks risky access rights to file server shares and finds your *open shares*.
This means that data can no longer be accessed unnoticed.



By enabling you to check your systems on a daily basis, CARO supports you where Access Rights Management and IDM systems reach their limits.

Best Practices

CARO analyses and use cases

EBIS

ARCA

ARCA

Account risk and compliance assessment

- Analysed account-based on best practice criteria
- For Active Directory and Entra ID

Active Directory (AD)

- Inactive user or computer accounts
- Deactivated user accounts
- User never logged in
- Empty groups and groups without description
- Accounts with passwords that never expire
- User with outdated password

Use case: The BSI and other IT audits, such as TISAX and BAFIN, check security-critical KPIs in the Active Directory. This allows the quality of employee processes and IT security to be checked and guaranteed. The most important AD analyses are summarized in the ARCA module and can be individually adapted.

Entra ID - access checks in the cloud

- Check global administrators for permitted number
- Check the number of privileged role assignments
- Exclusive use of groups in role assignments
- Check that only cloud-native accounts are used for role assignments
- Find expiring client keys in the app registrations
- Finding inactive guest users who have not logged in for a longer period
- Finding all inactive cloud-native users who are not synchronized with an on-prem AD

Use case: With CARO, you can now check and clean up your access for cloud-based and hybrid resources on Entra ID. CARO integrates best practices for Microsoft Entra roles*.

*A detailed description of Microsoft Best Practices can be found here: https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/best-practices

Account risk and compliance analyses for Active Directory and Entra ID

Display and report permissions

EBIS

Recording the actual permission situation

- Records the permissions situation on file servers and in the Active Directory
- Analyses for interrupted inheritance hierarchies, moved directories or null DACL, among other things
- Shows in detail the changed permissions below, such as added or removed access rights

Use case: You want to regularly check your permissions in the global resource view or create permission reports, such as a who-has-where access report, use case report or a permission difference report.

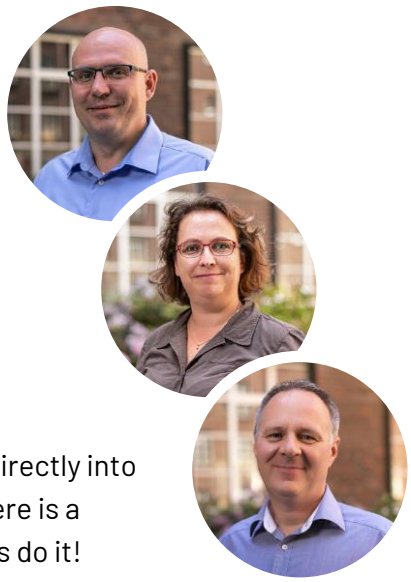
Recording the actual situation and report permissions

Best Practices

CUSATUM - Together for more safety!

CUSATUM Service GmbH in Berlin/Brandenburg is a software and consulting company with a focus on access rights management and the automation of employee processes. As "makers from the very beginning", we developed 8MAN from Protected Networks. This is now called SolarWinds-ARM and is still a great success in German-speaking countries today.

Today, we have combined our experience of one and a half decades in access rights management in our CARO-Suite. It is the necessary addition to ARM that was missing until now! The CARO-Suite supports companies in access rights management to fulfil common security and compliance guidelines.



Mike Wiedemann, CEO
His passion is customer satisfaction. He also goes the "extra mile" for satisfied customers!

Ute Wagner, CDO
A user interface must not only be easy to use, but it must also be a pleasure to use!

Christian Schönfeld, CEO
Converting my experience directly into CARO - that is my claim! There is a solution for everything. Let's do it!

CUSATUM

Publisher

CUSATUM Service GmbH

Head office
Wiesenweg 16
16548 Glienicke / Nordbahn

E-mail: info@cusatum.de
www.cusatum.de

Support

Telephone +49 30 94 86 3401
Mobile +49 175 221 11 04

e-mail support@cusatum.de

Status: Dezember 2024

SECURITY MADE IN GERMANY