COGNITUM Software

go:Roles - An efficient solution to analyze entitlements and design roles

Benefit from the advantages of an automated solution

The Problem

Who owns which permissions? Why? Today, in many organizations entitlements are assigned to users based on one's best knowledge.

Even with an Identity and Access Governance solution in place, entitlements and permissions are presumably assigned without best practices.

Furthermore, some organizations have de-ployed role-based access management based upon existing entitlements and permission assignments. This situation results from uncontrolled growth over the years, which leads to data security risks.

The Challenge

Requirements from Management, Data Protection and Auditors

The introduction and deployment of a role-based access concept is typically effective after go live.

In most cases existing entitlements and permission assignments are either revised superficially or transformed into business roles with a great deal of time and effort. With these general assumptions, we are left asking how standard processes can be implemented in a simple and cost-effective manner.

Constantly evolving regulatory requirements force reconsideration of legacy access assignment methods to a more flexible and agile role model concept.

Roles – a definition

- Roles are a logical reference between users and IT resources. A role defines tasks, properties and primarily permissions of a user
- A role describes why certain resources are required
- Instead of assigning permissions directly to a user, roles are defined to assign permissions to multiple users for the same purpose
- Roles are defined and configured independent from users
- Role management is essential to comply with the many regulations that manage governance and risk-management
- SoD (Segregation of Duties) Rules usually refer to functions or roles
- Roles are required to improve administrative efficiency in access management
- Roles are required to determine the responsibilities for certification of permissions
- Roles are the basis for structured Identity and Access Governance

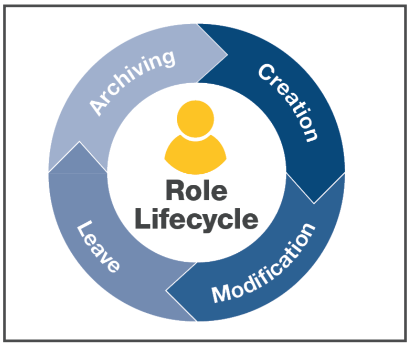
The Solution

A comprehensive, complete and centralized role management

go:Roles is a comprehensive tool to design, control and maintain business role models, which supports the concept of Identity and Access Governance (IAG). During an initial permission and entitlement assignment analysis, go:Roles helps to prepare role modelling. Role modelling simplifies the introduction and ongoing operation of an IAG solution with role-based access management.

go:Roles provides the foundation for Segregation of Duties (SoD). It is a standalone solution that can be implemented independently from any IAG solution.

go:Roles provides a central interface for role management. It is able to analyze individual applications, to inspect permissions and assigned accounts.



go:Roles supports the downstream certification process in 3rd party IAG solutions for entitlement objects (single and cumulative), and for permissions assigned to accounts through roles.

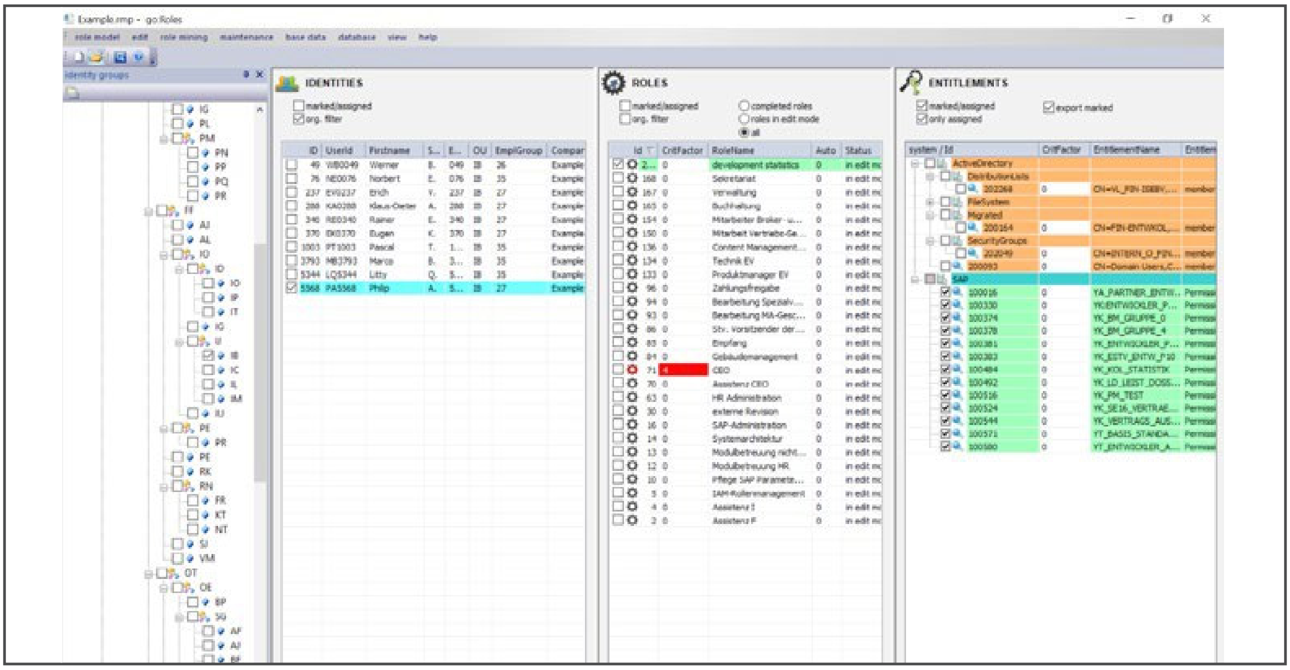
Core Features

Support in all phases and processes

- During data collection for organizations, identities, target system accounts and target system entitlements
- During initial role modelling, enhanced by smart role mining methods
- During deployment of an IAG solution
- During an as-is-assessment of target systems
- During the periodic maintenance of the role models
- During constant changes of the organizational structure and IT infrastructure

User Interface

Intuitive and user-friendly User Interface



IDENTITIES

□ marked/assigned
☑ org. filter

	ID	UserId	Firstname	S...	E...	OU	EmplGroup	Compar
□	49	WB0049	Werner	B.	049	IB	26	Example
□	76	NE0076	Norbert	E.	076	IB	35	Example
□	237	EV0237	Erich	V.	237	IB	27	Example
□	288	KA0288	Klaus-Dieter	A.	288	IB	27	Example
□	340	RE0340	Rainer	E.	340	IB	27	Example
□	370	EK0370	Eugen	K.	370	IB	27	Example
□	1003	PT1003	Pascal	T.	1...	IB	35	Example
□	3793	MB3793	Marco	B.	3...	IB	35	Example
□	5344	LQ5344	Litty	Q.	5...	IB	35	Example
☑	5368	PA5368	Philip	A.	5...	IB	27	Example

ROLES

□ marked/assigned
□ org. filter
○ completed roles
○ roles in edit mode
● all

	Id	CritFactor	RoleName	Auto	Status
☑	2...	0	development statistics	0	in edit mc
□	168	0	Sekretariat	0	in edit mc
□	167	0	Verwaltung	0	in edit mc
□	165	0	Buchhaltung	0	in edit mc
□	154	0	Mitarbeiter Broker - u...	0	in edit mc
□	150	0	Mitarbeit Vertriebs-Ge...	0	in edit mc
□	136	0	Content Management...	0	in edit mc
□	134	0	Technik EV	0	in edit mc
□	133	0	Produktmanager EV	0	in edit mc
□	96	0	Zahlungsfreigabe	0	in edit mc
□	94	0	Bearbeitung Spezialv...	0	in edit mc
□	93	0	Bearbeitung MA-Gesc...	0	in edit mc
□	86	0	Stv. Vorsitzender der...	0	in edit mc
□	85	0	Empfang	0	in edit mc
□	84	0	Gebäudemanagement	0	in edit mc
□	71	4	CEO	0	in edit mc
□	70	0	Assistenz CEO	0	in edit mc
□	63	0	HR Administration	0	in edit mc
□	30	0	externe Revision	0	in edit mc
□	16	0	SAP-Administration	0	in edit mc
□	14	0	Systemarchitektur	0	in edit mc
□	13	0	Modulbetreuung nicht...	0	in edit mc
□	12	0	Modulbetreuung HR	0	in edit mc
□	10	0	Pflege SAP Paramete...	0	in edit mc
□	5	0	IAM-Rollenmanagement	0	in edit mc
□	4	0	Assistenz I	0	in edit mc
□	2	0	Assistenz F	0	in edit mc

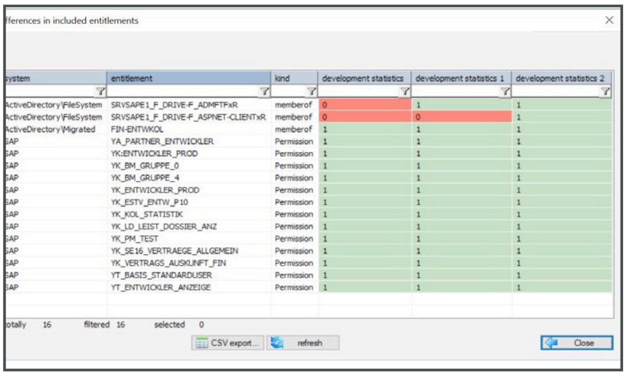
ENTITLEMENTS

☑ marked/assigned
☑ only assigned
☑ export marked

system / Id	CritFactor	EntitlementName	Entitlem
□ ActiveDirectory			
□ DistributionLists			
□ 202268	0	CN=VL_FIN-ISEBV,...	member
□ FileSystem			
□ Migrated			
□ 200164	0	CN=FIN-ENTWKOL,...	member
□ SecurityGroups			
□ 202049	0	CN=INTERN_O_FIN...	member
□ 200093	0	CN=Domain Users,C...	member
SAP			
☑ 100016	0	YA_PARTNER_ENTW...	Permiss
☑ 100330	0	YK:ENTWICKLER_P...	Permiss
☑ 100374	0	YK_BM_GRUPPE_0	Permiss
☑ 100378	0	YK_BM_GRUPPE_4	Permiss
☑ 100381	0	YK_ENTWICKLER_P...	Permiss
☑ 100383	0	YK_ESTV_ENTW_P10	Permiss
☑ 100484	0	YK_KOL_STATISTIK	Permiss
☑ 100492	0	YK_LD_LEIST_DOSS...	Permiss
☑ 100516	0	YK_PM_TEST	Permiss
☑ 100524	0	YK_SE16_VERTRAE...	Permiss
☑ 100544	0	YK_VERTRAGS_AUS...	Permiss
☑ 100571	0	YT_BASIS_STANDA...	Permiss
☑ 100580	0	YT_ENTWICKLER_A...	Permiss

*Figure: **go:Roles** displaying organizational structure, identities, roles and permissions*

- Clearly arranged and performant display of the relations between Organization ⟺ Identity ⟺ Roles ⟺ Entitlements
- Quick filtering of relevant information
- Mass operations on multiple roles
- Role comparison



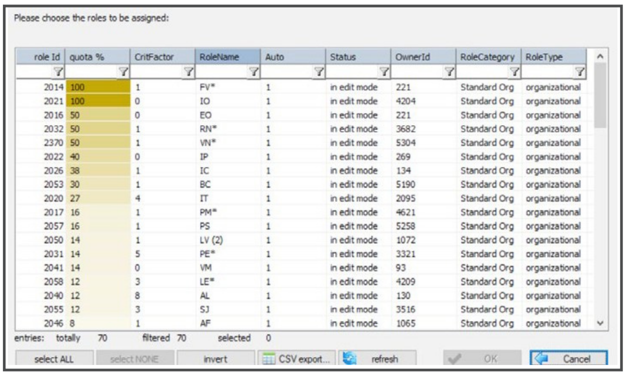
fferences in included entitlements

ystem	entitlement	kind	development statistics	development statistics 1	development statistics 2
ActiveDirectory\FileSystem	SRVSAPE1_F_DRIVE-F_ADMFTFxR	memberof	0	1	1
ActiveDirectory\FileSystem	SRVSAPE1_F_DRIVE-F_ASPNET-CLIENTxR	memberof	0	0	1
ActiveDirectory\Migrated	FIN-ENTWKOL	memberof	1	1	1
SAP	YA_PARTNER_ENTWICKLER	Permission	1	1	1
SAP	YK:ENTWICKLER_PROD	Permission	1	1	1
SAP	YK_BM_GRUPPE_0	Permission	1	1	1
SAP	YK_BM_GRUPPE_4	Permission	1	1	1
SAP	YK_ENTWICKLER_PROD	Permission	1	1	1
SAP	YK_ESTV_ENTW_P10	Permission	1	1	1
SAP	YK_KOL_STATISTIK	Permission	1	1	1
SAP	YK_LD_LEIST_DOSSIER_ANZ	Permission	1	1	1
SAP	YK_PM_TEST	Permission	1	1	1
SAP	YK_SE16_VERTRAEGE_ALLGEMEIN	Permission	1	1	1
SAP	YK_VERTRAGS_AUSKUNFT_FIN	Permission	1	1	1
SAP	YT_BASIS_STANDARDUSER	Permission	1	1	1
SAP	YT_ENTWICKLER_ANZEIGE	Permission	1	1	1

otally 16 filtered 16 selected 0

Figure: Role comparison based upon included permissions

- Illustration of role differences
- Cross-system search
- Task oriented access management
- List dialogs allow individual selections from displayed lists



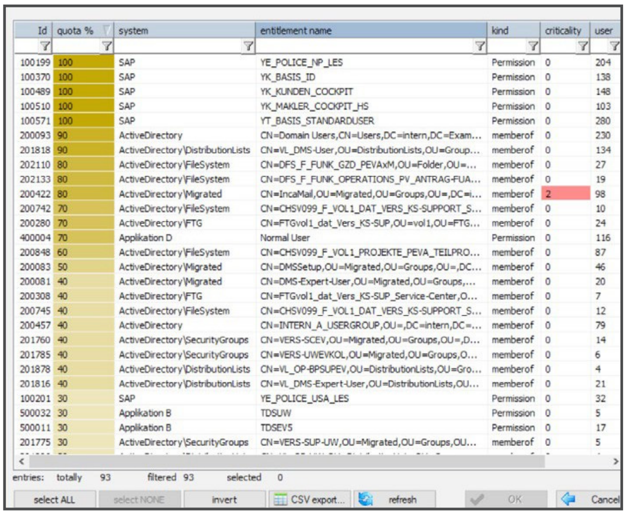
Please choose the roles to be assigned:

role Id	quota %	CritFactor	RoleName	Auto	Status	OwnerId	RoleCategory	RoleType
2014	100	1	FV*	1	in edit mode	221	Standard Org	organizational
2021	100	0	IO	1	in edit mode	4204	Standard Org	organizational
2016	50	0	EO	1	in edit mode	221	Standard Org	organizational
2032	50	1	RN*	1	in edit mode	3682	Standard Org	organizational
2370	50	1	VN*	1	in edit mode	5304	Standard Org	organizational
2022	40	0	IP	1	in edit mode	269	Standard Org	organizational
2026	38	1	IC	1	in edit mode	134	Standard Org	organizational
2053	30	1	BC	1	in edit mode	5190	Standard Org	organizational
2020	27	4	IT	1	in edit mode	2095	Standard Org	organizational
2017	16	1	PM*	1	in edit mode	4621	Standard Org	organizational
2057	16	1	PS	1	in edit mode	5258	Standard Org	organizational
2050	14	1	LV (2)	1	in edit mode	1072	Standard Org	organizational
2031	14	5	PE*	1	in edit mode	3321	Standard Org	organizational
2041	14	0	VM	1	in edit mode	93	Standard Org	organizational
2058	12	3	LE*	1	in edit mode	4209	Standard Org	organizational
2040	12	8	AL	1	in edit mode	130	Standard Org	organizational
2055	12	3	SJ	1	in edit mode	3516	Standard Org	organizational
2046	8	1	AF	1	in edit mode	1065	Standard Org	organizational

entries: totally 70 filtered 70 selected 0

Figure: Role assignment recommendations

One or multiple elements can be selected, displayed elements can be filtered.



Id	quota %	system	entitlement name	kind	criticality	user
100199	100	SAP	YE_POLICE_NP_LES	Permission	0	204
100370	100	SAP	YK_BASIS_ID	Permission	0	138
100489	100	SAP	YK_KUNDEN_COCKPIT	Permission	0	148
100510	100	SAP	YK_MAKLER_COCKPIT_HS	Permission	0	103
100571	100	SAP	YT_BASIS_STANDARDUSER	Permission	0	280
200093	90	ActiveDirectory	CN=Domain Users,CN=Users,DC=intern,DC=Exam...	memberof	0	230
201818	90	ActiveDirectory\DistributionLists	CN=VL_DMS-User,OU=DistributionLists,OU=Group...	memberof	0	134
202110	80	ActiveDirectory\FileSystem	CN=DFS_F_FUNK_GZD_PEVAxM,OU=Folder,OU=...	memberof	0	27
202133	80	ActiveDirectory\FileSystem	CN=DFS_F_FUNK_OPERATIONS_PV_ANTRAG-FUA...	memberof	0	19
200422	80	ActiveDirectory\Migrated	CN=IncaMail,OU=Migrated,OU=Groups,OU=,DC=i...	memberof	2	98
200742	70	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_DAT_VERS_KS-SUPPORT_S...	memberof	0	10
200280	70	ActiveDirectory\FTG	CN=FTGvol1_dat_Vers_KS-SUP,OU=vol1,OU=FTG...	memberof	0	24
400004	70	Applikation D	Normal User	Permission	0	116
200848	60	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_PROJEKTE_PEVA_TEILPRO...	memberof	0	87
200083	50	ActiveDirectory\Migrated	CN=DMSSetup,OU=Migrated,OU=Groups,OU=,DC...	memberof	0	46
200081	40	ActiveDirectory\Migrated	CN=DMS-Expert-User,OU=Migrated,OU=Groups,...	memberof	0	20
200308	40	ActiveDirectory\FTG	CN=FTGvol1_dat_Vers_KS-SUP_Service-Center,O...	memberof	0	7
200745	40	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_DAT_VERS_KS-SUPPORT_S...	memberof	0	12
200457	40	ActiveDirectory	CN=INTERN_A_USERGROUP,OU=,DC=intern,DC=...	memberof	0	79
201760	40	ActiveDirectory\SecurityGroups	CN=VERS-SCEV,OU=Migrated,OU=Groups,OU=,D...	memberof	0	14
201785	40	ActiveDirectory\SecurityGroups	CN=VERS-UWEVKOL,OU=Migrated,OU=Groups,O...	memberof	0	6
201878	40	ActiveDirectory\DistributionLists	CN=VL_OP-BPSUPEV,OU=DistributionLists,OU=Gro...	memberof	0	4
201816	40	ActiveDirectory\DistributionLists	CN=VL_DMS-Expert-User,OU=DistributionLists,OU...	memberof	0	21
100201	30	SAP	YE_POLICE_USA_LES	Permission	0	32
500032	30	Applikation B	TDSUW	Permission	0	5
500011	30	Applikation B	TDSEV5	Permission	0	17
201775	30	ActiveDirectory\SecurityGroups	CN=VERS-SUP-UW,OU=Migrated,OU=Groups,OU...	memberof	0	5

entries: totally 93 filtered 93 selected 0

Figure: Role Mining – Recommendations to enhance permission assignments

Role Modelling (Role-Mining)

- Free selection of organizational factors in a role model
- Support of inheritance upon hierarchical role modelling
- Top-down- und Bottom-up-Method
- Proven and optimized methods for role analysis
- Smart recommendations for creation and modification of candidate lists
- Organization and function-oriented role modelling

Role Definition

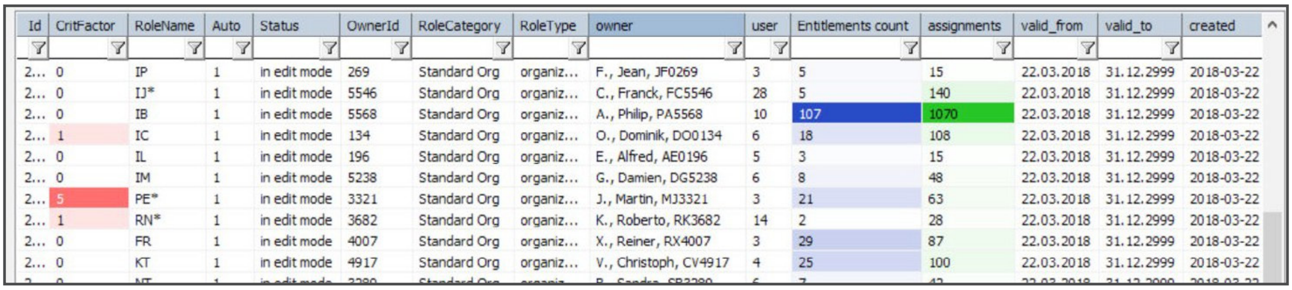
- Includes rules and policies for a recipient and requestor focused role assignment
- Expert and best practice role attributes
- Creation of role catalogues

Authorizations and assignments can be consolidated, analyzed and evaluated from different target systems. Likewise, organizational information can be imported to put it in context with the permissions, thereby automatically suggesting a role concept whose parameters can be adjusted.

Role Maintenance

- Role versioning
- Role status labelling to support approval workflows
- Role archiving
- Identification of possible duplicate role definitions with permissions and identity assignments
- Identification of roles contained in other roles
- Identification of unused roles
- Identification of speculative role assignments

Validation of Roles and Assignments



Id	CritFactor	RoleName	Auto	Status	OwnerId	RoleCategory	RoleType	owner	user	Entitlements count	assignments	valid_from	valid_to	created
2...	0	IP	1	in edit mode	269	Standard Org	organiz...	F., Jean, JF0269	3	5	15	22.03.2018	31.12.2999	2018-03-22
2...	0	IJ*	1	in edit mode	5546	Standard Org	organiz...	C., Franck, FC5546	28	5	140	22.03.2018	31.12.2999	2018-03-22
2...	0	IB	1	in edit mode	5568	Standard Org	organiz...	A., Philip, PA5568	10	107	1070	22.03.2018	31.12.2999	2018-03-22
2...	1	IC	1	in edit mode	134	Standard Org	organiz...	O., Dominik, DO0134	6	18	108	22.03.2018	31.12.2999	2018-03-22
2...	0	IL	1	in edit mode	196	Standard Org	organiz...	E., Alfred, AE0196	5	3	15	22.03.2018	31.12.2999	2018-03-22
2...	0	IM	1	in edit mode	5238	Standard Org	organiz...	G., Damien, DG5238	6	8	48	22.03.2018	31.12.2999	2018-03-22
2...	5	PE*	1	in edit mode	3321	Standard Org	organiz...	J., Martin, MJ3321	3	21	63	22.03.2018	31.12.2999	2018-03-22
2...	1	RN*	1	in edit mode	3682	Standard Org	organiz...	K., Roberto, RK3682	14	2	28	22.03.2018	31.12.2999	2018-03-22
2...	0	FR	1	in edit mode	4007	Standard Org	organiz...	X., Reiner, RX4007	3	29	87	22.03.2018	31.12.2999	2018-03-22
2...	0	KT	1	in edit mode	4917	Standard Org	organiz...	V., Christoph, CV4917	4	25	100	22.03.2018	31.12.2999	2018-03-22

Figure: Validation of roles and role assignments

- Current state (Target Systems) to desired state (go:**Roles**) analysis
- Templates for reassessment of entitlement assignments

More Functions

- Clearly arranged and performant display of role and entitlement assignments
- Focus on organization, branches and units
- Convenient filtering and sorting
- Support for validity periods (start/end dates)
- Export function (e.g. Role definitions)

go:Roles Technical Information

The application is based upon a Client-Server-Architecture and is

- Independent from existing Identity and Access Governance solutions
- Windows based
- MS SQL Database
- Multi-User-aware
- Auto-Update-aware

go:Roles Workshop

We provide a deployment workshop for **go:Roles**, to achieve optimal results:

- Step 1: Role concept, agreement on objectives and procedures
- Step 2: Design a role model basis
- Step 3: Data collection, data integration and data clearance
- Step 4: Determine role candidates
- Step 5: Definition and certification of roles
- Step 6: Go-live
- Step 7: Role management

go:Roles Workshop Method

- Think big, start small
- Combine Top-Down and Bottom-Up approach: Which roles are required by business (Top-Down) and which roles are derived from user privileges (Bottom-Up)?
- Roles and role models are multi-level and hierarchical.
- Roles allow more flexibility. Use it and constantly challenge the role model.
- Roles are designed to be re-used.
- Who has what responsibility? Only a clear definition of responsibilities will support long-term success.
- Always use current and valid data, which includes continual review and clean-up of source and target systems.
- Business and IT have to work together and drive the project to achieve the best results!

go:Roles

Benefit from an intuitive and automated entitlement analysis solution

✓ **go:efficient** – Reduce human workload

✓ **go:cost-effective** – Quick results

✓ **go:simple** – Resolve entitlement complexity

✓ **go:integrative** – Interoperate with any IAG solution

COGNITUM Software

go:Roles

COGNITUM Software combines long-term Identity and Access Governance expertise for the development of standard software.

Identity & Access Governance is a key component in building a secure IT infrastructure. With our comprehensive practical experience in consulting, implementation and our expertise in identity and access governance solutions, we have developed our software that is deployable rapidly and cost effective - for any business, regardless of industry and size. COGNITUM Software emerged from ITConcepts group, a leading, global IT service provider and agnostic system integrator.

COGNITUM Software Team GmbH
Leitschweg 2c, 38448 Wolfsburg, Germany • Phone: +49 5361 8349527 • Email: info@cognitum-software.com • Web: www.cognitum-software.com