Rollen und Rechte

Als erstes haben wir eine Übersicht der verschiedenen Rollen erstellt.
Diese ist hierarchisch aufgebaut: klicken Sie die Rolle auf und Sie sehen unterliegende(n) Rolle(n) zum Vorschein kommen:

Eine Übersicht über die wichtigsten Rollen und deren Rechte sind in der ersten Tabelle ersichtlich. Primäres Ziel ist es hier, eine einfache Lösung für die wichtigsten Rollen anzubieten, um eine transparente und effiziente Benutzerverwaltung inklusive Berechtigungen zu ermöglichen. Die Rollen Expert, Viewer, Coordinator und Admin können bei Bedarf feingranularer aufgeteilt werden, Details dazu mit den entsprechenden Berechtigungs-Zuteilungen sind in der zweiten Tabelle dargestellt.

Die grossgeschriebenen Bezeichnungen (z.B. ENDUSER) kommen bei der Rechtesynchronisation via LDAP zum Tragen, siehe LDAP (Active Directory) Systemparameter, Parameter LDAP_SECURITY_GROUPS_MAPPING.

Übersicht:

Berechtigung	**Enduser**	**Viewer**	**Expert**	**Admin**	**IT Support**
	(ENDUSER)	**(VIEWER)**	**(EXPERT)**	**(ADMIN)**	**(IT_SUPPORT)**
Anwendungsbeispiel	Mitarbeiter	internal Audit	IKS-Verantwortlicher	Admin für OE	System Verantwortlicher
Lesen Kontroll-Setup		X	X		X [9)]
Bearbeiten Kontroll-Setup			X		X [9)]
Lesen Kontroll-Task	X [11)]	X	X		X [9)]
Support leisten für Kontroll-Task [8)]					X [9)]
Bearbeiten eigener/delegierter Kontroll-Tasks	X				
Abschliessen eigener/delegierter[1)] Kontroll-Tasks	X				
Lesen Bericht	X [13)]	X [14)]	X [14)]		X [14)]
Bearbeiten Action/Bericht			X [14)]		X [14)]
Erstellen Action	X [2)]		X [14)]		X [14)]
Lesen Action	X [11)]	X [14)]	X [14)]		X [14)]
Support leisten für Action [8)]					X [14)]
Erfassen Implementierungs-Fortschritt	X[3)]		X [14)]		X [14)]
Abschliessen Action	X[4)]				X [14)]
Lesen Risiko/Prozess		X	X		X [9)]
Bearbeiten Risiko/Prozess			X		X [9)]
Verknüpfen Risiko/Prozess			X		X [9)]
Lesen Risiko Assessment	X	X	X		X [9)]
Bearbeiten Risiko Assessment			X		X [9)]
Benutzer wechseln					X [9)]
Bearbeiten Stellvertreter	X			X	X [9)]
Lesen Benutzerrechte				X	X [9)]
Bearbeiten Benutzerrechte				X	X [9)]
Bearbeiten Mitarbeiter/Organisationseinheiten				X	X [9)]
Bearbeiten System Konfiguration				X	X
Lesen System Parameter/BatchJobs				X	X
Bearbeiten Workflows				X	X
Bearbeiten System Parameter/BatchJobs					X

Lesen Ereignisse	X [11]	X [12]	X [12]		X [12]	
Bearbeiten Ereignisse			X [12]		X [12]	
Lesen Dokument [9]	X [11]	X	X	X	X [9]	
Bearbeiten (zentrales) Dokument [9] [10]				X	X [9]	

Weitere Rollen, feingranular aufgeteilt je nach Tätigkeitsgebiet:

Berechtigung	**Control Expert**	**Control Viewer**	**Action Expert**	**Action Viewer**	**Risk Expert**	**Risk Viewer**	**Incident Expert**	**Incident Viewer**	**Document Admin**	**Document Viewer**	**User Admin**	Coordinator	Control Coordinator	Action Coordinator
	(CONTROL_ EXPERT)	**(CONTROL_ VIEWER)**	**(ACTION_ EXPERT)**	**(ACTION_ VIEWER)**	**(RISK_ EXPERT)**	**(RISK_ VIEWER)**	**(INCIDENT_ EXPERT)**	**(INCIDENT_ VIEWER)**	(DOCUMENT_ADMIN)*	(DOCUMENT_VIEWER)*	**(USER_ ADMIN)**	(COORDINATOR)	(CONTROL_ COORDINATOR)	(ACTION_ COORDINATOR)
Hinweise	IKS (Interne Kontrollen)		IA (Issues & Actions)		Risikomanagement		Operationelle Ereignissse		DMS (Dokumente)		Administration	Sehr selten verwendet		
Lesen Kontroll-Setup	X	X										X	X	
Bearbeiten Kontroll-Setup	X													
Lesen Kontroll-Task	X	X										X	X	
Support leisten für Kontroll-Task [8]												X	X	
Bearbeiten eigener /delegierter Kontroll-Tasks														
Abschliessen eigener /delegierter[1] **Kontroll-Tasks**														
Lesen Bericht			X [14]	X [14]										
Bearbeiten Action /Bericht			X [14]											
Erstellen Action			X [14]											
Lesen Action			X [14]	X [14]								X [14]		X [14]
Support leisten für Action [8]												X [14]		X [14]
Erfassen Implementierungs-Forschritt			X [14]									X [14]		X [14]
Abschliessen Action												X [14]		X [14]
Lesen Risiko/Prozess					X	X								
Bearbeiten Risiko /Prozess					X									
Verknüpfen Risiko /Prozess	X		X		X									
Lesen Risiko Assessment					X	X								
Bearbeiten Risiko Assessment					X									
Benutzer wechseln												X	X	X
Bearbeiten Stellvertreter											X	X	X[5]	X[6]
Lesen Benutzerrechte											X	X	X	X
Bearbeiten Benutzerrechte											X			
Bearbeiten Mitarbeiter /Organisationseinheiten											X			
Bearbeiten System Konfiguration														
Lesen System Parameter/BatchJobs														
Bearbeiten Workflows														
Bearbeiten System Parameter/BatchJobs														
Lesen Ereignisse							X [12]	X [12]						
Bearbeiten Ereignisse							X [12]							
Lesen Dokument [9]	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Bearbeiten (zentrales) Dokument [9] [10]									X					

*noch nicht umgesetzt in der Rechte-Synchronisation

Fussnoten und Details:

[1] wenn delegiert mit Abschliessen
[2] wenn der Actiontyp die Erstellung von Enduser erlaubt
[3] nur wenn "darf bearbeiten" Checkbox für Action Owner selektiert ist
[4] nur wenn "darf bearbeiten" Checkbox für Action Owner selektiert ist & Enduser = Primary Action Owner ist
[5] nur für Kontrollen
[6] nur für Action
[7] inkl. Überwachung / Hochladen von Bewertungsgrundlagen
[8] via Benutzer wechseln
[9] Reichweiten sind: OE
[10] im Sinne von «zentralen» Dokumenten – bei Attachments (z.B. bei Tasks / Actions, ...) wird dieses Recht nicht abgefragt
[11] mit eigener OE
[12] geprüft werden OE UND Incident Type
[13] nur wenn der Enduser in einem spezifischen Bericht "zusätzliche Leseberechtigung" erhält
[14] geprüft werden OE UND Action Type

Scopes bestimmen die Reichweiten der Berechtigungen

Je nach Rolle sind verschiedene Scope-Einschränkungen möglich. Scopes bestimmen die Reichweite / Gültigkeitsgebiet der Rechte.
So können Rechte nur für eine bestimmte OE vergeben und sehr fein granular gemäss "Need-to-know"-Prinzip vergeben werden.

Nachfolgend die in der Applikation vorhandenen Scopes zur Übersicht. Hinweis: nicht alle Scopes sind für jede Rolle relevant. So sind beispielsweise die Administratoren des Systems nicht nach Typen getrennt und können alle Typen zu einem Themenbereich administrieren, während die Expertenrechte für bestimmte Typen vergeben werden können. Als Extremfall sei hier speziell die Rolle IT Support erwähnt: wenn man dieser Rolle keinerlei Scope zuteilt (weder OE noch Typen der verschiedenen Objekte), kann man einer Person die Systemkonfiguration ermöglichen, ohne dass sie irgendwo erfasste Daten sieht.

Scope	Erklärung	Details und Hinweise
OE	bestimmt für welche Organisationseinheiten die Rolle vergeben wird	Die genannte OE's und alle darunter liegenden werden dem Benutzer freigeschaltet. Mehrfach-Nennungen sind möglich.
Ereignis-Typen	ermöglicht die Einschränkung auf bestimmte Ereignistypen	nur relevant für das Modul OpLoss (Operationelle Ereignisse)
Action-Typen	ermöglicht die Einschränkung auf bestimmte Actiontypen	nur relevant für das Modul Action Tracking (IA), ab Release 2.24 möglich
Risiko Assessment -Typen	ermöglicht die Einschränkung auf bestimmte Risiko Assessment-Typen	Diese Reichweite wird mit OE kombiniert - falls die OE nicht gefüllt oder das Dropdown bei "Nur ausgewählte RA-Typen" leer ist, erhält der Benutzer keine Rechte auf Risiko Assessments.
Dokument-Typen	ermöglicht die Einschränkung auf bestimmte Dokument-Typen	nur relevant für das Modul DMS, falls es relevante Dokumenten-Typen gibt
Workflow-Typen	ermöglicht die Einschränkung auf bestimmte Workflow-Typen	nur relevant für Workflows, ab Release 2.22 möglich
BCM-Zyklus-Typen	ermöglicht die Einschränkung auf bestimmte BCM-Zyklus-Typen	nur relevant für das Modul BCM

Zusatzinformationen

Es gibt an einzelnen Stellen zusätzliche Regelungen die betreffend Benutzer-Rechten relevant sein können:

- In Produktion kann ein Administrator seine eigenen Rechte nicht ändern, in den Test-Umgebungen hingegen schon.
- Einzelne Rollen / Scopes sind nur relevant wenn die entsprechenden Module genutzt werden
- teilweise gibt es zusätzliche Einstellungen in den Konfigurationen um weitere Vertraulichkeitsstufen zu definieren, zwei Beispiele:
  - "Geschlossener Benutzerkreis" in den OE's
  - "Immer sichtbar für eigene OE" im Dokumenten-Typ (DMS)
- Mit dem Release 2.25 wurde am 14.07.2023 die Rolle "System Admin" entfernt, sie kann identisch mit dem IT Support ohne Scopes abgebildet werden

Verwandte Seiten

- Rollen und Rechte
- Aufsetzen eines Actiontyps
- Konfigurierbare Zusatzfelder für Actions, Issues und Berichte
- Action/Bericht/Issue Workflow
- Allgemeines zu Issues und Actions