Administration - Benutzerprofile

BIC Integrated GRC 2026 Summer

Dokument Version: Juni 2026

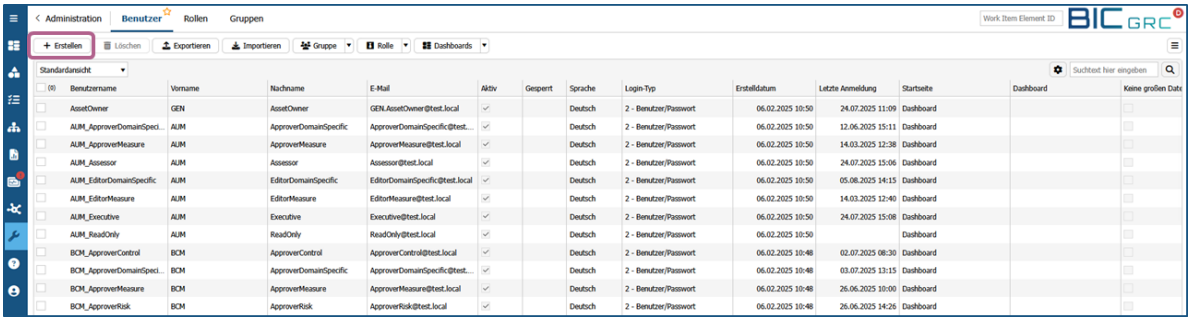
Inhaltsverzeichnis

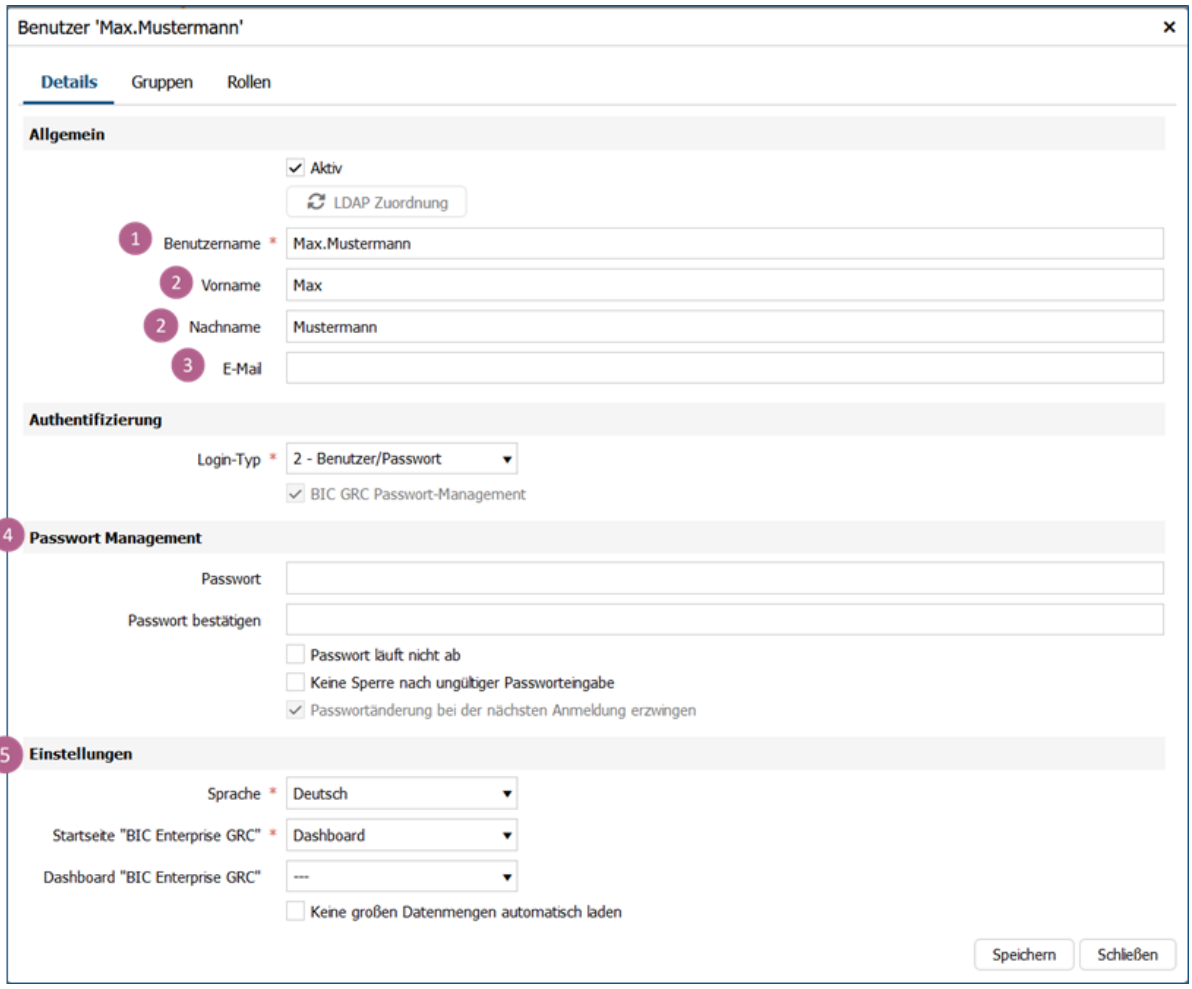
1 Benutzer

Ein Benutzer ist eine individuelle Person, die eine bestimmte Aufgabe im Zusammenhang mit GRC im Unternehmen übernimmt. Um dieser Aufgabe im GRC Umfeld nachkommen zu können, braucht der Benutzer einen passenden Zugang zu BIC GRC.

1.1 Benutzer anlegen

Benutzer werden unter dem Menüpunkt **Administration >> Benutzerverwaltung >> Benutzer** erstellt. Mittels des Buttons "Erstellen" kann ein neuer Benutzer angelegt werden.





1. **Benutzername**: Der Benutzername ist jener Name, mit dem sich der Benutzer immer in BIC GRC anmelden wird. Er ist verpflichtend anzugeben.
2. **Name**: Anschließend sind der Vor- und Nachnamen zu hinterlegen. Diese Angabe ist optional.

   Sind in BIC GRC keine Vor- oder Nachnamen hinterlegt, wird der Benutzername verwendet, um in Work Items User zu verlinken.
3. **E-Mail:** Soll der Benutzer im Rahmen seiner Tätigkeiten E-Mail-Notifikationen erhalten, muss hier eine Mail Adresse der Person angegeben werden.

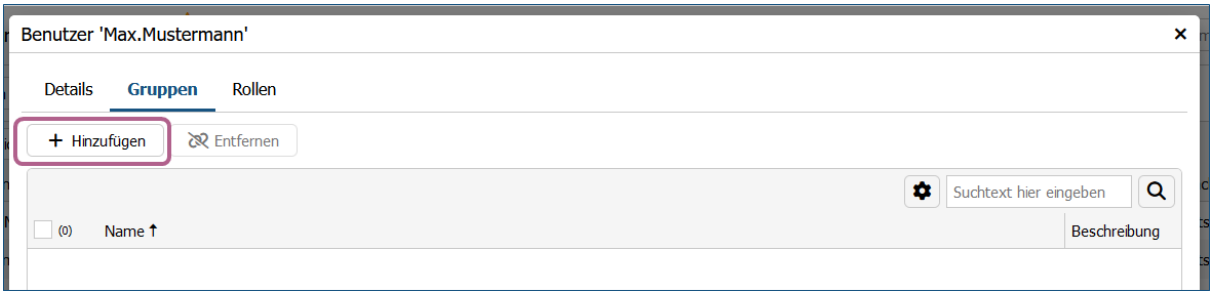
   > Ist in den Work Items eine Notifikation vorgesehen, der Benutzer hat allerdings keine Mail-Adresse hinterlegt, wird der durchführende Benutzer mittels Warnungshinweis darauf hingewiesen.
4. **Passwort**: Das Passwort wird für den Benutzer von der Person gesetzt, die seinen Benutzer anlegt.
5. Weitere Einstellungen: Neben den perönlichen Eingaben für den Benutzer, kann auch festeglegt werden, mit welchen Startbedingungen der Benutzer in BIC GRC startet, wie beispielsweise Sprache und Einstiegspunkt in BIC GRC

Nach einem ersten Speichervorgang wird der User in BIC GRC angelegt. Eine Zuteilung des Benutzerprofils erfolgt im nächsten Schritt.

1.1.1 Gruppen zuweisen

Nachdem ein Benutzer erstellt wurde kann eine (oder mehrere) Gruppe zugewiesen werden.

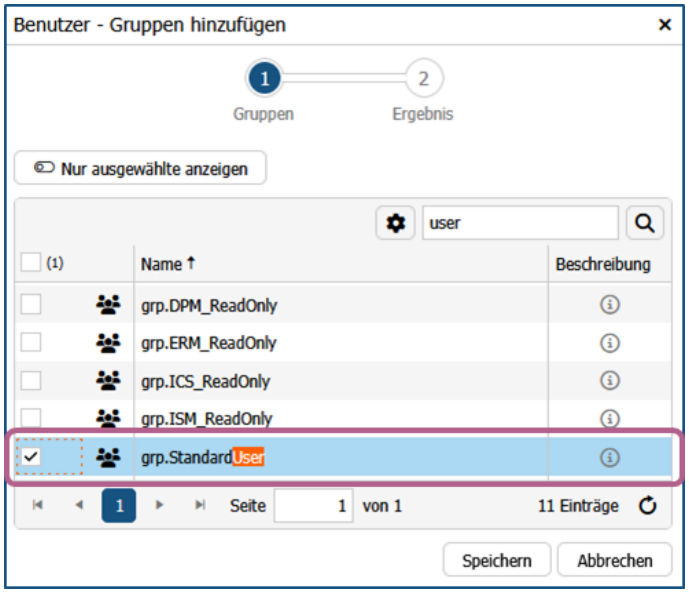
Die Zuteilung erfolgt im Reiter "Gruppen" in der spezifischen Benutzeransicht.



Anschließend geht eine neue Ansicht auf, in der verschiedene Gruppen vorgeschlagen werden, die zugewiesen werden können.

> Die Gruppen gehören dabei immer zu einem Benutzerprofil, dass sich aus einer Gruppe und einer Rolle zusammen setzen.

Durch setzen des Häckchens kann eine Gruppe ausgewählt werden. Danach kann die Auswahl gespeichert und die Ansicht geschlossen werden.



> Es wird empfohlen immer nur eine Gruppe und gleich im Anschluss die passende Rolle zu vergeben und nicht alle Berechtigungen auf einmal zu vergeben.

1.1.2 Rollen zuweisen

Nachdem ein Benutzer erstellt wurde und eine Gruppe passend zu einem Benutzerprofil vergeben wurden, kann die passende Rolle zugewiesen werden.

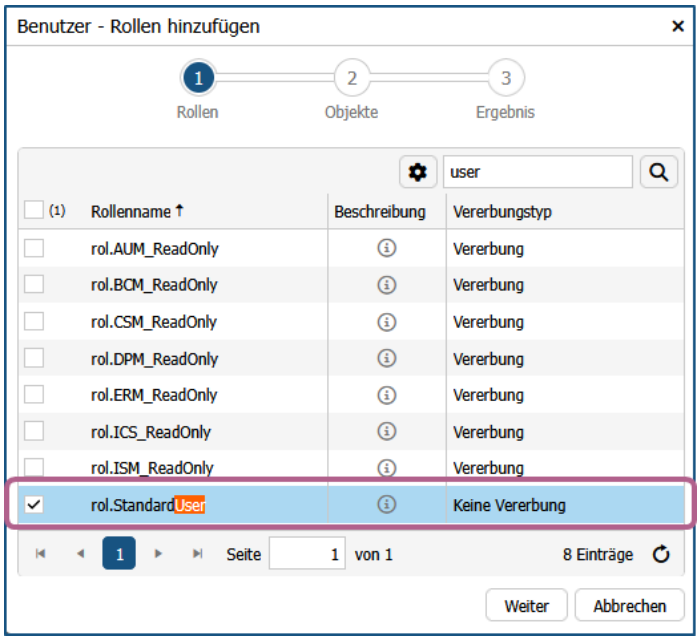
Die Zuteilung erfolgt im Reiter "Rollen" in der spezifischen Benutzeransicht.

Anschließend geht eine neue Ansicht auf, in der verschiedene Rollen vorgschlagen werden, die zugewiesen werden können.

> Die Rolle die zugewiesen wird sollte denselben Namen tragen, wie die zuvor zugewiesene Gruppe, um ein vollständiges Benutzerprofil herzustellen.

Durch setzen des Häckchens kann eine Rolle ausgewählt werden.

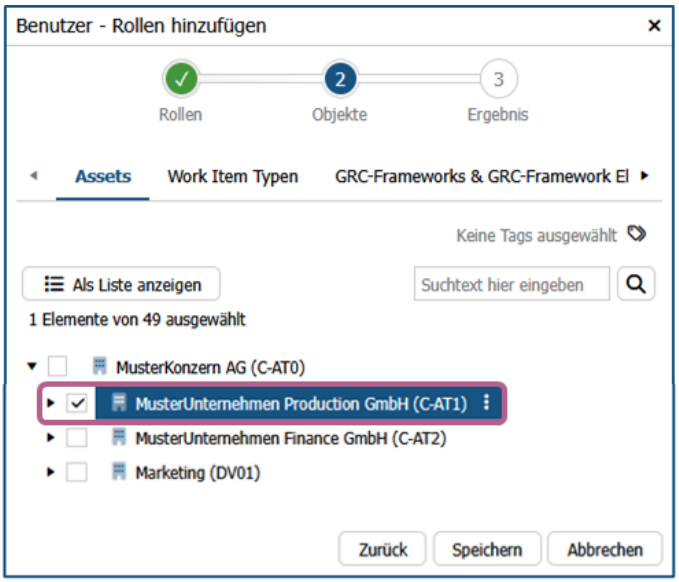
Danach kann im unteren rechten Abschnitt auf "Weiter" geklickt werden, um das passende Asset auszuwählen.



Im nächsten Schritt wird der Ersteller auf diese Ansicht weitergeleitet.

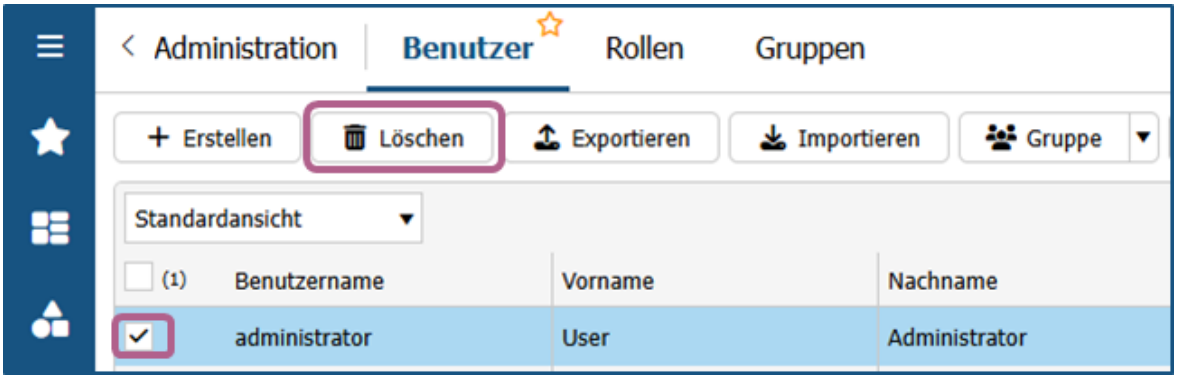
An dieser Stelle muss nur unter dem Punkt "Asset" bestimmt werden, auf welches Asset (Gesellschaft, Prozess,...) der spezifische Benutzer berechtigt werden soll.

Steht im vorherigen Schritt der Auswahl der Rolle neben der Rolle "Vererbung" bedeutet dies, dass das oberste Asset gewählt werden kann und der Benutzer für die unterliegenden Assets aufgrund der Vererbung auch berechtigt wird in einem Schritt. Steht "Keine Vererbung" müssen alle Assets markiert werden, wo dieses Benutzerprofil zur Anwendung kommen soll.



1.2 Benutzer löschen

Benutzer können unter dem Menüpunkt **Administration >> Benutzerverwaltung >> Benutzer** gelöscht werden. Mittels der Markierung des Benutzers mittels klicken der Checkbox und anschließenden klicken des Buttons "Löschen" kann ein bestehender Benutzer gelöscht werden.



> Dem Benutzer werden bei dem Löschvorgang durch das System auch die Rollen- und Gruppenrechte entzogen.

2 Benutzerprofile

Alle Module in BIC GRC basieren auf einem einheitlichen Konzept: dem der Benutzerprofile. Ein Benutzerprofil definiert die Berechtigungen einer Person innerhalb des Systems und steuert, welche Informationen diese Person sehen, bearbeiten oder auswerten darf.

Mittels Benutzerprofilen werden Berechtigungen definiert, welche eine definierte Gruppe von Personen, zum arbeiten benötigt – beispielsweise ein Prozessverantwortlicher, ein Risikoeigner oder eine Ansprechperson für Datenschutz sowie Audit.

Damit eine Person aktiv in BIC GRC arbeiten kann – z. B. um Inhalte zu erfassen, Maßnahmen zu dokumentieren oder Berichte zu generieren–, muss sie als Benutzer in BIC GRC angelegt sein. Nur mit einem Benutzer kann das System:

- Lese- und Bearbeitungsrechte je nach Kontext zuweisen
- Notifikationen (z. B. Aufgaben, Erinnerungen) zustellen
- Beteiligungen an Workflows oder Freigaben steuern

Jedes Benutzerprofil in BIC GRC besteht aus zwei zentralen Berechtigungselementen – unabhängig vom verwendeten Modul:

- Gruppe: Bestimmt den fachlichen Zugriff auf Inhalte. Sie legt fest, welche Daten der Benutzer sehen darf – beispielsweise aus einer bestimmten Domäne wie Enterprise Risk, Information Security oder Internal Control.
- Rolle: Definiert den organisatorischen Bezug zu bestimmten Assets (z.B. Organisationseinheiten, Prozessen oder Systemen). Sie steuert, wo der Benutzer auf Inhalte zugreifen darf – also innerhalb welcher Kontextobjekte (Assets) diese Gruppe wirkt.

Das Zusammenspiel von Gruppe und Rolle ergibt ein vollständiges Benutzerprofil – es legt fest, wer was wo darf.

Die genaue Funktionsweise dieser beiden Ebenen, ihr Zusammenwirken mit konkreten Benutzern sowie die praktische bzw. hierarchische Zuweisung von Benutzerprofilen wird in den folgenden Kapiteln im Detail erläutert.

2.1 Benutzerprofile benutzen

In BIC GRC kann Benutzern ein oder mehrere Benutzerprofile zugewiesen werden. Die Anzahl und Art der Profile richtet sich dabei flexibel nach der Größe und Struktur des Unternehmens.

> **Bei kleinen Unternehmen kann eine Führungskraft alle Profile erhalten, welche für die Durchführung von Freigaben notwendig sind. Während es sich bei großen Unternehmen anbietet jedes dieser für Freigaben notwendigen Profile einer auf diese spezialisierten Person aufzuteilen.**

Im nächsten Schritt zeigen wir Ihnen, wie die Benutzerprofile abhängig von der jeweiligen Hierarchiestufe sinnvoll verteilt werden können – damit Benutzer genau die Zugriffsrechte und Funktionen erhalten, die sie für ihre Aufgaben benötigen.

2.1.1 Grundprämissen / Best Practice

- Klare Rollenverteilung

  Jede Person erhält eine oder mehrere Benutzerprofile im System. Diese Benutzerprofile bestimmen, welche Inhalte eingesehen, bearbeitet oder freigegeben werden können. So wird sichergestellt, dass jede Person nur die Funktionen nutzt, die sie für ihre Arbeit benötigt.

- Trennung von Aufgaben

  Für zentrale Arbeitsschritte – etwa das Erfassen, Prüfen oder Freigeben von Inhalten – sind unterschiedliche Personen vorgesehen. Damit wird das Vier- Augen- Prinzip eingehalten und die Qualität der Inhalte erhöht.

- Zugriff nur auf relevante Inhalte

  Benutzerinnen und Benutzer sehen nur die Objekte (z. B. Risiken, Maßnahmen, Kontrollen), die zu ihrem Verantwortungsbereich gehören. So bleibt der Fokus auf den eigenen Aufgaben und die Übersicht im System erhalten.

- Einheitliches Konzept in allen Modulen

  Das Berechtigungssystem funktioniert in allen GRC-Domänen gleich – etwa im Risiko-, Informationssicherheits- oder BCM-Modul. Dadurch sind Rollen, Zuständigkeiten und Abläufe überall konsistent.

- Klare Trennung zwischen Administration und Facharbeit

  Administrative Rollen kümmern sich um Strukturen, Benutzerverwaltung und Systemeinstellungen. Fachrollen bearbeiten Inhalte, ohne in die Systemkonfiguration einzugreifen.

- Nachvollziehbarkeit und Transparenz

  Alle Änderungen werden automatisch im System dokumentiert.Dadurch ist jederzeit nachvollziehbar, wer wann welche Inhalte bearbeitet oder freigegeben hat.

- Zentral gepflegte Berechtigungsstruktur

  Berechtigungen werden zentral verwaltet. So bleiben Zuständigkeiten übersichtlich, konsistent und leicht anpassbar.

2.1.2 Domänenunabhängige Benutzerprofile

Während in den nächsten Kapiteln auf die Zuweisung von domänenspezifischen Benutzerprofilen eingegangen wird, behandelt dieses Kapitel die domänenunabhängigen Benutzerprofile, also mit anderen Worten Benutzerprofile die allgemein gelten.

- Standard User
- Asseteigner
- Asset Manager
- Tester
- Dokumenteneigner
- Dokumentenmanager
- Interner Anfrageempfänger
- Berechtigungsanfrageempfänger
- Fachlicher Administrator
- Technischer Administrator
- BIC Connector

2.1.2.1 Standard User

Das Benutzerprofil Standard User berechtigt alle Benutzer BIC GRC zu öffnen. Es handelt sich um ein "Basis"-Benutzerprofil das jedem Benutzer zugeteilt werden muss.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser

2.1.2.2 Asseteigner

Der Asseteigner ist ein Benutzer der für ein Asset verantwortlich ist. Dabei kann es sich um einen Prozesseigner (Primary Asset) oder eine verantwortliche Person für einen Unternehmensstandort (BusinessUnit) handeln. Es wird empfohlen pro Asset nur einen verantwortlichen Asseteigner zu hinterlegen.

Anders als bei anderen Benutzerprofilen wird die Berechtigung nicht auf darunterliegende Assets vererbt, sondern es muss jedes Asset, für das der Asseteigner verantwortlich eigens angegeben werden.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.AssetOwner	• rol.AssetOwner

2.1.2.3 Asset Manager

Das Benutzerprofil Asset Manager kümmert sich um das Managen der Assets in BIC GRC. So kann es beispielsweise für einen Standort einen eigenen Asset Manager geben, der alle darunterliegenden Assets verwaltet, pflegt und den zugehörigen Benutzern zugänglich macht, für diese Assets aber nicht im Unternehmenskontext verantwortlich ist.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AssetManager	• rol.StandardUser • rol.AssetManager

> Der Asseteigner ist der fachlich Verantwortliche für ein Asset, während der Asset Manager sich um die Verwaltung des Assets in BIC GRC kümmert.

2.1.2.4 Tester

Das Benutzerprofil Tester kann jedem Benutzer in BIC GRC zugeordnet werden, der sich um die Testung von Kontrollen kümmert. Dabei ist es nicht relevant aus welchem Modul die Kontrolle kommt, sonder nur dass sie im Unternehmenskontext nicht irreführend ist.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.Tester	• rol.StandardUser • rol.Tester

2.1.2.5 Dokumenteneigner

Das Benutzerprofil Dokumenteneigner kann jedem Benutzer in BIC GRC zugeordnet werden, der sich um die Erstellung und Pflege von internen Dokumenten, Richtlinies oder andern Informationen kümmert. Die von ihm gepflegten "Dokumentierten Informationen" können anschließend in jedem Modul verwendet und verlinkt werden.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.DocumentOwner	• rol.StandardUser • rol.DocumentOwner

2.1.2.6 Dokumentenmanager

Das Benutzerprofil Dokumentenmanagerist für die Freigabe von "Dokumentierten Informationen" zuständig, wenn sie in seinen Zuständigkeitsbereich fallen.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.DocumentManager	• rol.StandardUser • rol.DocumentManager

2.1.2.7 Interner Anfrageempfänger

Benutzer die dieser Gruppe zugeteilt werden können den spezifischen Work Item Typen "Interne Anfrage" beantworten bzw. den richtigen Verantwortlichen zukommen lassen. Da dieses Benutzerprofil keinem Asset zugeordnet wird sollte dieses Benutzerprofil nur an Benutzer mit vielen Aufgaben und Rechten in BIC GRC vergeben werden.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.InternalRequestReceiver	• rol.StandardUser

2.1.2.8 Berechtigungsanfrageempfänger

Benutzer die dieser Gruppe zugeteilt werden können den spezifischen Work Item Typen Berechtigungsanfrage" bearbeiten. Da dieses Benutzerprofil keinem Asset zugeordnet wird sollte dieses Benutzerprofil nur an Benutzer mit vielen Aufgaben und Rechten in BIC GRC vergeben werden.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.PermissionRequestReceiver	• rol.StandardUser

2.1.2.9 Fachlicher Administrator

Der Fachliche Administrator ist für den operativen Betrieb verantwortlich. Um dieser Aufgabe nachzukommen hat er den Zugang zu allen Work Items, Assessments und Dashboards jedes aktiven Moduls.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.FunctionalAdministrator	• rol.StandardUser

2.1.2.10 Technischer Administrator

Der Technische Administrator ist in erster Linie für die Vergabe von Berechtigungen verantwortlich. Des weiteren ist er für den technischen Support und Einrichtung des Systems bzw. für Updates verantwortlich.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.TechnicalAdministrator	• rol.StandardUser

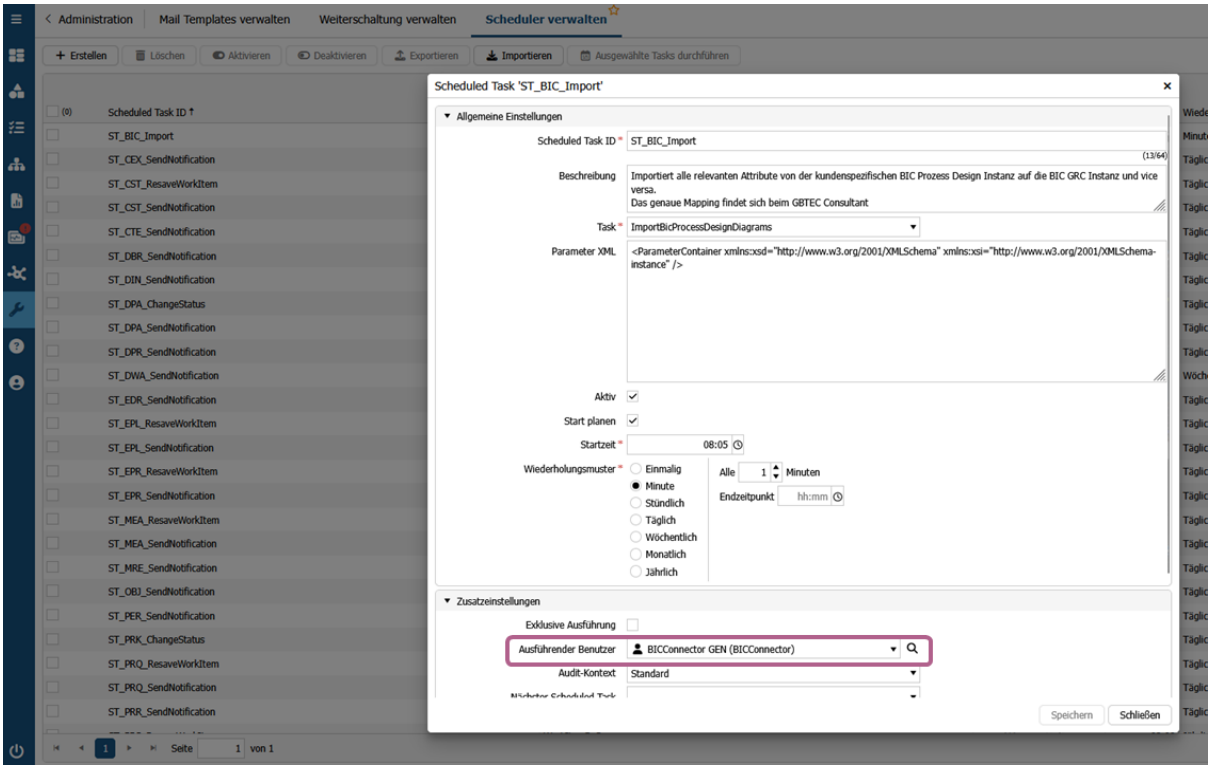
2.1.2.11 BIC Connector

Es wird empfohlen einen eigenen Benutzer "BIC Connector" anzulegen, wenn Prozesse und Work Items aus BIC Process Design übernommen werden.

Dafür muss diesem Benutzer nur die Gruppe "sys.BICConnector" zugeordnet werden.

Der Grund für diese Empfehlung ist folgende: Wenn über die Schnittstelle zwischen BIC Process Design und BIC GRC Work Items wie beispielsweise *Prozessrisiko* oder *Kontrolle* importiert werden, wird in den erstellten Work Items ein Ersteller angezeigt. Dieser Ersteller würde mit der Empfehlung "BIC Connector" ausgefüllt werden, sodass später für Dritte leichter zu erkennen ist, dass die Work Items nicht manuell erstellt wurden, sondern mittels einer Schnittstelle importiert wurden.

Des weiteren wird empfohlen, den Benutzer "BIC Connector" unter Administration >> Automation >> Scheduler verwalten >> ST_BIC_Import >> Ausführender Benutzer einzutragen.



2.1.3 Benutzerprofile in Enterprise Risk

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Enterprise Risk?

In BIC Enterprise Risk erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Erstellung und Freigabe von ERM Top-Down Assessments, sowie der Freigabe und Überprüfung der Eingaben des Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Unternehmensrisiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Erstellung und Dokumentation von Simulations Use Cases, Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit / Häufigkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Enterprise Risk gibt es standardmäßig nur zwei erweiterte Benutzerprofile. Ein weiteres erweitertes Benutzerprofil kommt durch den Zukauf des Simulations-Modules hinzu.

Assessor

Der Assessor ist für das bewerten eines oder mehrerer "ERM Top- Down"- Assessments verantwortlich. Er evaluiert mittels einer Ersteinschätzung ob zu bestimmten Risikokategorien an seinem Asset (Business Unit) ein potenzielles Risiko besteht oder nicht.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Simulationsanalyst

Der Simulationsanalyst kann bei den freigeschaltenen Modulen Enterprise Risk mit Simulation den Bearbeiter Risiko während seiner Bewertung eines Unternehmensrisikos unterstützen und bei entsprechender Konfiguration das Unternehmensrisiko gesondert freigeben.

Read Only

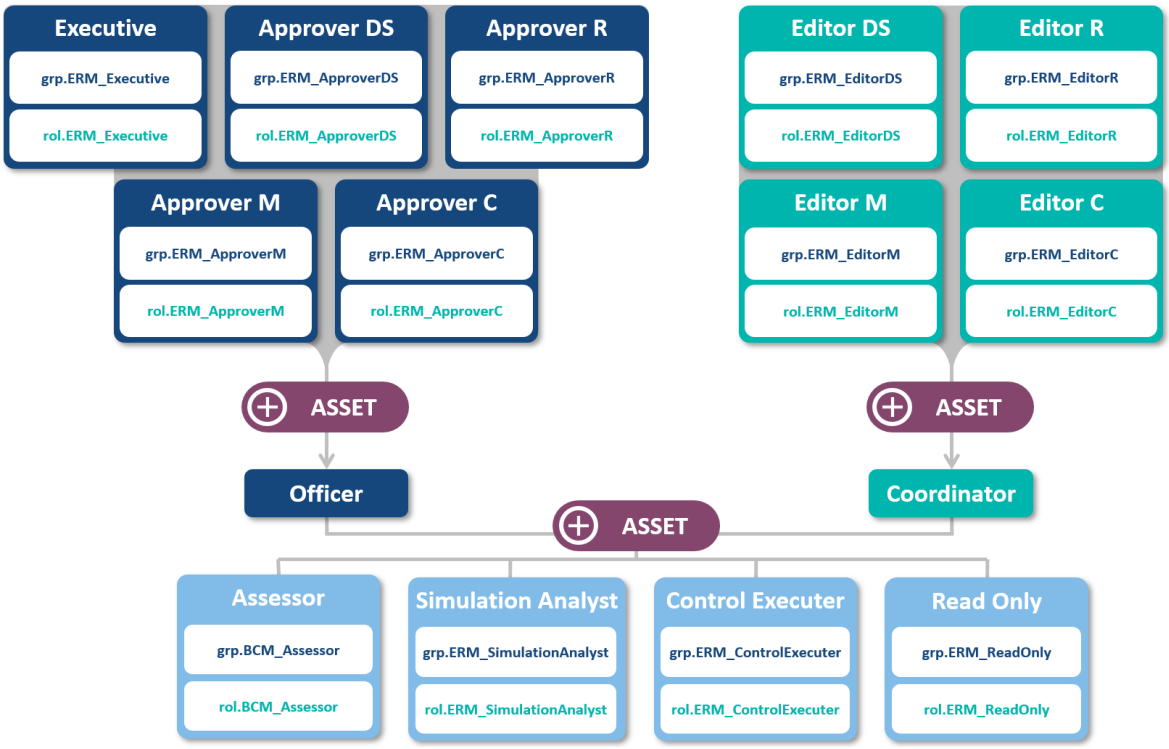
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.4 Mehrstufige Rollenstruktur in BIC Enterprise Risk

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.4.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_Executive	• rol.ERM_Executive
• grp.ERM_ApproverDS	• rol.ERM_ApproverDS
• grp.ERM_ApproverR	• rol.ERM_ApproverR
• grp.ERM_ApproverM	• rol.ERM_ApproverM
• grp.ERM_ApproverC	• rol.ERM_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_EditorDS	• rol.ERM_EditorDS
• grp.ERM_EditorR	• rol.ERM_EditorR
• grp.ERM_EditorM	• rol.ERM_EditorM
• grp.ERM_EditorC	• rol.ERM_EditorC

2.1.4.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur

Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_Executive	• rol.StandardUser • rol.ERM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

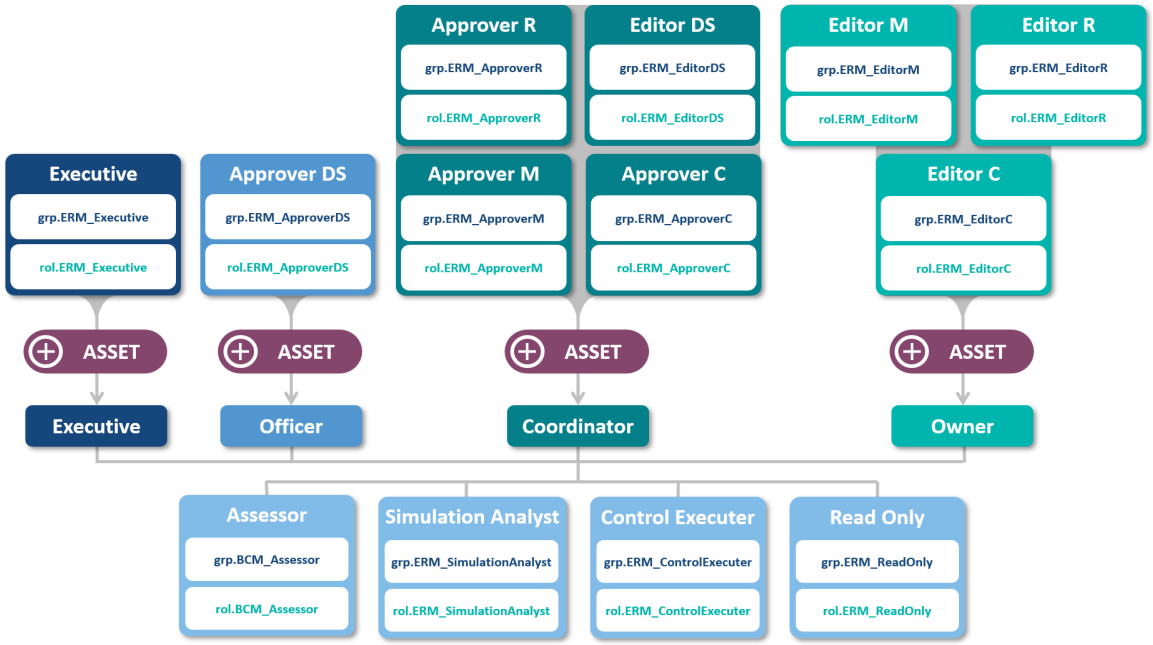
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_ApproverDS • grp.ERM_ApproverR • grp.ERM_ApproverM • grp.ERM_ApproverC	• rol.StandardUser • rol.ERM_ApproverDS • rol.ERM_ApproverR • rol.ERM_ApprovM • rol.ERM_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_EditorDS	• rol.ERM_EditorDS
• grp.ERM_EditorR	• rol.ERM_EditorR
• grp.ERM_EditorM	• rol.ERM_EditorM
• grp.ERM_EditorC	• rol.ERM_EditorC

2.1.4.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_Executive	• rol.ERM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_ApproverDS	• rol.ERM_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_ApproverR	• rol.ERM_ApproverR
• grp.ERM_ApproverM	• rol.ERM_ApproverM
• grp.ERM_ApproverC	• rol.ERM_ApproverC
• grp.ERM_EditorDS	• rol.ERM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ERM_EditorR	• rol.ERM_EditorR
• grp.ERM_EditorM	• rol.ERM_EditorM
• grp.ERM_EditorC	• rol.ERM_EditorC

2.1.4.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Assessor

Beschreibung: Fachliche Verantwortung für die Durchfühung unternehmenseinheit- bezogener Assessments

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_Assessor	• rol.StandardUser • rol.ERM_Assessor

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_ControlExecuter	• rol.StandardUser • rol.ERM_ControlExecuter

Simulationsanalyst

Beschreibung: Fachlicher Verantwortlicher für Risiken mit Simulation

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_SimulationAnalyst	• rol.StandardUser • rol.ERM_SimulationAnalyst

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ERM_ReadOnly	• rol.StandardUser • rol.ERM_ReadOnly

> Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.5 Benutzerprofile in Information Security

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Information Security?

In BIC Information Security erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Security-Risiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Bearbeitung und Dokumentation von Vorfällen, Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Information Security gibt es mehrere erweiterte Benutzerprofile.

Assessor

Ein Assessor ist ein Benutzer, der die Aufgabe hat an seinem Asset Assessments nach

- BSI IT-Grundschutz
- Generische Risiken - ISO 27002
- ISO 27001
- NIS-2 Audit View und
- Elementare Gefährdungen - Anforderungen IT Grundschutz

durchzuführen und gegebenenfalls Security-Risiken und Maßnahmen zu erstellen.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Read Only

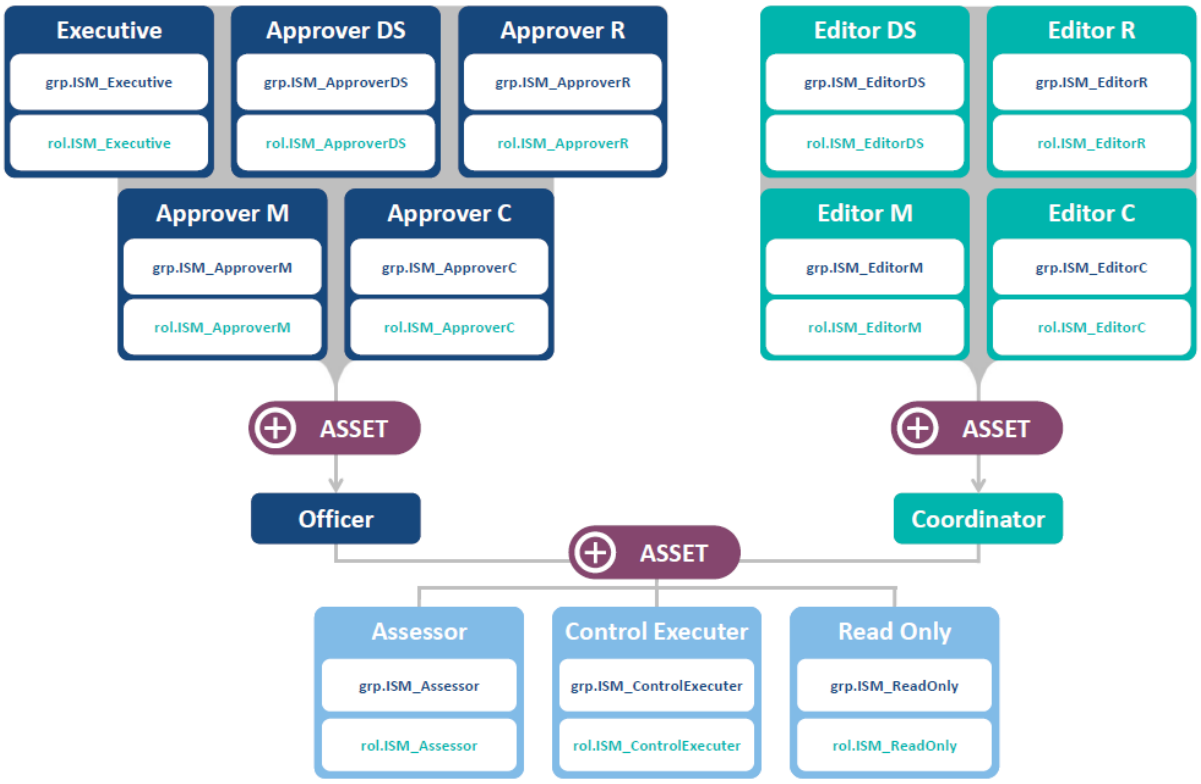
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.6 Mehrstufige Rollenstruktur in BIC Information Security

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.6.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

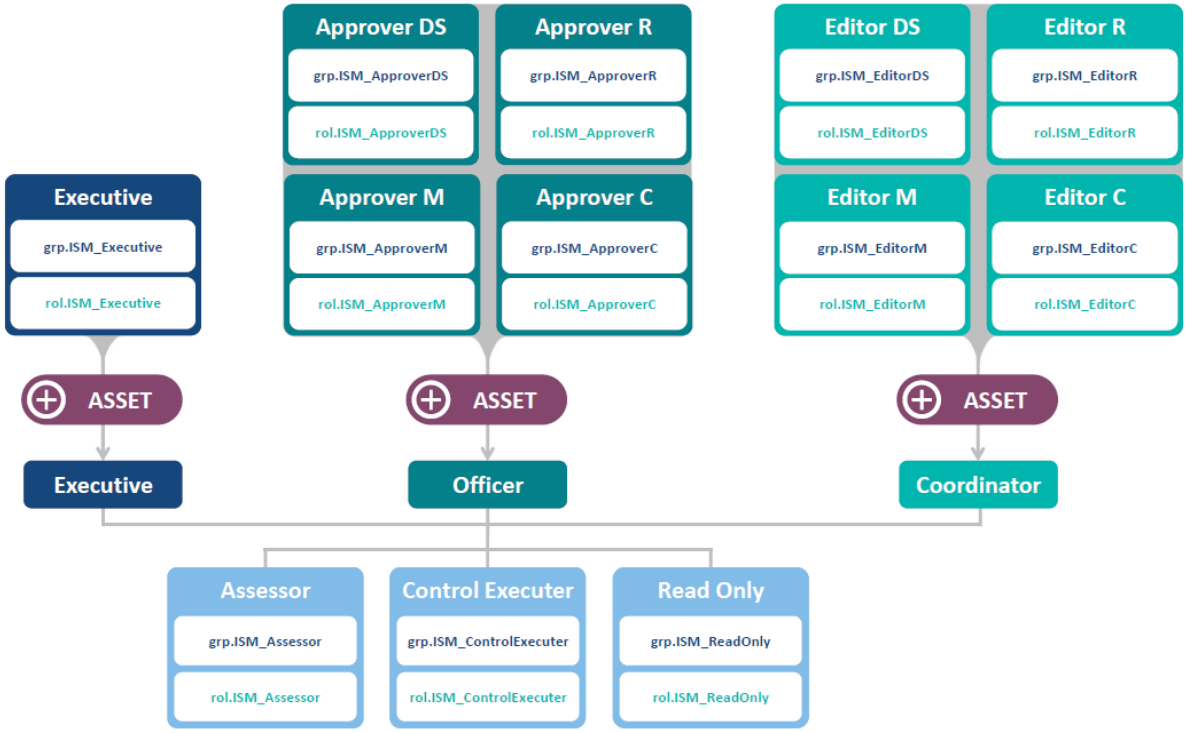
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_Executive	• rol.ISM_Executive
• grp.ISM_ApproverDS	• rol.ISM_ApproverDS
• grp.ISM_ApproverR	• rol.ISM_ApproverR
• grp.ISM_ApproverM	• rol.ISM_ApproverM
• grp.ISM_ApproverC	• rol.ISM_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_EditorDS	• rol.ISM_EditorDS
• grp.ISM_EditorR	• rol.ISM_EditorR
• grp.ISM_EditorM	• rol.ISM_EditorM
• grp.ISM_EditorC	• rol.ISM_EditorC

2.1.6.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_Executive	• rol.ISM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

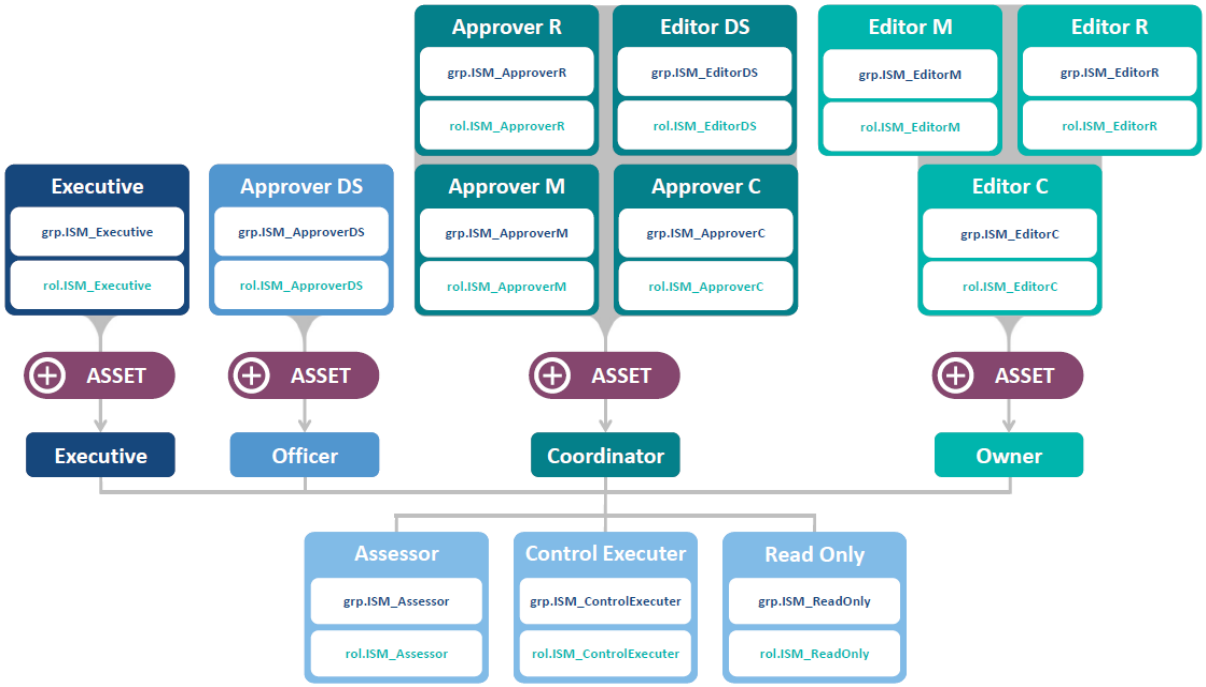
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_ApproverDS	• rol.ISM_ApproverDS
• grp.ISM_ApproverR	• rol.ISM_ApproverR
• grp.ISM_ApproverM	• rol.ISM_ApprovM
• grp.ISM_ApproverC	• rol.ISM_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_EditorDS	• rol.ISM_EditorDS
• grp.ISM_EditorR	• rol.ISM_EditorR
• grp.ISM_EditorM	• rol.ISM_EditorM
• grp.ISM_EditorC	• rol.ISM_EditorC

2.1.6.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_Executive	• rol.ISM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_ApproverDS	• rol.ISM_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_ApproverR	• rol.ISM_ApproverR
• grp.ISM_ApproverM	• rol.ISM_ApproverM
• grp.ISM_ApproverC	• rol.ISM_ApproverC
• grp.ISM_EditorDS	• rol.ISM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_EditorR	• rol.ISM_EditorR
• grp.ISM_EditorM	• rol.ISM_EditorM
• grp.ISM_EditorC	• rol.ISM_EditorC

2.1.6.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Assessor

Beschreibung: Fachlicher Verantwortlicher für Bewertung an einem Asset

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_Assessor	• rol.ISM_Assessor

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_ControlExecuter	• rol.ISM_ControlExecuter

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ISM_ReadOnly	• rol.ISM_ReadOnly

> Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.7 Benutzerprofile in BIC Business Continuity

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Business Continuity?

In BIC Business Continuity erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS und dem Prepardness Coordinator verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Security-Risiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Bearbeitung und Dokumentation von Vorfällen, Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden.

Assessor

Ein Assessor ist ein Benutzer, der die Aufgabe hat an seinem Asset Assessments nach BSI Business Continuity 200-4 IIA durchzuführen und gegebenenfalls Security-Risiken und Maßnahmen zu erstellen.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Vorsorgekoordinator / Prepardness Coordinator

Der Vorsorgekoordinator (Prepardness Coordinator) ist eine zentrale Rolle innerhalb der Domäne Business Continuity Management (BCM) in BIC GRC. Er trägt maßgeblich dazu bei, die organisatorische Resilienz zu sichern und eine strukturierte Notfallvorsorge aufzubauen. Zu seinen wesentlichen Aufgaben zählen unter anderem die Planung, Koordination und Durchführung von Notfallübungen, die regelmäßige Aktualisierung von Notfallplänen sowie die Pflege kritischer Informationen zur Betriebsfortführung.

Read Only

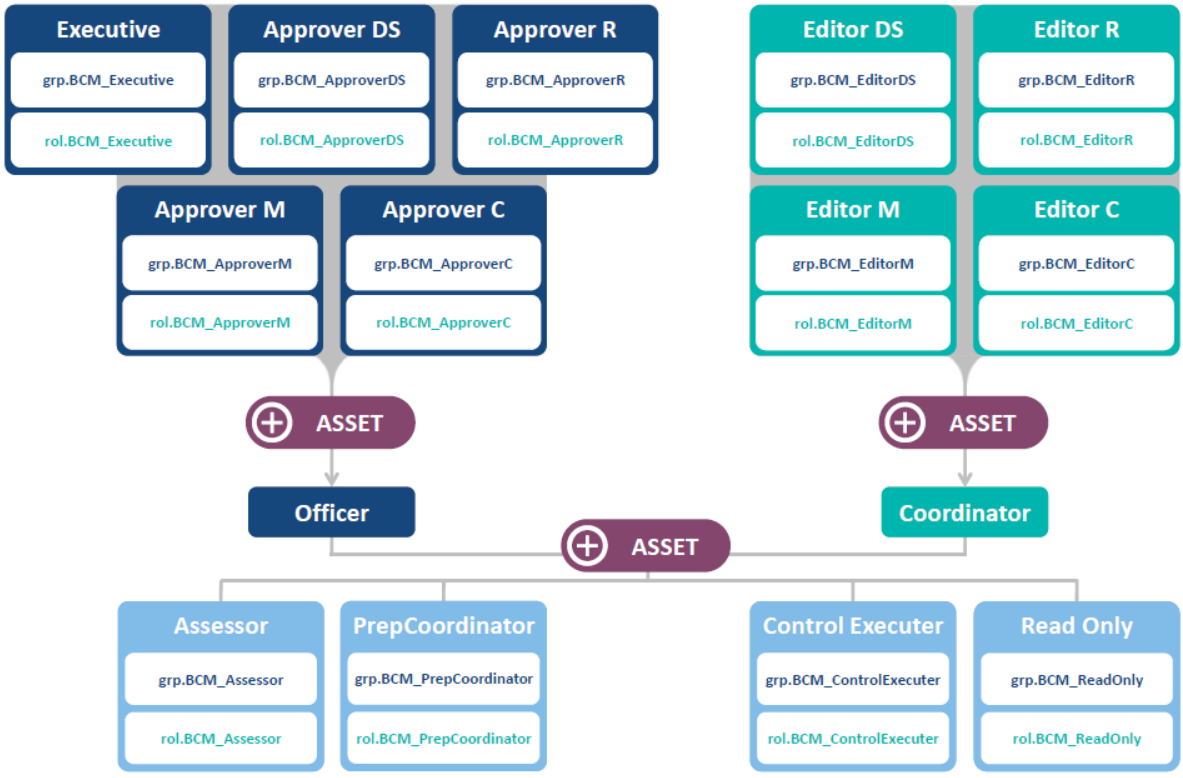
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.8 Mehrstufige Rollenstruktur in BIC Business Continuity

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.8.1 Zuweisung von Benutzerprofilen bei zweistuf



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

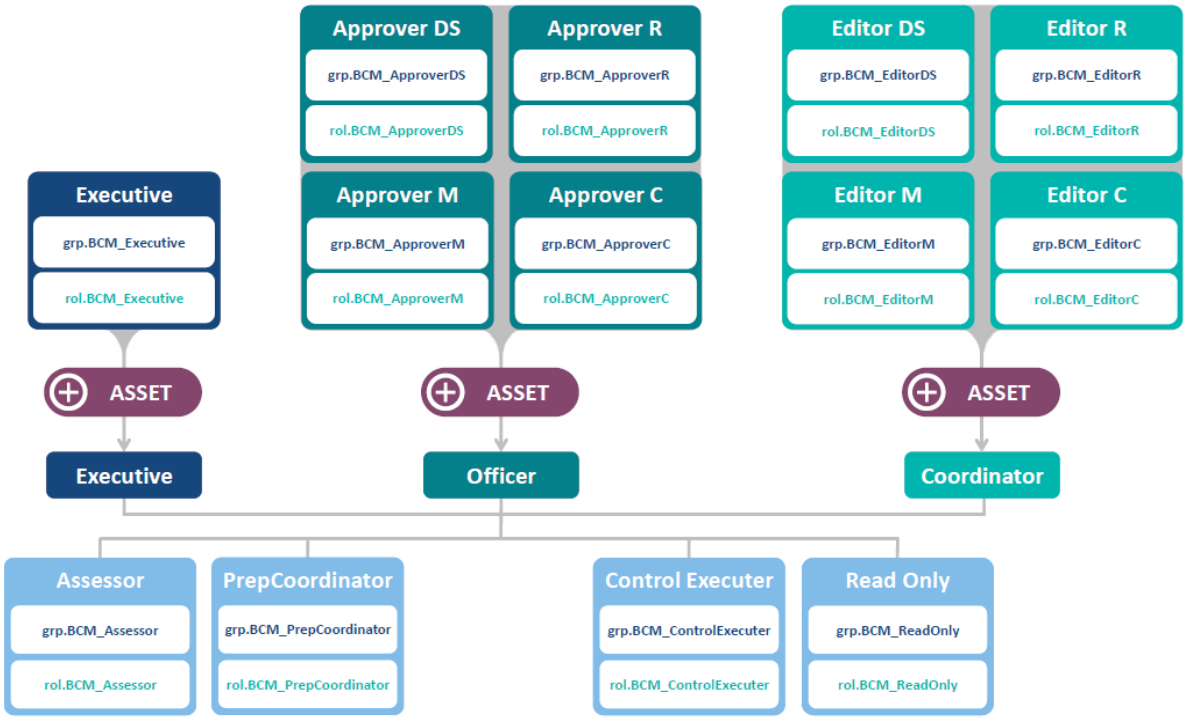
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_Executive	• rol.BCM_Executive
• grp.BCM_ApproverDS	• rol.BCM_ApproverDS
• grp.BCM_ApproverR	• rol.BCM_ApproverR
• grp.BCM_ApproverM	• rol.BCM_ApproverM
• grp.BCM_ApproverC	• rol.BCM_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_EditorDS	• rol.BCM_EditorDS
• grp.BCM_EditorR	• rol.BCM_EditorR
• grp.BCM_EditorM	• rol.BCM_EditorM
• grp.BCM_EditorC	• rol.BCM_EditorC

2.1.8.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_Executive	• rol.BCM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

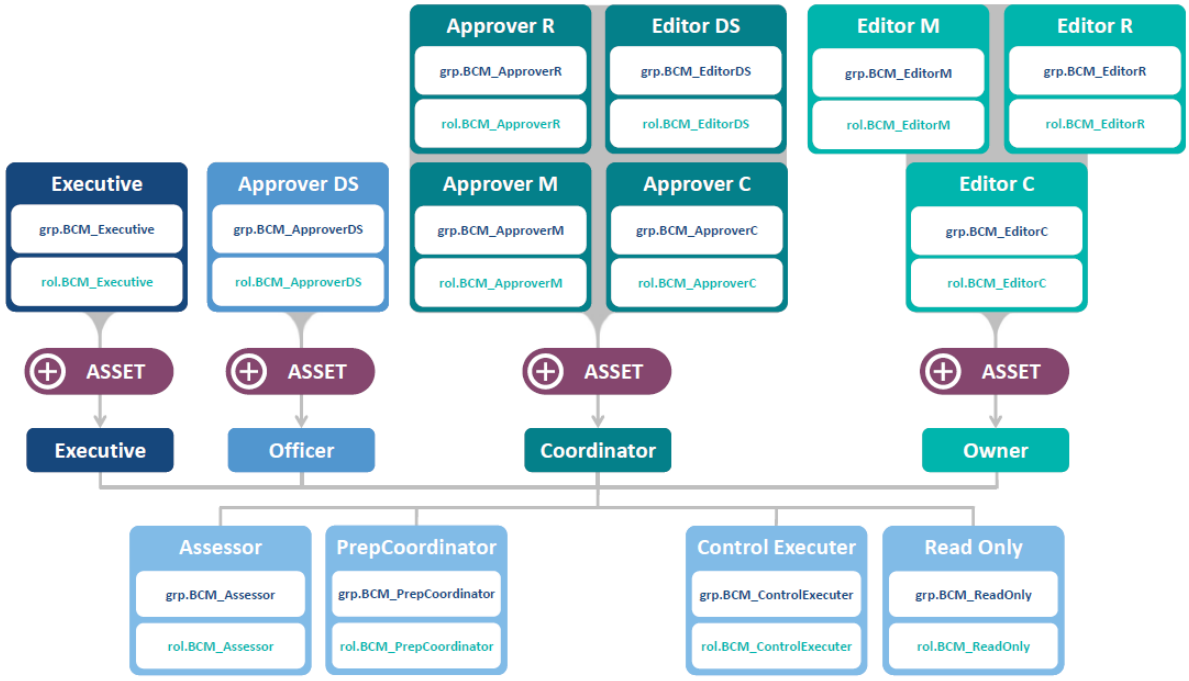
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_ApproverDS	• rol.BCM_ApproverDS
• grp.BCM_ApproverR	• rol.BCM_ApproverR
• grp.BCM_ApproverM	• rol.BCM_ApprovM
• grp.BCM_ApproverC	• rol.BCM_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_EditorDS	• rol.BCM_EditorDS
• grp.BCM_EditorR	• rol.BCM_EditorR
• grp.BCM_EditorM	• rol.BCM_EditorM
• grp.BCM_EditorC	• rol.BCM_EditorC

2.1.8.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.BCM_Executive	• rol.StandardUser • rol.BCM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.BCM_ApproverDS	• rol.StandardUser • rol.BCM_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.BCM_ApproverR • grp.BCM_ApproverM • grp.BCM_ApproverC • grp.BCM_EditorDS	• rol.StandardUser • rol.BCM_ApproverR • rol.BCM_ApproverM • rol.BCM_ApproverC • rol.BCM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_EditorR	• rol.BCM_EditorR
• grp.BCM_EditorM	• rol.BCM_EditorM
• grp.BCM_EditorC	• rol.BCM_EditorC

2.1.8.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Preparedness Coordinator

Beschreibung: Fachlicher Experte für den Bereich Business Coninuity

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_PreparednessCoordinator	• rol.BCM_PreparednessCoordinator

Assessor

Beschreibung: Fachlicher Verantwortlicher für Bewertung an einem Asset

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_Assessor	• rol.BCM_Assessor

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_ControlExecuter	• rol.BCM_ControlExecuter

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.BCM_ReadOnly	• rol.BCM_ReadOnly

> Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.9 Benutzerprofile in Internal Control

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Internal Control?

In BIC Internal Control erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Unternehmensrisiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit/Häufigkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Internal Control gibt es zwei erweiterte Benutzerprofile.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Read Only

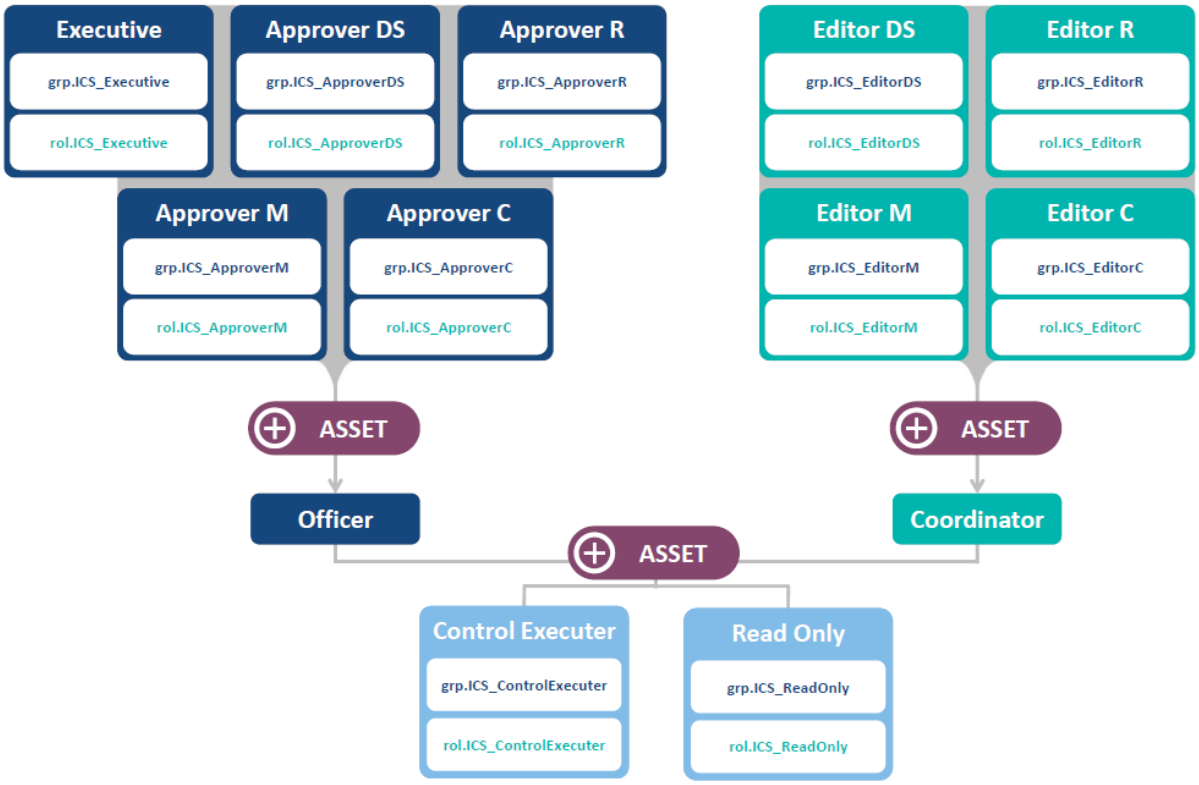
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.10 Mehrstufige Rollenstruktur in BIC Internal Control

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.10.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

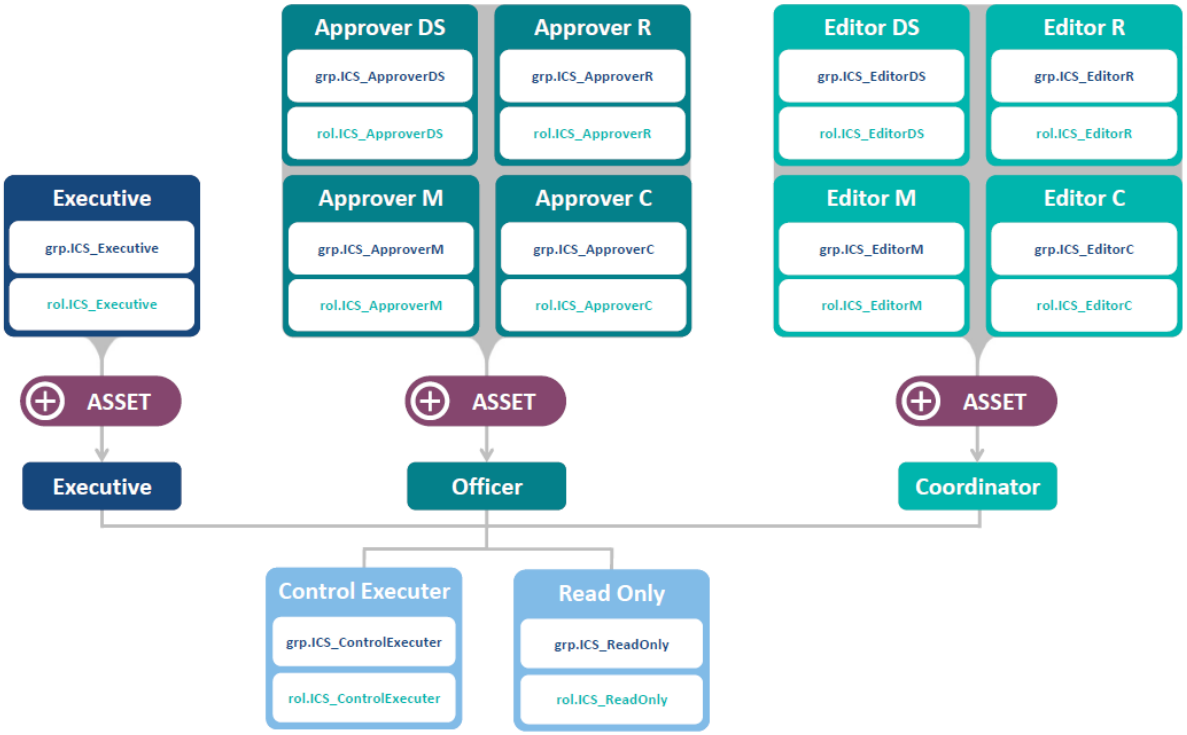
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_Executive	• rol.ICS_Executive
• grp.ICS_ApproverDS	• rol.ICS_ApproverDS
• grp.ICS_ApproverR	• rol.ICS_ApproverR
• grp.ICS_ApproverM	• rol.ICS_ApproverM
• grp.ICS_ApproverC	• rol.ICS_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_EditorDS	• rol.ICS_EditorDS
• grp.ICS_EditorR	• rol.ICS_EditorR
• grp.ICS_EditorM	• rol.ICS_EditorM
• grp.ICS_EditorC	• rol.ICS_EditorC

2.1.10.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ICS_Executive	• rol.StandardUser • rol.ICS_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

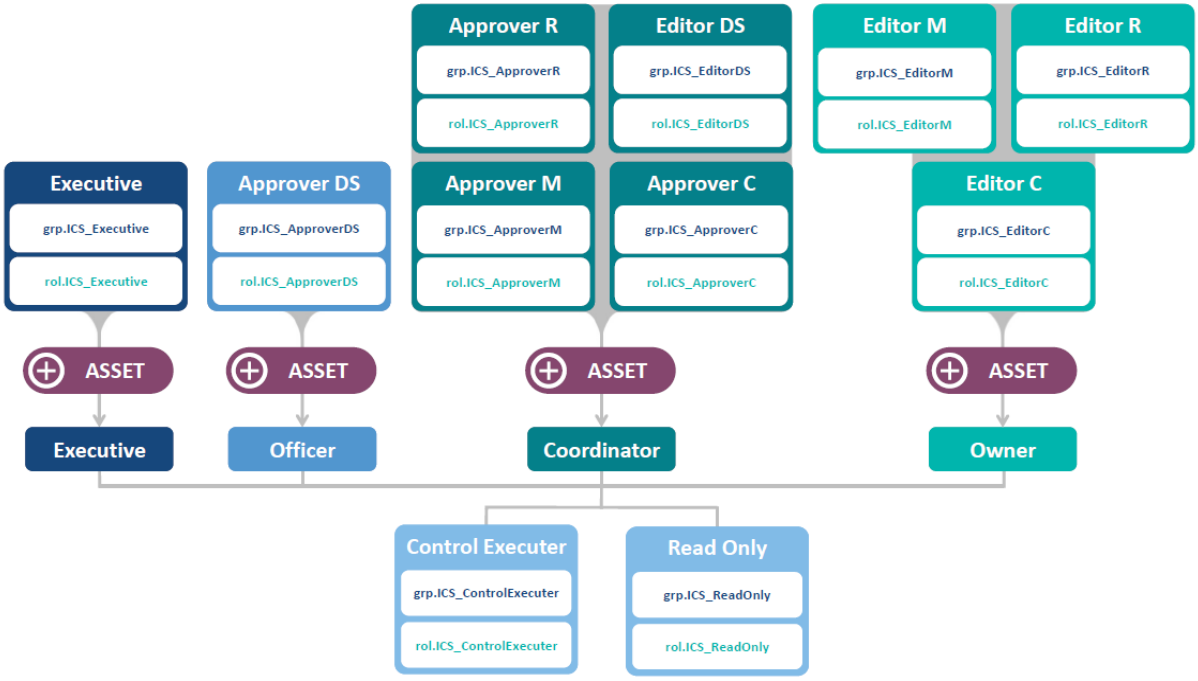
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.ICS_ApproverDS • grp.ICS_ApproverR • grp.ICS_ApproverM • grp.ICS_ApproverC	• rol.StandardUser • rol.ICS_ApproverDS • rol.ICS_ApproverR • rol.ICS_ApproverM • rol.ICS_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_EditorDS	• rol.ICS_EditorDS
• grp.ICS_EditorR	• rol.ICS_EditorR
• grp.ICS_EditorM	• rol.ICS_EditorM
• grp.ICS_EditorC	• rol.ICS_EditorC

2.1.10.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_Executive	• rol.ICS_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_ApproverDS	• rol.ICS_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_ApproverR	• rol.ICS_ApproverR
• grp.ICS_ApproverM	• rol.ICS_ApproverM
• grp.ICS_ApproverC	• rol.ICS_ApproverC
• grp.ICS_EditorDS	• rol.ICS_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_EditorR	• rol.ICS_EditorR
• grp.ICS_EditorM	• rol.ICS_EditorM
• grp.ICS_EditorC	• rol.ICS_EditorC

2.1.10.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_ControlExecuter	• rol.ICS_ControlExecuter

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.ICS_ReadOnly	• rol.ICS_ReadOnly

Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.11 Benutzerprofile in Data Protection

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Data Protection?

In BIC Data Protection erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Security-Risiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Data Protection gibt es mehrere erweiterte Benutzerprofile.

Assessor

Ein Assessor ist ein Benutzer, der die Aufgabe hat an seinem Asset ein Assessment nach ISO 27701 durchzuführen und gegebenenfalls Security-Risiken und Maßnahmen zu erstellen.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Read Only

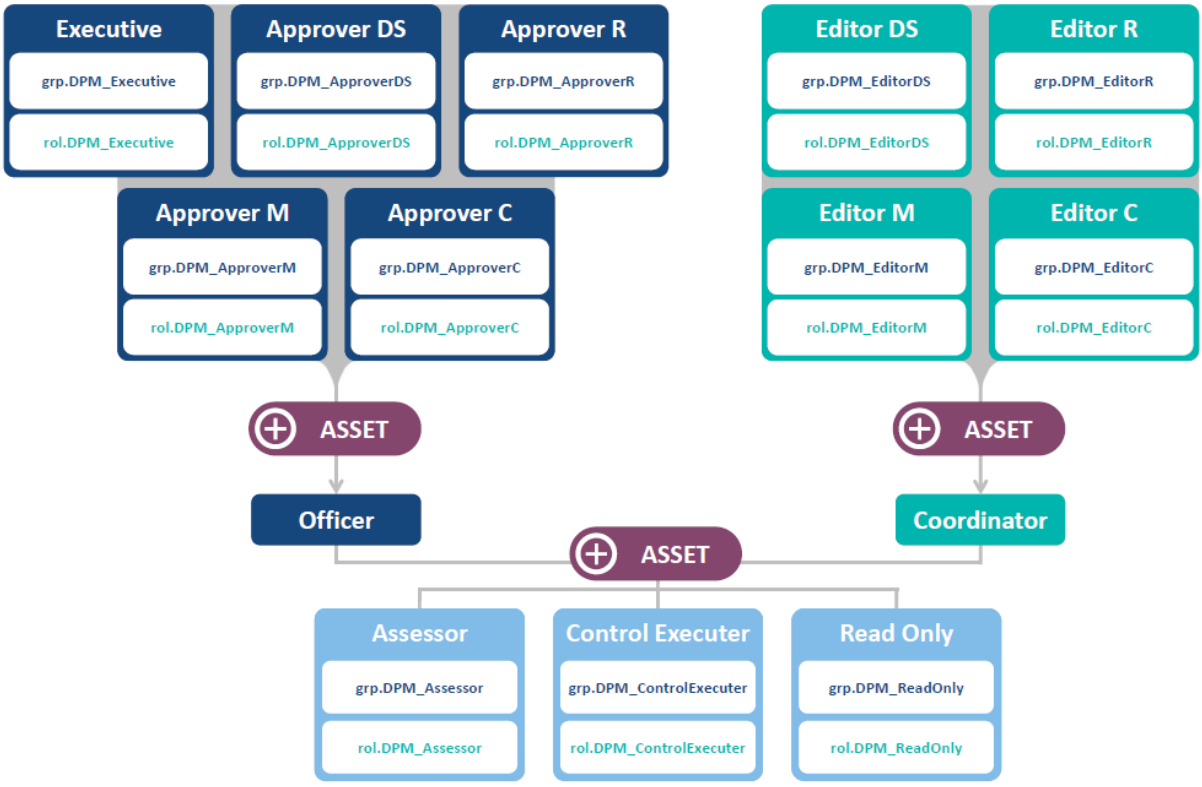
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.12 Mehrstufige Rollenstruktur in BIC Data Protection

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.12.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

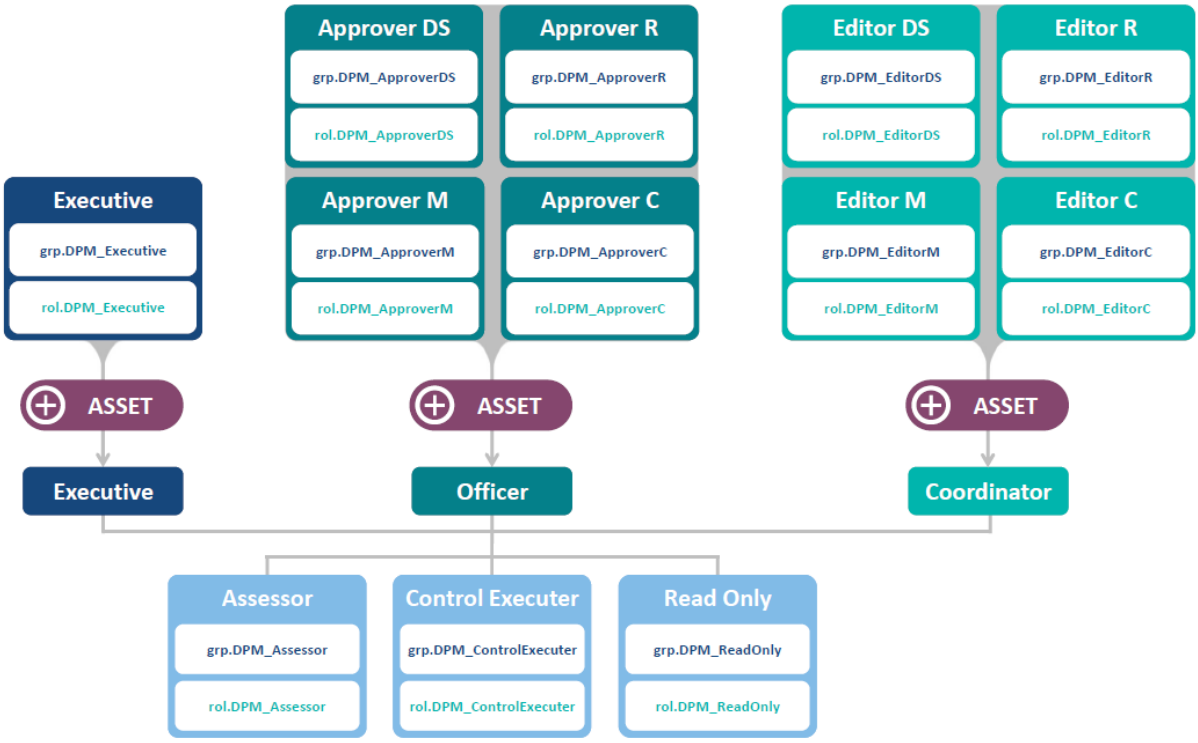
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_Executive	• rol.DPM_Executive
• grp.DPM_ApproverDS	• rol.DPM_ApproverDS
• grp.DPM_ApproverR	• rol.DPM_ApproverR
• grp.DPM_ApproverM	• rol.DPM_ApproverM
• grp.DPM_ApproverC	• rol.DPM_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_EditorDS	• rol.DPM_EditorDS
• grp.DPM_EditorR	• rol.DPM_EditorR
• grp.DPM_EditorM	• rol.DPM_EditorM
• grp.DPM_EditorC	• rol.DPM_EditorC

2.1.12.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.DPM_Executive	• rol.StandardUser • rol.DPM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

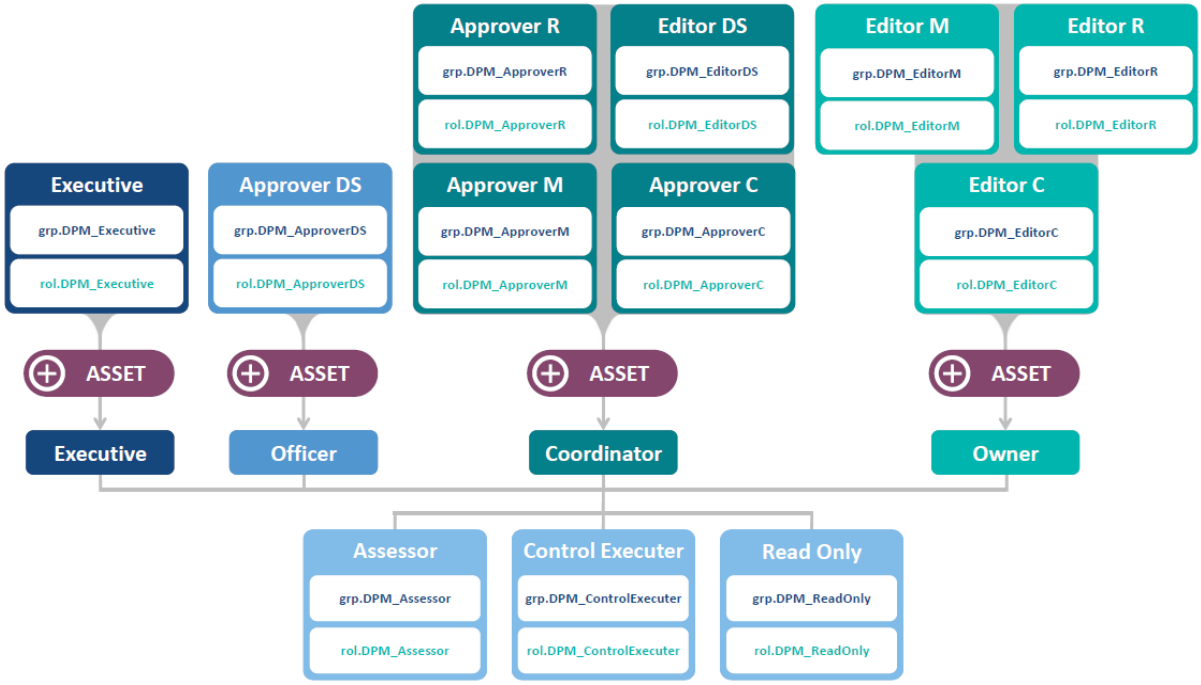
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.DPM_ApproverDS • grp.DPM_ApproverR • grp.DPM_ApproverM • grp.DPM_ApproverC	• rol.StandardUser • rol.DPM_ApproverDS • rol.DPM_ApproverR • rol.DPM_ApprovM • rol.DPM_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_EditorDS	• rol.DPM_EditorDS
• grp.DPM_EditorR	• rol.DPM_EditorR
• grp.DPM_EditorM	• rol.DPM_EditorM
• grp.DPM_EditorC	• rol.DPM_EditorC

2.1.12.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_Executive	• rol.DPM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_ApproverDS	• rol.DPM_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_ApproverR	• rol.DPM_ApproverR
• grp.DPM_ApproverM	• rol.DPM_ApproverM
• grp.DPM_ApproverC	• rol.DPM_ApproverC
• grp.DPM_EditorDS	• rol.DPM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_EditorR	• rol.DPM_EditorR
• grp.DPM_EditorM	• rol.DPM_EditorM
• grp.DPM_EditorC	• rol.DPM_EditorC

2.1.12.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Assessor

Beschreibung: Fachlicher Verantwortlicher für Bewertung an einem Asset

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_Assessor	• rol.DPM_Assessor

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_ControlExecuter	• rol.DPM_ControlExecuter

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.DPM_ReadOnly	• rol.DPM_ReadOnly

> Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.13 Benutzerprofile in Corporate Sustainability

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Corporate Sustainability?

In BIC Corporate Sustainability erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Risiko / Approver Risk (R)

Der Freigeber "Risiko" ist für die Freigabe von Unternehmensrisiken verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Freigeber Kontrolle / Approver Control (C)

Der Freigeber "Kontrolle" ist für die Freigabe von Kontrolle verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch / Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Bewertung von finanziellen und nicht-finanziellen Auswirkungen, Erstellung und Dokumentation von Management Reviews, ...) die nicht in dem Kontext von Risiken, Maßnahmen oder Kontrollen bzw. in den Aufgabenbereich von domänenunabhängigen Benutzerprofilen wie "Dokumenteneigner" fallen.

Bearbeiter Risiko / Editor Risk (R)

In BIC GRC ist der Bearbeiter "Risiko" in erster Linie für die Erstellung, Bewertung und Behandlung eines Risikos verantwortlich. Er besitzt die Kompetenz, ein Risiko anhand seiner Eintrittswahrscheinlichkeit/Häufigkeit und seines monetären Schadenpotenzials vom ursprünglichen Zustand bis zum Zielwert einzuschätzen.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Bearbeiter Kontrolle / Editor Control (C)

Der Bearbeiter "Kontrolle" ist in BIC GRC für mindestens eine Kontrolle verantwortlich. Er kann durch andere Benutzer oder durch eigene Erstellung für eine Kontrolle verantwortlich werden.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Corporate Sustainability gibt es mehrere erweiterte Benutzerprofile.

Assessor

Ein Assessor ist ein Benutzer, der die Aufgabe hat an seinem Asset Assessments nach ESRS 1 - AR16 durchzuführen und gegebenenfalls Finanzielle Wesentlichkeiten oder Auswirkungswesentlichkeiten zu erstellen.

Kontolldurchführer / Control Executer

Der Kontrolldurchführer ist für die Durchführung einer Kontrolle eines spezifischen Assets verantwortlich. Die Aufgabe des Kontrolldurchführers in BIC GRC ist die Bestätigung der Durchführung und bei Bedarf die Hinterlegung zugehöriger Dokumente.

Simulationsanalyst

Der Simulationsanalyst kann bei den freigeschaltenen Modulen Corporate Sustainability mit Simulation den Bearbeiter Risiko während seiner Bewertung eines Unternehmensrisikos unterstützen und bei Bedarf das Unternehmensrisiko gesondert freigeben.

Read Only

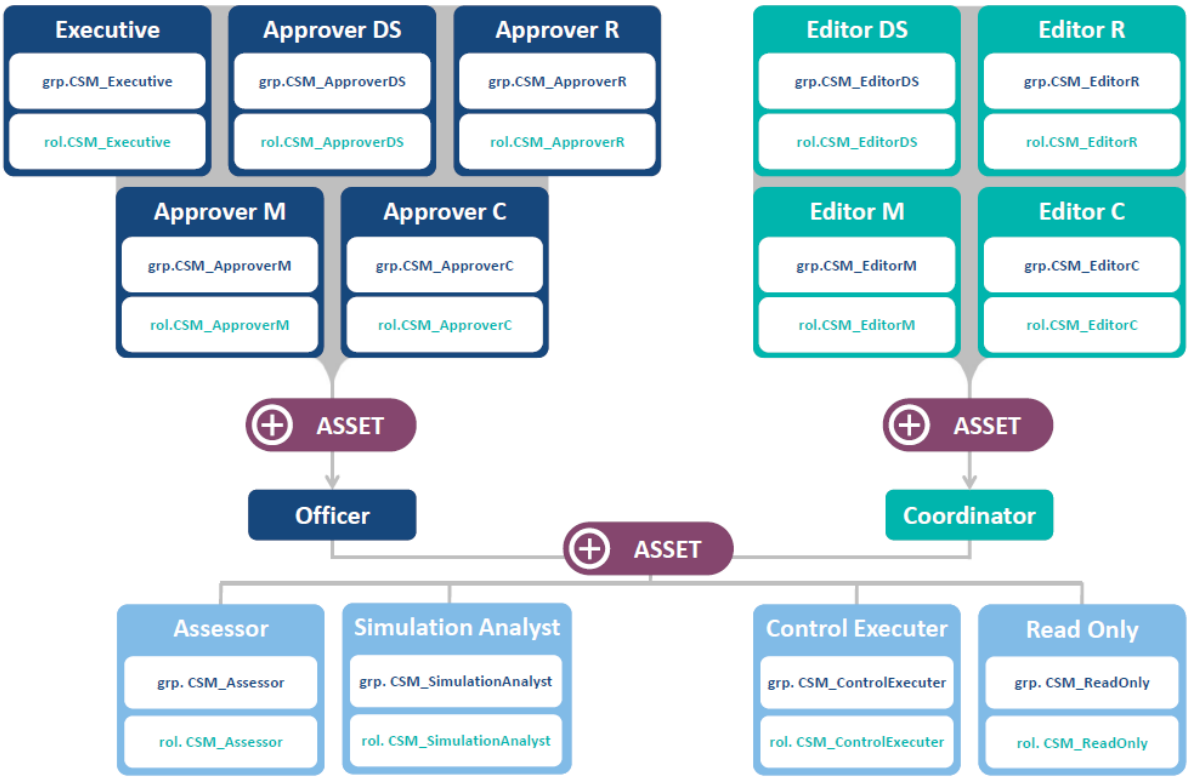
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.14 Mehrstufige Rollenstruktur in BIC Corporate Sustainability

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Officer", "Coordinator" und "Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.14.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Officer

Beschreibung: Freigabe von Risiken, strategische Risikoentscheidungen, Eskalation

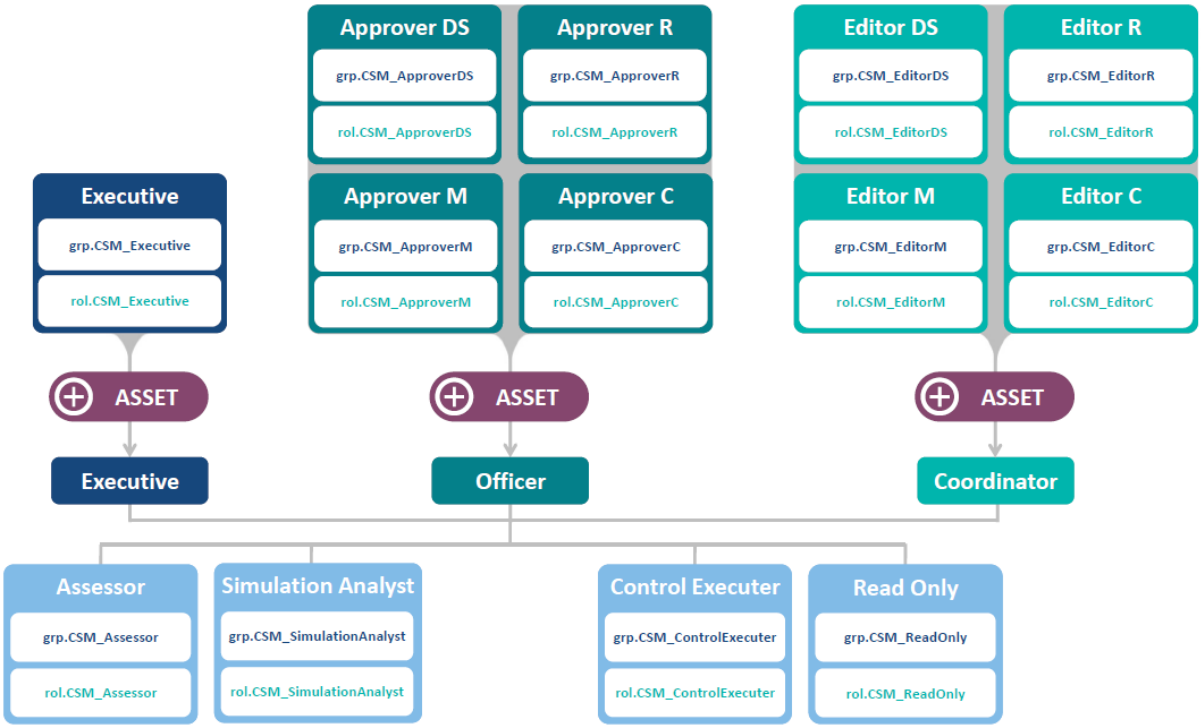
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_Executive	• rol.CSM_Executive
• grp.CSM_ApproverDS	• rol.CSM_ApproverDS
• grp.CSM_ApproverR	• rol.CSM_ApproverR
• grp.CSM_ApproverM	• rol.CSM_ApproverM
• grp.CSM_ApproverC	• rol.CSM_ApproverC

Koordinator

Beschreibung: Risikoerfassung, Risikobewertung, Pflege von Maßnahmen und Status

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_EditorDS	• rol.CSM_EditorDS
• grp.CSM_EditorR	• rol.CSM_EditorR
• grp.CSM_EditorM	• rol.CSM_EditorM
• grp.CSM_EditorC	• rol.CSM_EditorC

2.1.14.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.CSM_Executive	• rol.StandardUser • rol.CSM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

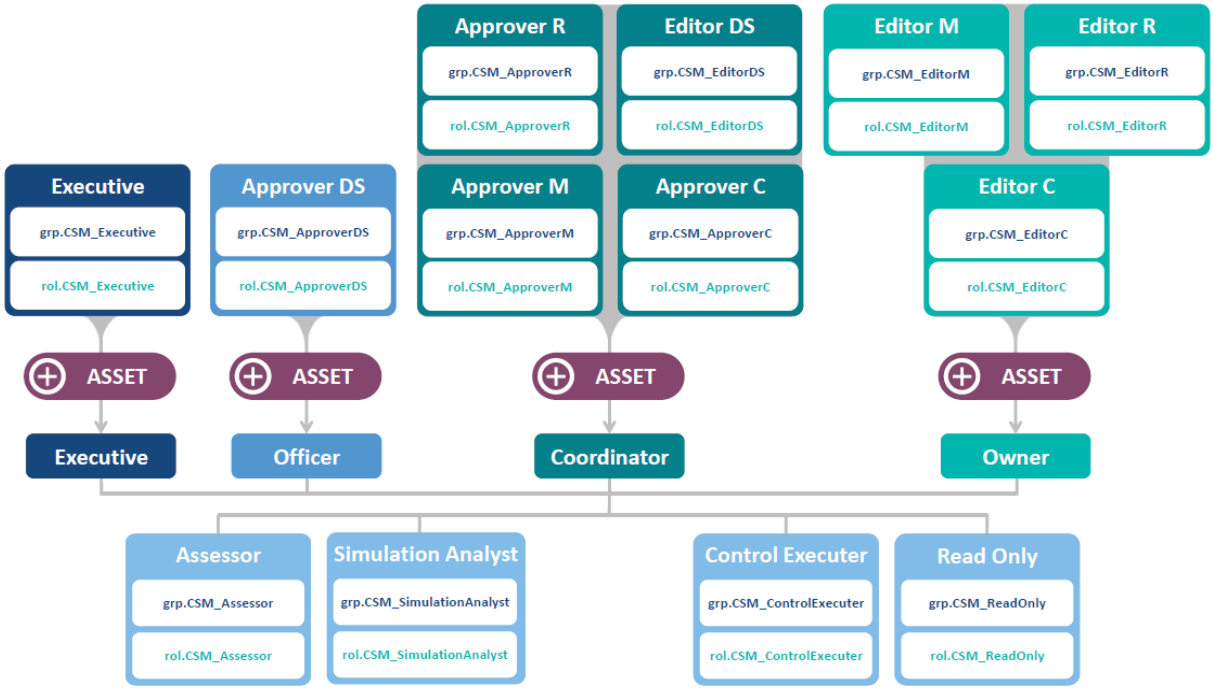
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.CSM_ApproverDS • grp.CSM_ApproverR • grp.CSM_ApproverM • grp.CSM_ApproverC	• rol.StandardUser • rol.CSM_ApproverDS • rol.CSM_ApproverR • rol.CSM_ApprovM • rol.CSM_ApproverC

Koordinator

Beschreibung: Operative Bearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_EditorDS	• rol.CSM_EditorDS
• grp.CSM_EditorR	• rol.CSM_EditorR
• grp.CSM_EditorM	• rol.CSM_EditorM
• grp.CSM_EditorC	• rol.CSM_EditorC

2.1.14.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_Executive	• rol.CSM_Executive

Officer

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_ApproverDS	• rol.CSM_ApproverDS

Koordinator

Beschreibung: Operative Fachbearbeitung innerhalb einer Domäne

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_ApproverR	• rol.CSM_ApproverR
• grp.CSM_ApproverM	• rol.CSM_ApproverM
• grp.CSM_ApproverC	• rol.CSM_ApproverC
• grp.CSM_EditorDS	• rol.CSM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_EditorR	• rol.CSM_EditorR
• grp.CSM_EditorM	• rol.CSM_EditorM
• grp.CSM_EditorC	• rol.CSM_EditorC

2.1.14.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Assessor

Beschreibung: Fachlicher Verantwortlicher für Bewertung an einem Asset

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_Assessor	• rol.CSM_Assessor

Control Executer

Beschreibung: Fachliche Verantwortung für die Durchfühung domänenspezifischer Kontrollen

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_ControlExecuter	• rol.CSM_ControlExecuter

Simulationsanalyst

Beschreibung: Fachlicher Verantwortlicher für Risiken mit Simulation

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_SimulationAnalyst	• rol.CSM_SimulationAnalyst

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.CSM_ReadOnly	• rol.CSM_ReadOnly

> Ergänzend zu den bisher genannten Benutzerprofilen in diesem Modul können auch die Benutzerprofile aus dem Modul Audit "Bearbeiter Audit" und "Freigeber Audit" vergeben werden, falls Audits durchgeführt werden. Mehr dazu unter Benutzerprofile in Internal Audit.

2.1.15 Benutzerprofile in Internal Audit

Da Gruppen- und Rollennamen in BIC GRC nur in einer einzigen, neutralen Sprache gepflegt werden können, wurden die englischen Bezeichnungen übernommen.

> Approver sind in BIC GRC "Freigeber" und Editoren sind "Bearbeiter".

Was machen die einzelnen Benutzerprofile in BIC Internal Audit?

In BIC Internal Audit erfüllen die einzelnen Benutzerprofile unterschiedliche Aufgaben und Verantwortlichkeiten.

Jedes Profil legt fest, welche Funktionen im System genutzt werden können und welche Inhalte sichtbar oder bearbeitbar sind.

Executive

Personen mit dem Benutzerprofil Executive bzw. Manager sind Benutzer, die Teil des Management-Boards der Organisation sind. Dieser hat weitgehende Rechte in BIC GRC, um auf Basis der eingegeben Daten und Informationen im System Entscheidungen für unterschiedliche Bereiche treffen zu können. Dabei übernimmt er keine operativen Aufgaben.

Freigeber Domänenspezifisch / Approver Domain Specific (DS)

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich sowie für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

Er ist in erster Linie für die Freigabe und Überprüfung der Eingaben von Editor DS verantwortlich.

Zudem hat er die Berechtigungen, um alle Work Items zu erstellen, die auch der Editor DS erstellen kann, um gegebenenfalls einen Workflow zu beginnen, auch wenn er keine operative Rolle einnimmt.

Freigeber Maßnahme / Approver Measure (M)

Der Freigeber "Maßnahme" ist für die Freigabe von Maßnahmen verantwortlich, wenn sie seiner Organisationseinheit und explizit seiner Verantwortung unterliegen.

Bearbeiter Domänenspezifisch /Editor Domain Specific (DS)

Ein Bearbeiter "Domänenspezifisch" ist ein Benutzer, der für eine bestimmte Domäne alle Aufgaben übernimmt (Erstellung, Dokumentation, ...) die nicht in den Kontext von Maßnahmen fallen. Für Maßnahmen gibt es eigene Bearbeiter.

Bearbeiter Maßnahme / Editor Measure (M)

Der Bearbeiter "Maßnahme" ist für die Erstellung und Umsetzung einer oder mehrerer spezifischen Maßnahme(n) im Unternehmen verantwortlich. Seine Aufgabe besteht in der Erfassung, Planung, Umsetzung und Dokumentation des stetigen Fortschritts der Maßnahme in BIC GRC.

Was machen erweiterte Benutzerprofile?

Erweiterte Benutzerprofile können individuell und ergänzend Benutzern zugewiesen werden. Für das Modul BIC Internal Audit gibt es nur ein erweitertes Benutzerprofil.

Read Only

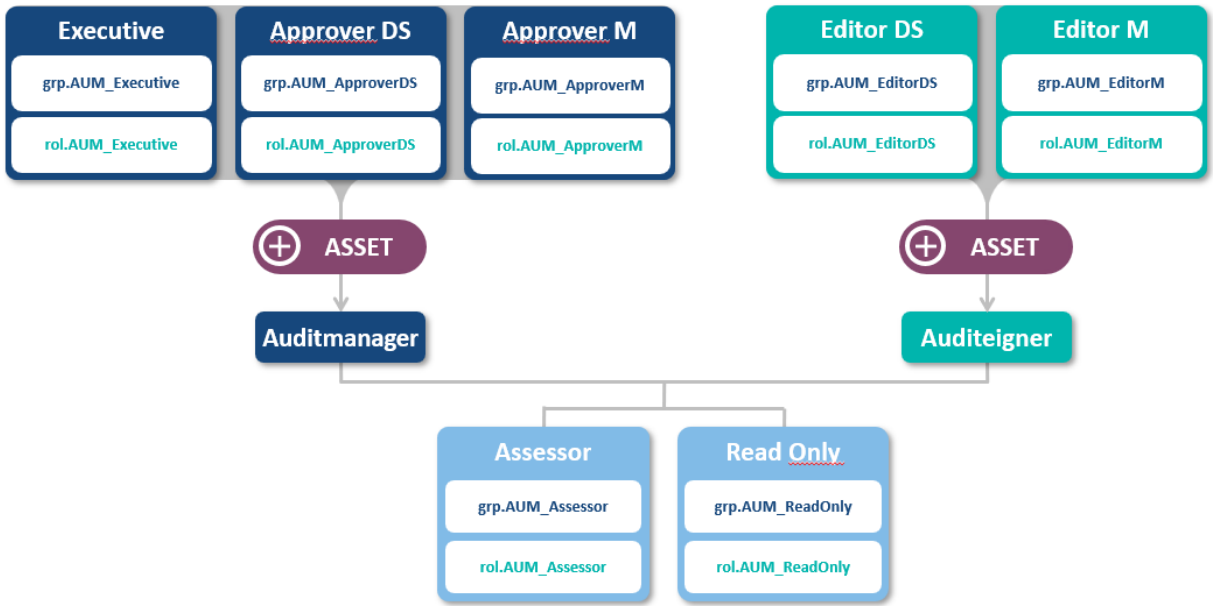
Read Only Benutzer können alle Work Items an einem ihnen zugewiesenen Asset sehen die zu dem Modul bestehen.

2.1.16 Mehrstufige Rollenstruktur in BIC Internal Audit

In BIC GRC können abhängig von der Größe des Unternehmens unterschiedliche Rollenstrukturen angewendet werden. Die Bezeichnungen "Executive", "Auditmanager", "Auditeigner" und "Measure Owner" sind keine in BIC Integrated GRC vorkommenden Gruppen oder Rollen Bezeichnungen, sondern dienen dazu das Benutzerkonzept besser zu vermitteln.

In Organisationen mit einer Rollenstruktur erfolgt die Zuweisung von Benutzerprofilen in BIC GRC entlang fachlich und domänenspezifisch differenzierter Verantwortlichkeiten. Die Rollen sind in sogenannte Teil- Profile gegliedert, die je nach Funktionsebene (strategisch, freigebend, koordinierend oder verantwortend) und Fachdomäne vergeben werden. So wird sichergestellt, dass jede Person nur auf die Inhalte zugreifen kann, die für ihre Aufgaben relevant sind.

2.1.16.1 Zuweisung von Benutzerprofilen bei zweistufiger Rollenstruktur



Auditmanager

Beschreibung: Freigabe von Audits und Maßnahmen, strategische Planung

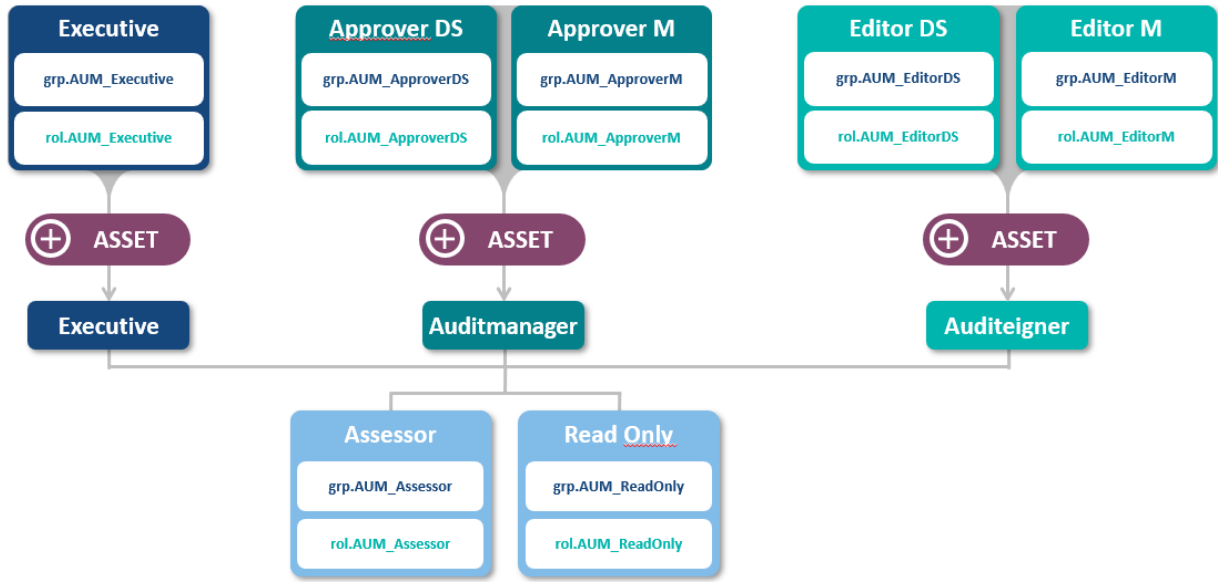
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser	• rol.StandardUser
• grp.AUM_Executive	• rol.AUM_Executive
• grp.AUM_ApproverDS	• rol.AUM_ApproverDS
• grp.AUM_ApproverM	• rol.AUM_ApproverM

Auditeigner

Beschreibung: Führt Audits operativ durch, dokumentiert Feststellungen und erstellt Berichtsentwürfe.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_EditorDS • grp.AUM_EditorM	• rol.StandardUser • rol.AUM_EditorDS • rol.AUM_EditorM

2.1.16.2 Zuweisung von Benutzerprofilen bei dreistufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_Executive	• rol.StandardUser • rol.AUM_Executive

Auditmanager

Beschreibung: Domänenspezifische Steuerung und Freigabe

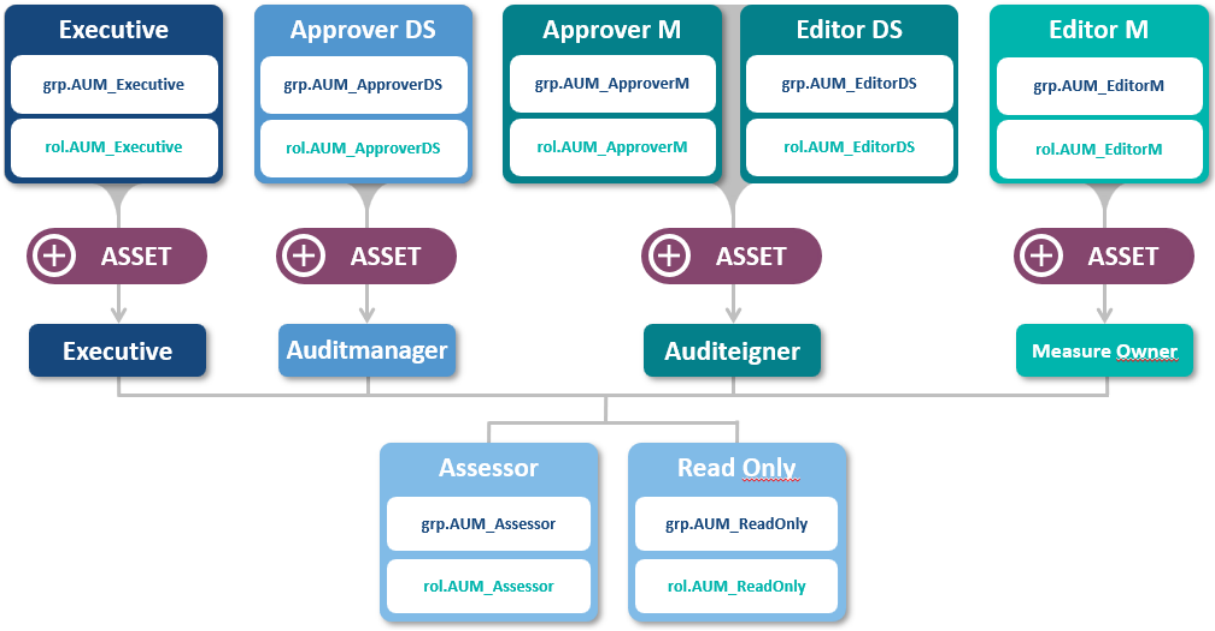
Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_ApproverDS • grp.AUM_ApproverM	• rol.StandardUser • rol.AUM_ApproverDS • rol.AUM_ApproverM

Auditeigner

Beschreibung: Führt Audits operativ durch, dokumentiert Feststellungen und erstellt Berichtsentwürfe.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_EditorDS • grp.AUM_EditorM	• rol.StandardUser • rol.AUM_EditorDS • rol.AUM_EditorM

2.1.16.3 Zuweisung von Benutzerprofilen bei vierstufiger Rollenstruktur



Executive

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_Executive	• rol.StandardUser • rol.AUM_Executive

Auditmanager

Beschreibung: Domänenspezifische Steuerung und Freigabe

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_ApproverDS	• rol.StandardUser • rol.AUM_ApproverDS

Auditeigner

Beschreibung: Führt Audits operativ durch, dokumentiert Feststellungen und erstellt Berichtsentwürfe.

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_ApproverM • grp.AUM_EditorDS	• rol.StandardUser • rol.AUM_ApproverM • rol.AUM_EditorDS

Owner

Beschreibung: Fachlich Verantwortliche/r für die Umsetzung einer Maßnahme

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_EditorM	• rol.StandardUser • rol.AUM_EditorM

2.1.16.4 Zusätzliche Benutzerprofile

Nach demselben Prinzip wie die zuvor beschriebenen Benutzerprofile können auch erweiterten Benutzerprofile für eine Domäne einzelnen Benutzern zugewiesen werden.

Assessor

Beschreibung: Fachlicher Verantwortlicher für Bewertung an einem Asset

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_Assessor	• rol.StandardUser • rol.AUM_Assessor

Read Only

Beschreibung: Übergreifende Sicht, keine Bearbeitung

Schritt 1: Gruppenzuordnung	Schritt 2: Rollen- + Assetzuordnung
• grp.StandardUser • grp.AUM_ReadOnly	• rol.StandardUser • rol.AUM_ReadOnly

Disclaimer