BIC Corporate Sustainability - User Manual

BIC Integrated GRC 2026 Summer

Dokument Version: Juni 2026

Inhaltsverzeichnis

1 Für wen ist dieses User Manual?

Dieses User Manual richtet sich an Benutzer von BIC Integrated GRC. Es soll unterstützen, sich in BIC GRC zurechtzufinden, sowie spezifische Aufgaben im Tool zu kennen und auszuführen.

1.1 Schreibweise

In diesem Handbuch wird folgende Schreibweise verwendet:

- Begriffe in doppelten Anführungszeichen: Alle Namen wie Dialogtitel, Tab- Titel, Menüoptionen, Feldnamen usw. werden mit doppelten Anführungszeichen gekennzeichnet. Beispiel: Klicken Sie auf "Erstellen".
- Begriffe in einfachen Anführungszeichen: Zum Kennzeichnen von speziellen Begriffen.
- Befehlspfade: Die Anweisung 'Wählen Sie **Architektur >> Dashboards >> Kacheln** bedeutet, dass Sie in der Sidebar die Option "Architektur", dann die Option "Dashboards" und dann "Kacheln" wählen müssen.
- Fette Schreibweise: Besonders wichtige Informationen werden **fett** hervorgehoben.
- Verweise: Verweise auf andere Kapitel oder andere Dokumente werden als Hyperlinks angezeigt.
- Geschlechtsneutrale Formulierung: Aus Gründen der einfacheren Lesbarkeit wird auf geschlechtsspezifische Bezeichnungen (z.B. "BearbeiterIn", "Administrator:in") verzichtet Entsprechende Begriffe gelten grundsätzlich für alle Geschlechter.
- Hintergründe: Bestimmte Textinhalte haben in BIC GRC eine Hintergrundfarbe, mit den folgenden Bedeutungen:

Allgemeine Informationen: Für den User zu beachten bei der Arbeit in BIC GRC

Wichtige Informationen: Für den User unbedingt zu beachten bei der Arbeit in BIC GRC

Zusätzliche Informationen: Für den User interessant zu wissen bei der Arbeit in BIC GRC

Fachliche Informationen und Beispiele

Warnung: Erklärungen für Fehlermeldungen oder spezifische Verhalten

1.2 Überblick Symbole

In BIC GRC gibt es eine Vielzahl Icons, die der User im Laufe seiner Arbeit in BIC Enterprise GRC wiederfinden wird. Im Folgenden findet sich eine Übersicht über alle gängigen und notwendigen Icons in BIC GRC.

Der Name eines Icons wird im System angezeigt, wenn man den Mauszeiger über das Symbol bewegt.

1.2.1 Allgemein

 Bearbeiten

 Graph anzeigen

 Filtern

 Listeneinstellungen

 Suchen

 Kein Wert

1.2.2 Dashboard

 In den Anzeigebereich scrollen

 Fixieren

 Detaillierte Liste aller Elemente anzeigen

 Loslösen

1.2.3 Work Item

 User suchen

 Informationen

 Erstellen

 Verlinken

 Info

 Erfolgreiche Simulation

 Hinweis

 Error

 Link - Attribute anzeigen

 Beschreibung

 Work Item Links - Aufklappen

 Weitere Optionen

2 BIC Corporate Sustainability - Work Item Typen

Im folgenden Kapitel werden die unterschiedlichen Benutzerprofile sowie deren zugehörige Aufgaben innerhalb von BIC GRC beschrieben. Die Benutzerprofile setzen sich aus Gruppen und Rollen zusammen, welche im Rahmen von BIC Solutions durch GBTEC bereits vordefiniert wurden.

Jedes Benutzerprofil wird kurz erläutert, anschließend folgen die jeweils zugehörigen Aufgaben.

> Bitte informieren Sie sich vorab bei Ihrem Technischen Administrator, welches Benutzerprofil Ihnen zugeordnet ist.

2.1 Standard User

Das Profil „Standard User“ stellt ein allgemeines Benutzerprofil dar, das jedem Nutzer standardmäßig zugewiesen werden sollte.

> Der Standard User kann auch als Basis-Profil angesehen werden.

Folgende Aufgaben kann der Standard User in BIC GRC übernehmen:

- Nachhaltigkeitsmeldung melden & erstellen
- Interne Anfrage definieren & erstellen
- Berechtigungsanfrage definieren & erstellen

2.1.1 Nachhaltigkeitsmeldung melden & erstellen

Sollte im Bereich Corporate Sustainability eine *Nachhaltigkeitsmeldung* notwendig sein, da einem Benutzer eine Ungereimtheit im Bereich Nachhaltigkeit aufgefallen ist, kann diese von jedem Benutzer erstellt und gemeldet werden.

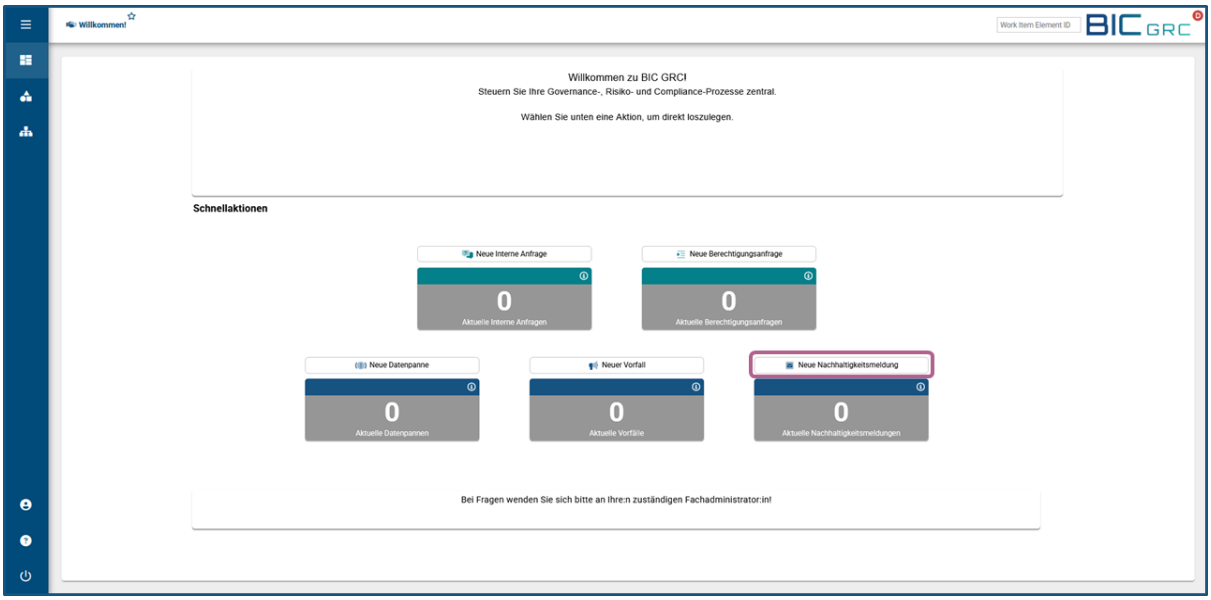
> Die Erstellung von Work Items des Typs *Nachhaltigkeitsmeldung* wird bei dem aktiven Modul "Corporate Sustainability" auch anderen aktiven Modulen ermöglicht. So können Benutzer aus allen Modulen bei Bedarf *Nachhaltigkeitsmeldungen* melden und nicht nur Benutzer aus dem Bereich "Corporate Sustainability".

Schritt 1: Nachhaltigkeitsmeldung erstellen

Der Standard User kann in BIC GRC an mehreren Stellen *Nachhaltigkeitsmeldungen* erstellen.

1. Erstellen über Dashboard

Der Benutzer navigiert über die Menüleiste zu **Dashboards >> Willkommen >> "Neue Nachhaltigkeitsmeldung"** .

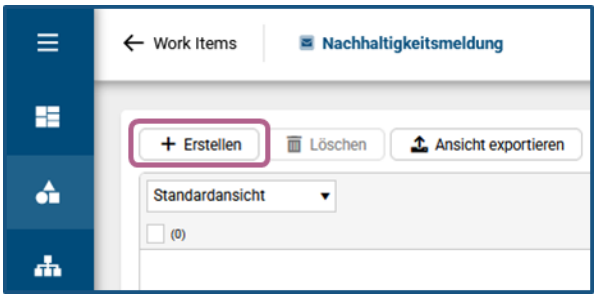


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Nachhaltigkeitsmeldung >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Nachhaltigkeitsmeldung* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht die *Nachhaltigkeitsmeldung* einzigartig.
2. **Entdeckt am**: Es ist anzugeben, wann der Umstand entdeckt worden ist.
3. **Beschreibung**: Die *Nachhaltigkeitsmeldung* sollte so ausführlich wie möglich dokumentiert werden, inklusive der Angabe aller beteiligten Personen.

   > So kann hier angegeben werden, ob das Thema schon länger vorliegt, wie es aufgefallen ist und welche Maßnahmen schon ergriffen worden sind.

4. **Geltungsbereich**: Mittels des Asset- Links kann der Geltungsbereich der *Nachhaltigkeitsmeldung* angegeben werden. Dabei erlaubt ein Filter nur die Auswahl von "Organisationseinheiten".

Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer kein Asset auf der Rolle "rol.StandardUser" zugewiesen. Mittels des Work Items *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

5 **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen kann die *Nachhaltigkeitsmeldung* erstmalig gespeichert werden

Beim Speichervorgang wird der Ersteller automatisch als "Verantwortlicher" eingetragen.

Schritt 3: Details ergänzen

1 **Verantwortlichkeiten**: Der Benutzer der die *Nachhaltigkeitsmeldung* gemeldet hat wird automatisch in das Attribut "Gemeldet von" geschrieben und kann auch nicht mehr geändert werden. Der "Freigeber" für die *Nachhaltigkeitsmeldung* kann mittels des Icons gesucht und hinterlegt werden.

Durch einen hinterlegten Filter muss der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

2 **Priorität**: Der Benutzer kann eine Priorität hinterlegen, anhand der festgemacht werden kann, wie wichtig dieser *Nachhaltigkeitsmeldung* für das Unternehmen ist.

3 **Zuordnung der Nachhaltigkeitsmeldung**: Danach muss der Benutzer eine Zuordnung zu einem Überthema (Umwelt, Soziales oder Unternehmensführung - ESG) machen.

4 **Auswirkung**: Des weiteren muss der Benutzer angeben ob bei seiner *Nachhaltigkeitsmeldung* das Unternehmen auf die Umwelt wirkt oder sein Unternehmen von der Umwelt beeinflusst wird.

So wirkt eine CO2-Besteuerung auf das Unternehmen, während beispielsweise ein Fischereibetrieb Auswirkungen auf die Meere und somit Umwelt hat.

5 **Risikoarten nach Auswirkung**: Zudem kann der Benutzer freiwillig noch passende Risikoarten aus einem GRC Framework auswählen.

6 **Mögliche Auswirkungen**: Neben der "Beschreibung" sollte an dieser Stelle explizit auf die Auswirkungen die zu erwarten sind eingegangen werden.

7 **Verursacher**: Der Benutzer kann aus mehreren Kategorien an "Verursachern" wählen.

Ein Verusacher kann beispielsweise ein Lieferant sein der aufgrund aufgedeckter Kinderarbeit in seinem Betrieb nicht mehr den unternehmensinternen ESG-Richtlinien entspricht.

8 **Betroffene**: Der Benutzer kann aus mehreren Kategorien an "Verursachern" wählen.

> Betroffene können beispielsweise die eigenen Mitarbeiter sein, wenn ein wichtiger Lieferant aufgrund von Kinderarbeit nicht mehr liefern kann und somit die Produktion still steht.

> Abhängig von der Auswahl gehen sowohl bei den "Verursachern" als auch bei den "Betroffenen" zusätzliche Links zu "Abteilungen" (Asset) oder beispielsweise "Kunden" (GRC Frameworks) auf.

9 **Beweismittel**: Sollten Beweismittel für die *Nachhaltigkeitsmeldung* vorliegen, können diese optional dokumentiert und in der Dokumentenablage im Tab "*Meldung*" unter dem Abschnitt "Beweismittel" abgelegt werden. Diese Dokumente können dem "Freigeber" helfen, im nachgelagerten Workflow die richtigen Entschlüsse für die Bewertung zu ziehen.

> Handelt es sich um eine Datei kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend im Attributsfeld verlinkt.

10 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Gemeldet" durchgeführt.

2.1.2 Interne Anfrage definieren & erstellen

Jeder Benutzer in BIC GRC hat die Möglichkeit eine *Interne Anfrage* zu stellen.

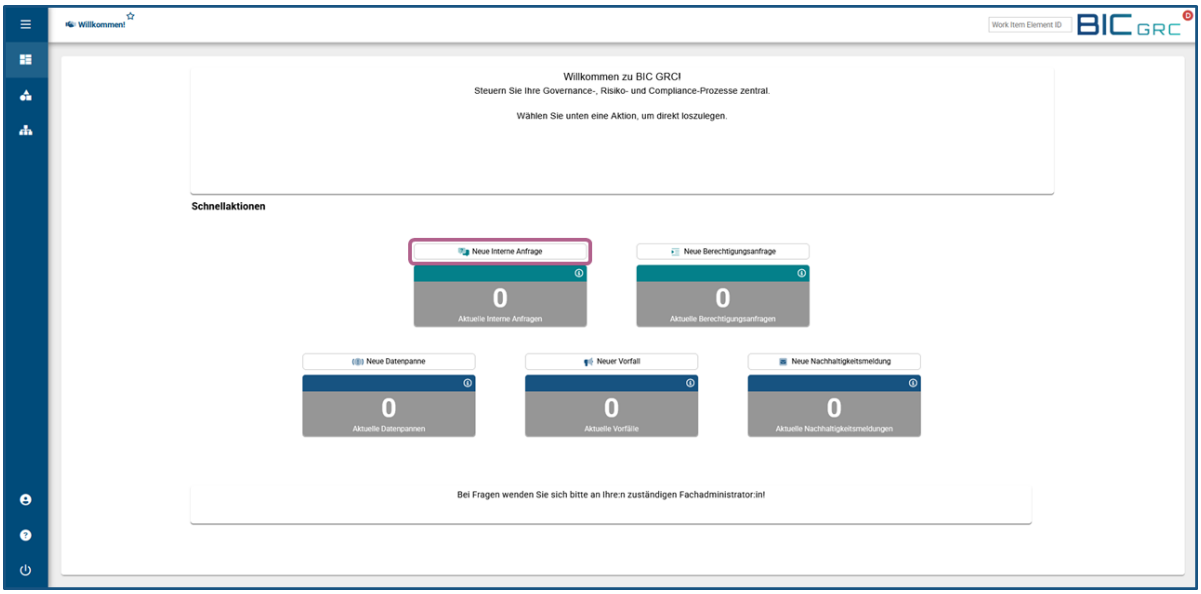
Diese Anfrage kann genutzt werden, um neue Profile oder einzelne Berechtigungen zu beantragen. Auch Anpassungen an bestehenden Profilen können angefragt werden.

Schritt 1: Interne Anfrage erstellen

Der Standard User kann in BIC GRC an mehreren Stellen *Interne Anfragen* erstellen.

1. Erstellen über Dashboard

Der Benutzer navigiert über die Menüleiste zu **Dashboards >> Willkommen >> "Neue Interne Anfrage"**.

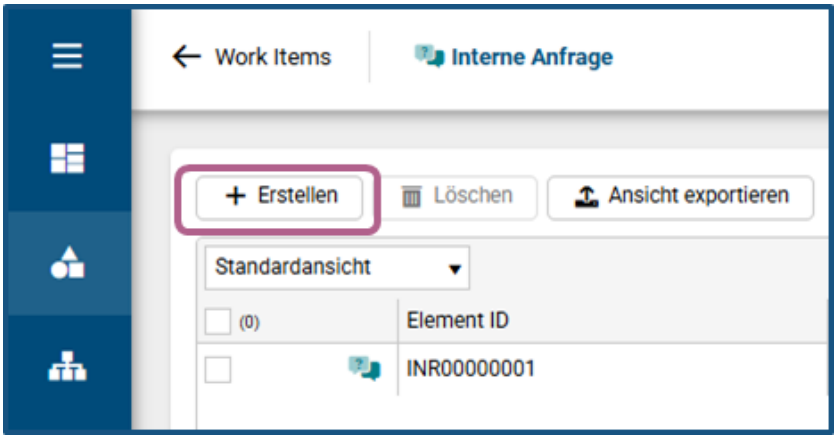


Ein neues Fenster öffnet sich anschließend automatisch.

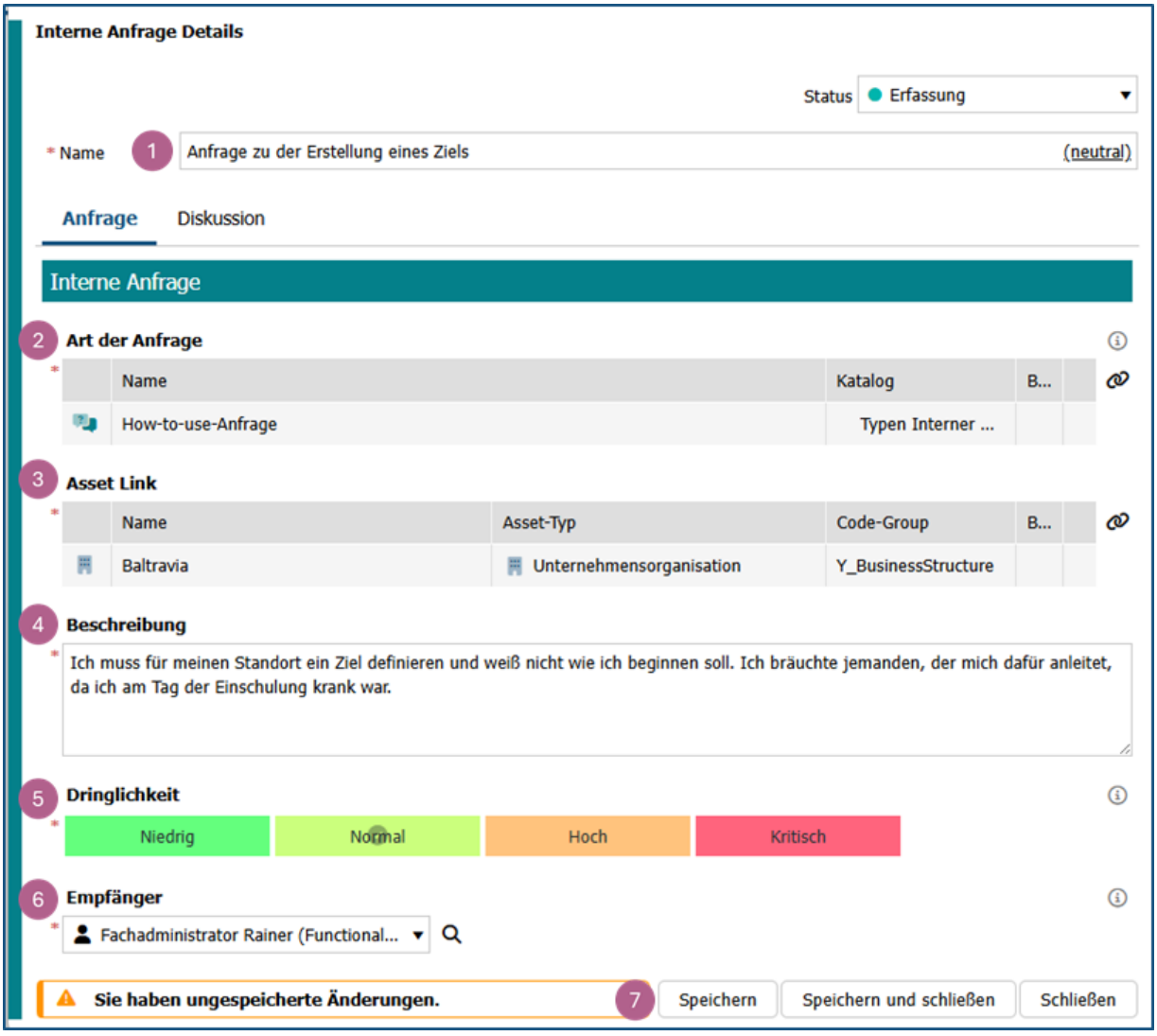
2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Interne Anfrage >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen



1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Interne Anfrage* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Interne Anfrage* einzigartig.
2. **Art der Anfrage**: Anschließend muss der Benutzer angeben, um welche Art von *Interner Anfrage* es sich handelt, wobei der Benutzer mehrere Angaben machen kann. Hinter dem Link befindet sich ein GRC Framework mit vordefinierten "Arten der Anfrage", die mittels des Icons verlinkt werden können.

> Der GRC Framework "Typen Interne Anfrage" wird vom eigenen Management gepflegt und kann von diesem bei Bedarf erweitert werden.

3. **Asset Link**: Eine Verlinkung mittels des Icons zu einem "Assets" ist notwendig.

> Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer kein Asset auf der Rolle "rol.StandardUser" zugewiesen. Mittels des Work Items

> *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

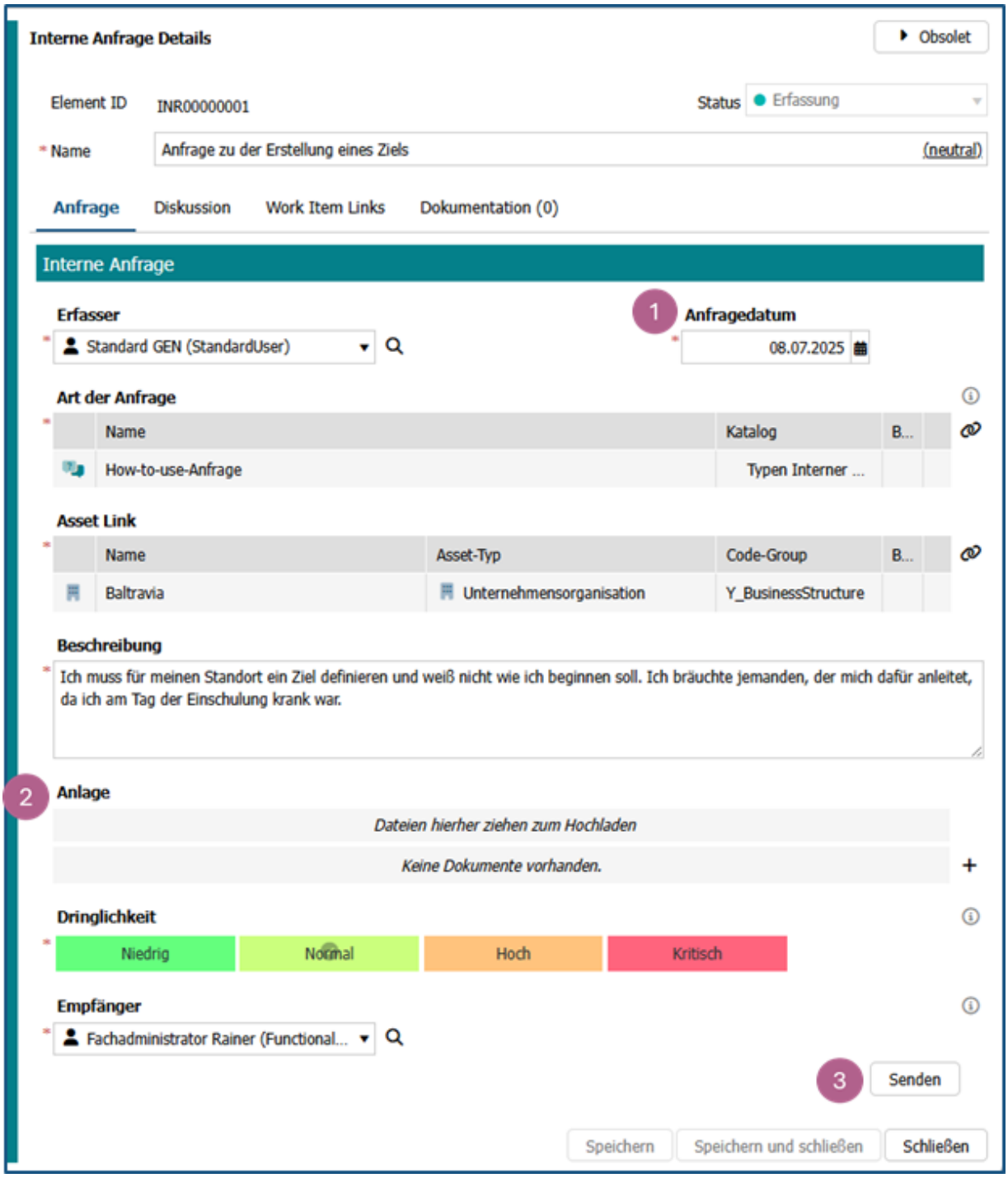
4. **Beschreibung**: Der Benutzer kann angeben, worum es sich bei seinem Anliegen handelt. Dies kann dem nachfolgenden Benutzer im Workflow helfen, die Anfrage besser einordnen zu können
5. **Dringlichkeit**: Mittels vier vorgegebenen Klassifizierungen kann der Benutzer seine "Dringlichkeit", mit der die *Interne Anfrage* beantwortet werden sollte, angeben.
6. **Empfänger**: Der Benutzer hat einen "Empfänger" auszuwählen, der seine *Interne Anfrage* beantworten wird.

> Es werden nur Benutzer als "Empfänger" vorgeschlagen die eine passende Gruppenzuordnung zu "grp.InternalRequestReceiver" aufweisen können.

7. **Speichern**: Sobald die Informationen angegeben sind kann der Benutzer speichern.

Schritt 3: Interne Anfrage abschließen

Nach dem erstmaligen Speichern wird das Datum der Anfrage automatisch befüllt (1). Weiters kannn – falls erforderlich – freiwillig eine Anlage (2) ergänzt werden.
Sobald keine weiteren Ergänzungen mehr notwendig sind, kann der Statusübergang durch Betätigung des Buttons „Senden“ (3) ausgelöst werden.

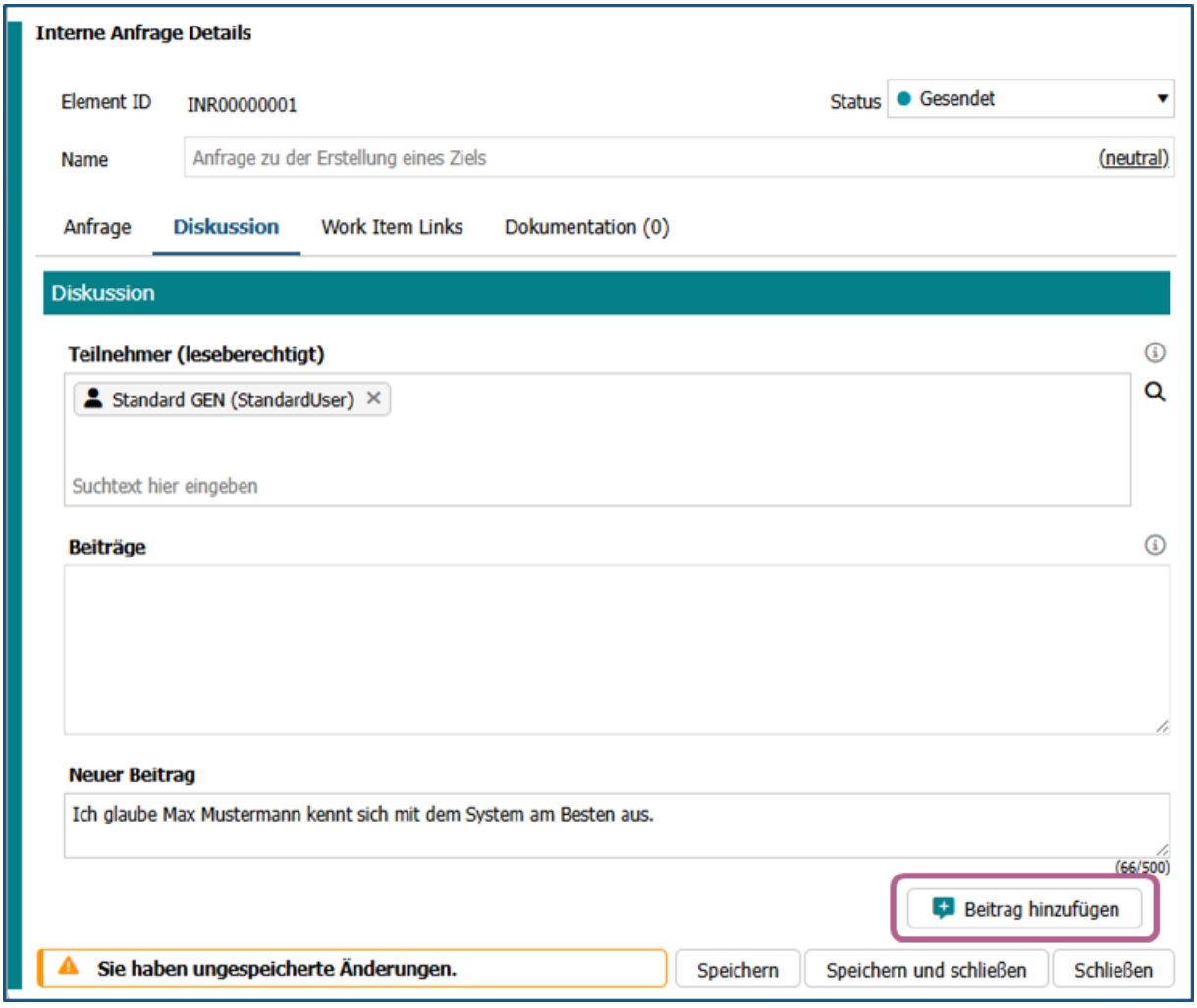


Der nächste Status wird von Interner Anfrageempfänger - Interne Anfrage beantworten & bearbeiten durchgeführt. Der Interner Anfrageempfänger prüft die Anfrage, ergänzt sie bei Bedarf und entscheidet, ob sie genehmigt oder zurückgewiesen wird.

Der Benutzer bekommt eine Notifikation zugesendet sobald der Empfänger mit der Bearbeitung der *Internen Anfrage* beginnt.

Optional Schritt 4: Diskussion starten

Es besteht jederzeit die Möglichkeit, eine Diskussion zur jeweiligen *Internen Anfrage* zu starten. Dies dient der schnelleren Klärung durch die zuständigen Personen.



2.1.3 Berechtigungsanfrage definieren & erstellen

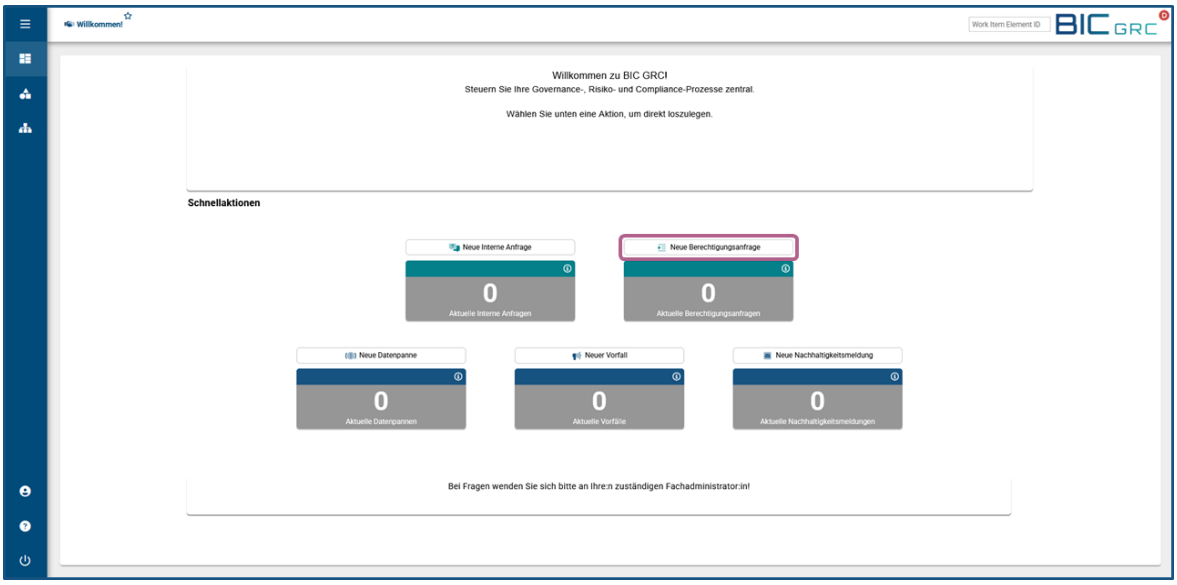
Jeder Benutzer in BIC GRC hat die Möglichkeit eine *Berechtigungsanfrage* zu stellen.

Schritt 1: Berechtigungsanfrage erstellen

Der Standard User kann in BIC GRC an mehreren Stellen *Berechtigungsanfragen* erstellen.

1. Erstellen über Dashboard

Der Benutzer navigiert über die Menüleiste zu **Dashboards >> Willkommen >> "Neue Berechtigungsanfrage"**.

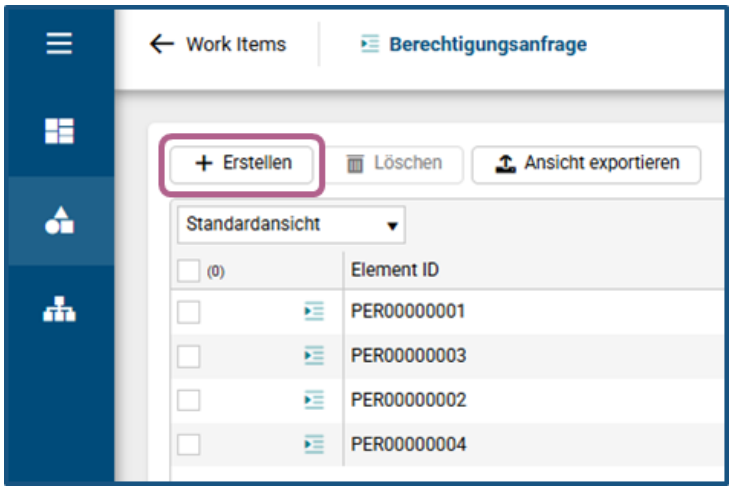


Ein neues Fenster öffnet sich anschließend automatisch.

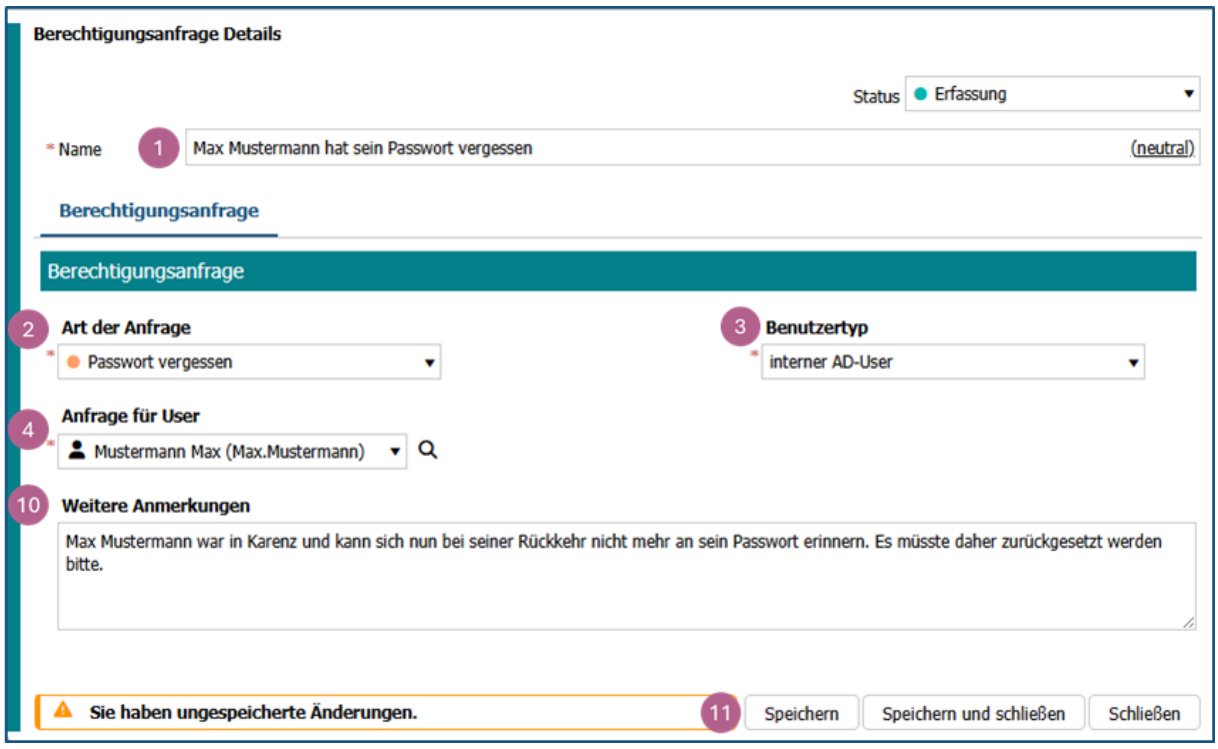
2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Berechtigungsanfrage >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen



1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für den *Berechtigungsanfrage* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Berechtigungsanfrage* einzigartig.
2. **Art der Anfrage**: Anschließend muss der Benutzer angeben um welche Art von *Berechtigungsanfrage* es sich handelt.

> Bei der Art der Anfrage kann in erster Linie unterschieden werden zwischen Anfragen für bestehende Benutzer und Anfragen für Benutzer die in BIC GRC angelegt werden sollen.

3. **Benutzertyp**: Der "Benutzertyp" ist abhängig von der "Art der Anfrage". So können unterschiedliche Benutzertypen - von internen sowie externen - AD-User bis zu internen oder externen manuell neu anzulegenden Benutzern ausgewählt werden.

> So macht es beispielsweise Sinn bei einer "Neuanlage Berechtigungen" nur manuell anzulegende Benutzer anzugeben, da sie in BIC GRC eben noch kein Benutzer sind. Auf der anderen Seite kann nur Benutzern eine Berechtigung entzogen werden die zum aktuellen Zeitpunkt schon einen Benutzer in BIC GRC haben.

4. **Anfrage für Benutzer**: Für die Anzeige dieses Attributes muss bei dem "Benutzertypen" interner oder externer AD-User angegeben sein. Nur wenn es sich um einen bestehenden Benutzer in BIC GRC handelt kann mittels des Icons 🔍 ein Benutzer gesucht und ausgewählt werden.
5. **Anfrage für neuen Benutzer**: Bei der "Anfrage für neuen Benutzer" müssen drei Attribute ausgefüllt werden:

- Nachname
- Vorname
- E-Mail Adresse

> Bei diesen Daten handelt es sich um die Mindestangaben die der Antragsverwalter später braucht, um den Benutzer erfolgreich anlegen zu können.

> Unter den "Weiteren Anmerkungen" könnte beispielsweise ergänzt werden, welche Position der neue Benutzer in BIC GRC hat oder welches Dashboard ihm als Standard Dashboard angezeigt werden soll.

6 **Grundlage der Berechtigung**: Abhängig von der gewählten "Art der Anfrage" und dem "Benutzertypen" werden dem Antragssteller unterschiedliche Grundlagen für die Berechtigungsvergabe angezeigt.

> Sollte keine passende Auswahl für die "Grundlage der Berechtigung" möglich sein kann der Antragssteller "sonstiges" wählen. Anschließend wird ihm ein Textfeld eingeblendet, wo eine "Andere Grundlage" verpflichtend anzugeben ist.

7 **Angefragte Profile**: Der Antragssteller kann aus allen Benutzerprofilen das passende Profil aussuchen.

> Dabei werden dem Antragssteller alle Benutzerprofile angezeigt die es laut der Standard Solution gibt. Sollten weitere Benutzerprofile hinzugefügt worden sein (customized) werden diese nicht automatisch in diese Liste übernommen.

> Sollte der letzte Wert - Zusätzliche Berechtigung - ausgewählt werden muss verpflichtend ein Textfeld mit weiteren Informationen ausgefüllt werden.

8 **Asset-Verantwortung**: Da in BIC GRC ein Asset-zentriertes Berechtigungskonzept die Basis für alle Berechtigungen darstellt, muss dem Benutzer nicht nur ein passendes Profil, sondern auch ein Asset zugeordnet werden, für welchen Bereich das Profil gelten soll..

> Sollte die Berechtigung beispielsweise für eine Organisationseinheit und alle darunter liegende Elemente gelten, sollte zusätzlich die Checkbox "Die Asset-Berechtigungen erstrecken sich auch auf darunterliegenden Elemente" angeklickt werden, sodass der Antragsverwalter weiß, dass er die Berechtigungen dementsprechende einstellen muss.

> Dem Antragssteller werden nur Assets angezeigt wo er auch die entsprechenden Berechtigungen besitzt.

9 **Zeitraum bzw. Von-Datum**: Sollte der Antragssteller eine Ruhendstellung (Zeitraum) oder den Entzug von Berechtigungen (Von- Datum) anfragen ist von ihm ein Datum zu

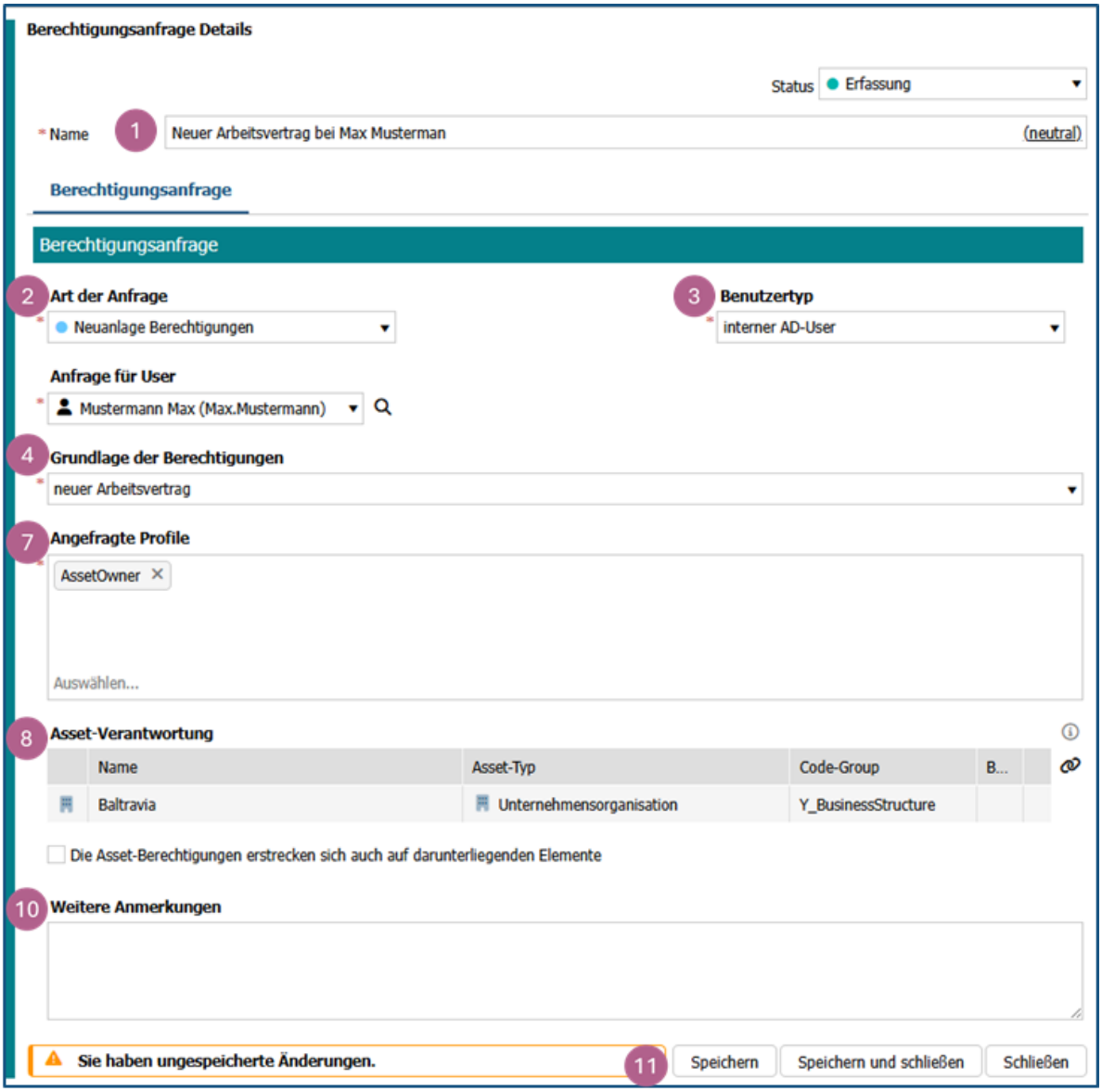
hinterlegen.

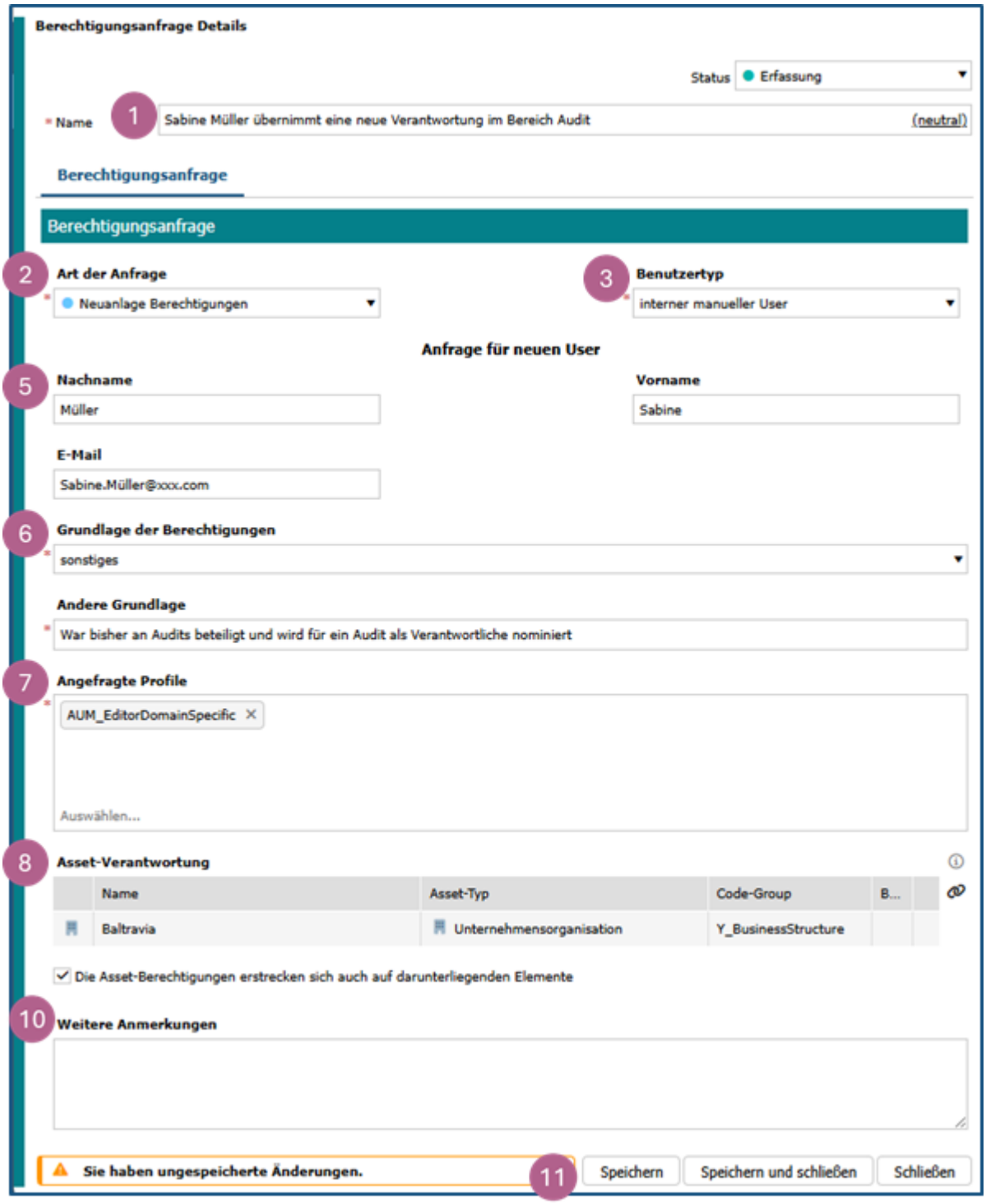
10 **Weitere Anmerkungen**: In diesem Textfeld können weitere Informationen hinterlegt werden.

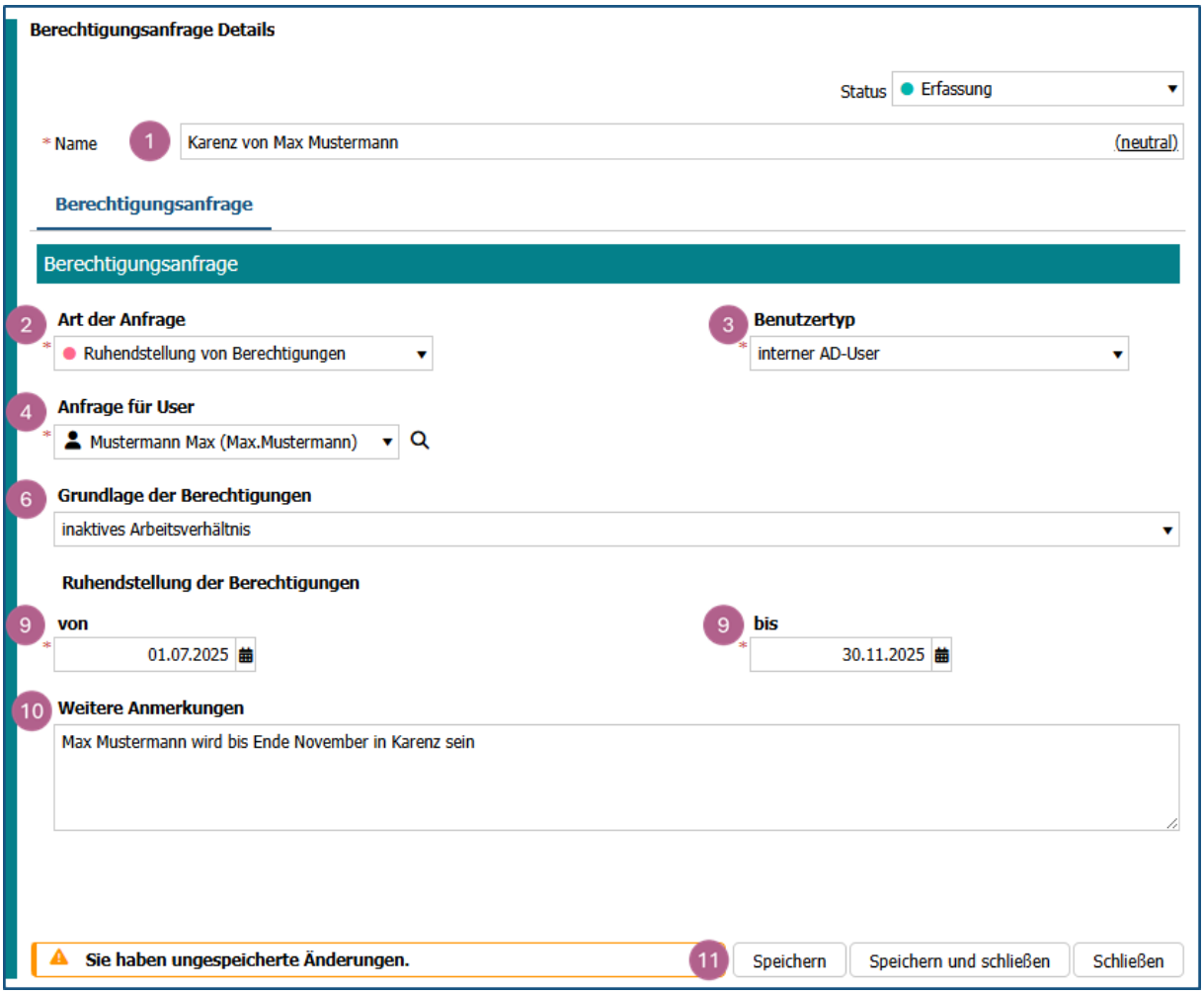
> So können hier besondere Umstände dokumentiert werden, wie beispielsweise die Ruhendstellung von Berechtigungen durch längeren Krankenstand oder Karenz-Modellen eines Benutzers.

11 **Speichern**: Sobald die Informationen angegeben sind kann der Benutzer speichern.

Weitere Beispiele:



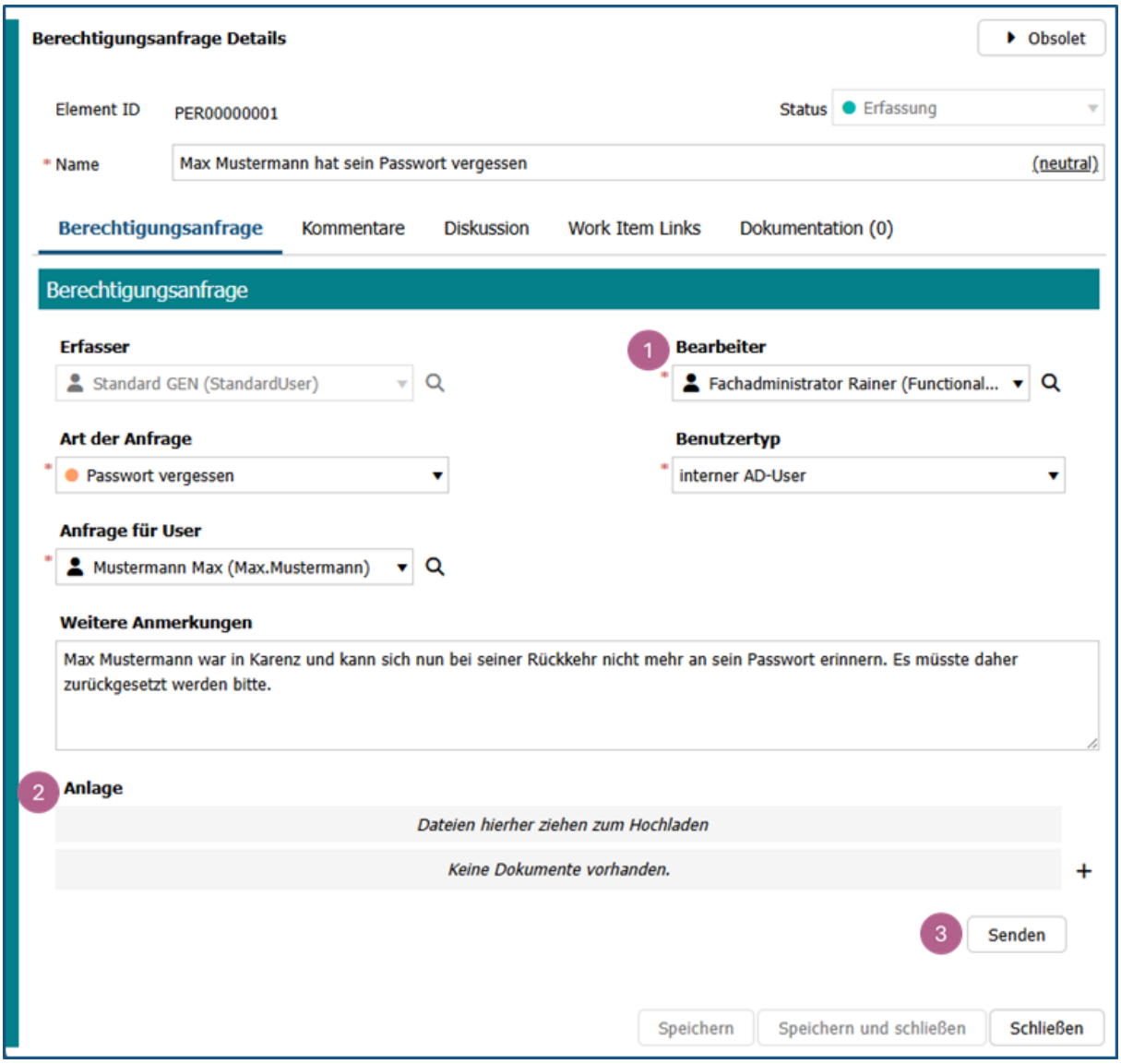

Berechtigungsanfrage Details
Status
Erfassung
Name
1
Sabine Müller übernimmt eine neue Verantwortung im Bereich Audit
(neutral)
Berechtigungsanfrage
Berechtigungsanfrage
2
Art der Anfrage
Neuanlage Berechtigungen
3
Benutzertyp
interner manueller User
Anfrage für neuen User
5
Nachname
Müller
Vorname
Sabine
E-Mail
Sabine.Müller@xxx.com
6
Grundlage der Berechtigungen
sonstiges
Andere Grundlage
War bisher an Audits beteiligt und wird für ein Audit als Verantwortliche nominiert
7
Angefragte Profile
AUM_EditorDomainSpecific
Auswählen...
8
Asset-Verantwortung
Name
Asset-Typ
Code-Group
B...
Baltravia
Unternehmensorganisation
Y_BusinessStructure
Die Asset-Berechtigungen erstrecken sich auch auf darunterliegenden Elemente
10
Weitere Anmerkungen
Sie haben ungespeicherte Änderungen.
11
Speichern
Speichern und schließen
Schließen



Schritt 3: Berechtigungsanfrage abschließen

Nach dem erstmaligen Speichern wird der Erfasser automatisch hinterlegt und es muss ein Bearbeiter angegeben werden 1. Weiters kannn – falls erforderlich – freiwillig eine Anlage 2 ergänzt werden.

Sobald keine weiteren Ergänzungen mehr notwendig sind, kann der Statusübergang durch Betätigung des Buttons „Senden“ 3 ausgelöst werden.



Der nächste Status wird von Berechtigungsanfrageempfänger - Berechtigungsanfrage beantworten & bearbeiten durchgeführt.

Der Benutzer bekommt eine Notifikation zugesendet sobald der Empfänger mit der Bearbeitung der *Berechtigungsanfrage* beginnt.

2.2 Asset Manager

Der Asset Manager ist für einen bestimmten Knoten innerhalb der Asset-Hierarchie verantwortlich – beispielsweise für eine Organisationseinheit – sowie für alle darunter liegenden Assets (z. B. Primary oder Supporting Assets).

> **Der Asset Manager ist für das Anlegen, Bearbeiten und Pflegen von Assets verantwortlich. Diese Rolle trägt zur Sicherstellung einer vollständigen und aktuellen Asset-Datenbasis innerhalb der Asset-Hierarchie bei.**

Folgende Aufgabe(n) hat ein Asset Manager in BIC GRC:

- Assets vorbereiten & pflegen

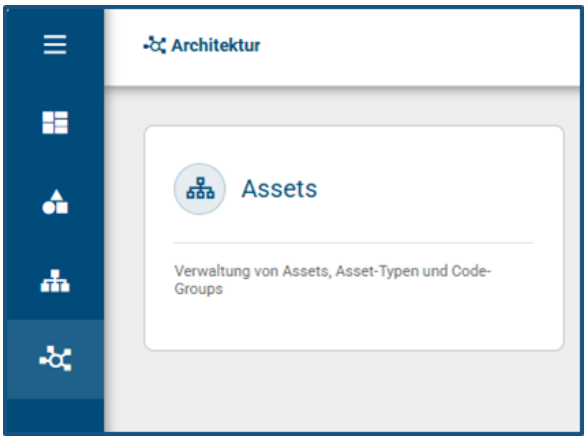
2.2.1 Assets vorbereiten & pflegen

Sofern einem Asset Manager ein oder mehrere Assets zugewiesen wurden, ist er für deren Verwaltung verantwortlich.

Schritt 1: Navigieren zu Assets

Über die Menüleiste **Administration >> Assets** kann er zu der Asset-Hierarchie in BIC GRC navigieren.

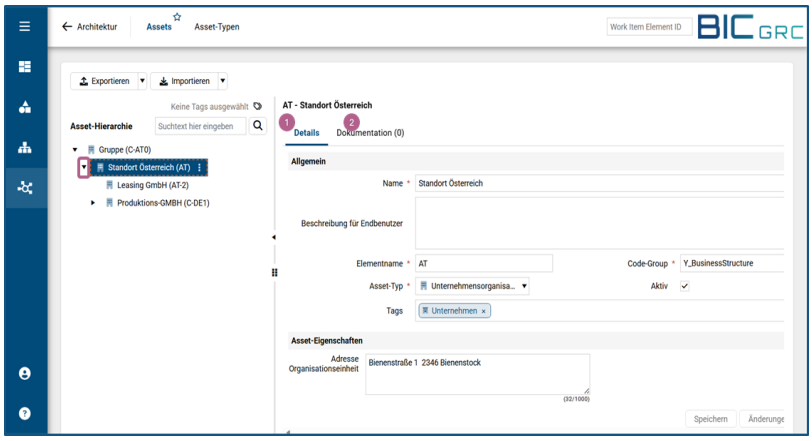
Dabei ist die Ansicht auf Berechtigungsebene beschränkt und kann je nach Benutzer variieren.

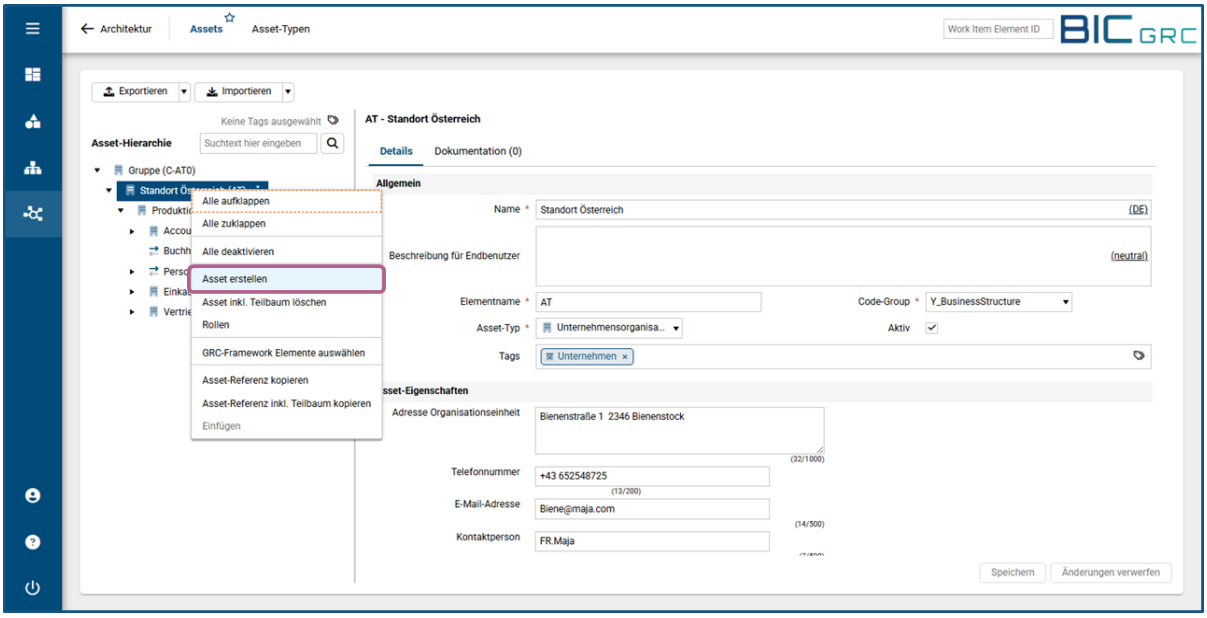


Schritt 2: Assets erstellen

Der Asset Manager bekommt bei dem Menüunterpunkt **Assets** eine zweigeteilte Ansicht:

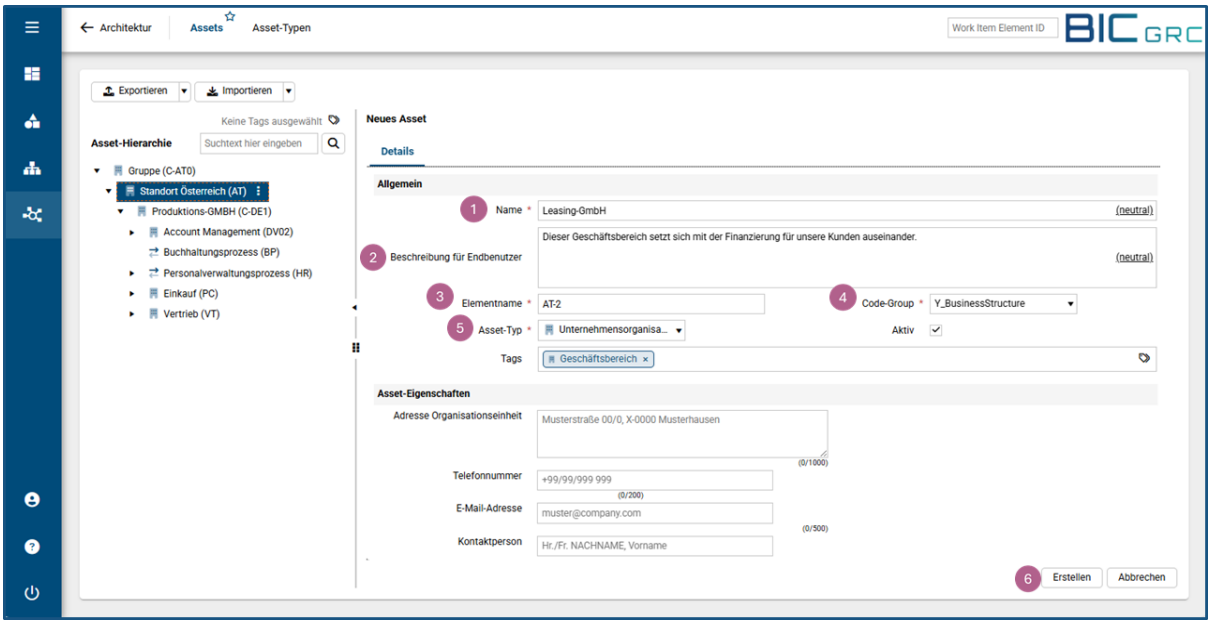
- Linke Seite: Baumstruktur der Asset-Hierarchie. Diese kann über das entsprechende Icon ▸ auf- und zugeklappt werden.
- Rechte Seite: Detailansicht des ausgewählten Assets mit Informationen (1) und hinterlegter Dokumentation (2)





Ein neues Asset wird durch Rechtsklick (bzw. Klick auf die drei Punkte ) auf ein vorhandenes Asset und Auswahl von „Asset erstellen“ erzeugt.

Anschließend erscheint auf der rechten Seite das Fenster „Neues Asset“, in dem relevante Informationen hinterlegt werden.



1 **Name**: Für das Asset muss ein passender "Name" hinterlegt werden.

> Dabei ist darauf zu achten, dass nicht nur der "Neutrale Name", sondern auch die deutsche und englische Version des Asset-Namens gepflegt wird.

> An mehreren Stellen in BIC GRC wird der "Neutrale Name" für die Anzeige übernommen, daher wird stark empfohlen den Namen sinnvoll zu wählen.

2 **Beschreibung für Endbenutzer**: Es wird empfohlen eine Beschreibung für ein Asset zu hinterlegen, um die Wichtigkeit oder Grundstrukturen des Assets den Endbenutzern zu erklären.

3 **Elementname**: Der "Elementname" macht das Asset später einzigartig in BIC GRC. Der "Elementname" wird auch immer neben dem Namen des Assets in der Asset-Hierarchie angezeigt.

> Im Beispiel ist der Elementname "C-DE2" weil es auf der gleichen Ebene in der Asset-Hierachie einen Geschäftbereich "Medikamente" gibt, der den Elementnamen "C-DE1" hat. Daher wurde der "Elementname" des neuen Assets angepasst an das bestehende Asset vergeben.

4 **Code-Group**: Für die Erstellung von Assets sind nicht alle Code Groups relevant. Folgende Code Groups sollten für Assets verwendet werden:

- X_ ListStructureElement: Soll für Assets des Typen "Listenstrukturelement" verwendet werden
- Y_ BusinessStructure: Soll für Assets des Typen "Unternehmensorganisationen" verwendet werden
- Z_Asset: Soll für Assets der Typen "Primary Asset" und "Supporting Asset" verwendet werden

5 **Asset-Typ**: In BIC GRC gibt es vier verschiedene Asset-Typen:

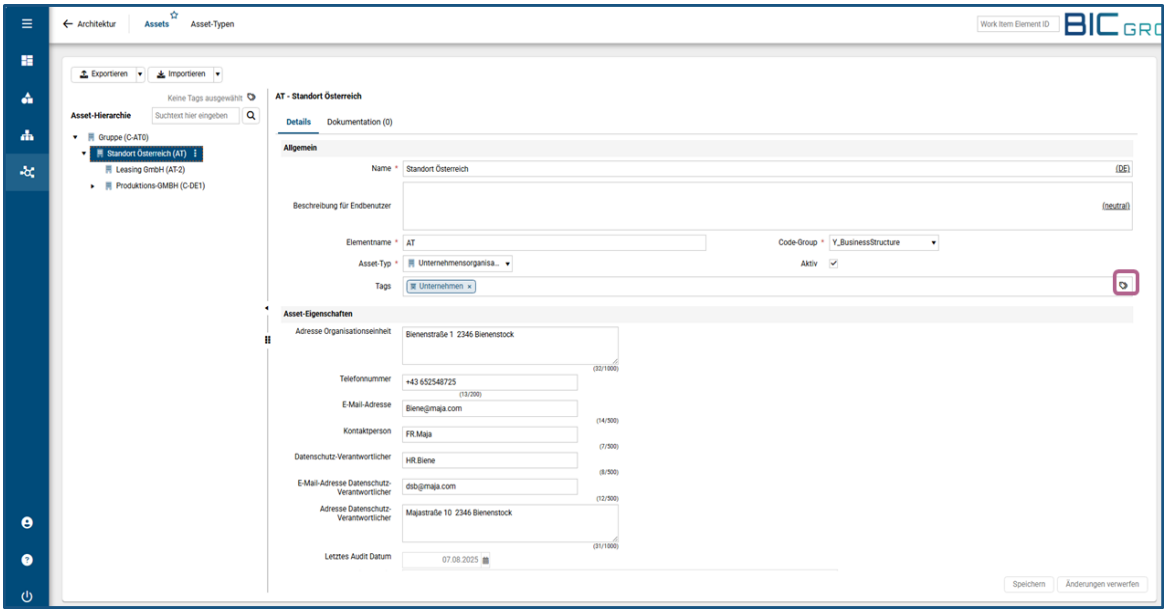
- Unternehmensorganisation: Stellen nach dem obersten Knotenpunkt in der Assethierarchie die höchstmögliche Ebene/Level da.
- Primary Asset: Sind direkt unter den Unternehmensorganisationen einzuordnen und sind Informationen oder Prozesse.
- Supporting Asset: Stellen alle Elemente da, die den Prozess oder die Information untertützen.
- Listenstrukturelement: Soll den Benutzer unterstützen eine Struktur in der Asset-Hierarchie herzustellen.

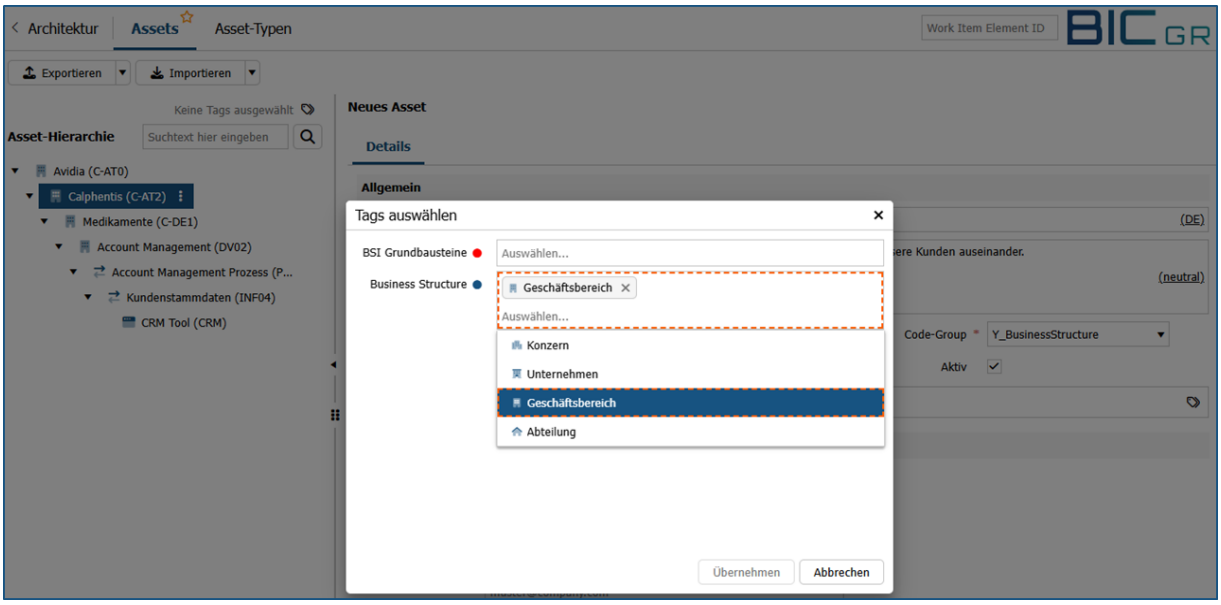
> Änderungen an den Asset-Typen können in der Solution zu Problemen führen. Daher ist eine Änderung zu vermeiden!

6 **Erstellen**: Nachdem diese Eingaben gemacht wurden kann das Asset erstellt werden.

Schritt 3: Assets tagen

Nach Erstellung des Assets werden passende Tags vergeben. Durch Klick auf das entsprechende Icon werden alle verfügbaren Tags vorgeschlagen, die dem Asset zugeordnet werden können.





Abhängig von dem Asset- Typen werden dem Asset Manager unterschiedliche Tag Kategorien vorgeschlagen.

Der Schritt, das Asset zu tagen, darf nicht vergessen werden, da in vielen Bereichen in BIC GRC nicht nur nach dem passenden Asset-Typen, sondern auch nach dem passenden Tag gefragt wird.

Schritt 4: Asseteigenschaften pflegen

Für die Asset- Typen „Unternehmensorganisationseinheit“ oder „Supporting Assets“ können zusätzliche Eigenschaften gepflegt werden.

Diese Asseteigenschaften können bei Bedarf vom Unternehmen erweitert oder reduziert werden. Für mehr Informationen kann sich an den verantwortlichen Fachlichen Administrator des eigenen Unternehmens gewandt werden.

"Primary Assets" haben auch Asseteigenschaften, diese sollen aber nicht vom Asset Manager bearbeitbar werden, sondern werden durch unterschiedliche Mechanismen von BIC GRC automatisch befüllt.

2.3 Assessor

Ein Assessor ist ein Benutzer, der die Aufgabe hat an seinem Asset unterschiedliche Assessments durchzuführen.

Assessments sind Fragenkataloge mit Fragen zu spezifischen Themen, wie beispielsweise Doppelte Wesentlichkeitsanalyse .

Folgende Aufgaben hat ein Assessor in BIC GRC:

Doppelte Wesentlichkeitsanalyse

- Assessment erstellen & starten
- Bewertung durchführen & bewerten
  - Finanzielle Wesentlichkeit ableiten & erstellen
  - Finanzielle Wesentlichkeit kopieren & erstellen
  - Auswirkungs-Wesentlichkeit ableiten & erstellen
  - Auswirkungs-Wesentlichkeit kopieren & erstellen
- Bewertung abschließen & überprüfen
- Assessment abschließen & auswerten
- Assessment überprüfen & neubewerten

Folgende Aufgaben können sich aus den Assessments ergeben:

- Finanzielle Wesentlichkeit überprüfen & freigeben
- Auswirkungs-Wesentllichkeit überprüfen & freigeben

Der Assessor kann darüber hinaus noch weitere Work Items erstellen in BIC GRC. Da dies aber nicht seine Hauptaufgabe ist, wird an dieser Stelle nur auf andere Benutzerprofile verwiesen:

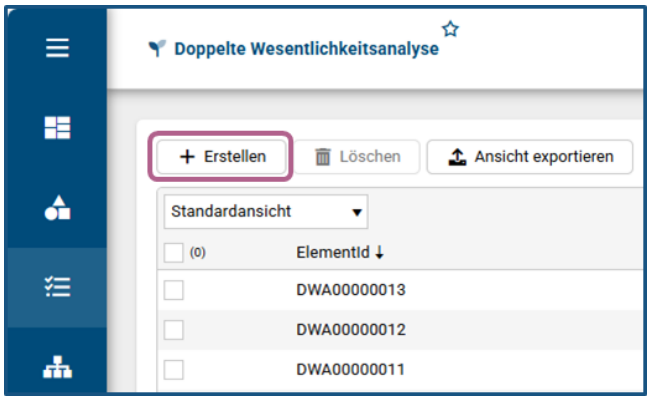
- Ziel definieren & erstellen
  - Zwischenziel definieren & erstellen
- Maßnahme definieren & erstellen
- Kontrolle ableiten & erstellen
- Nachhaltigkeitsrisiko identifizieren & erstellen

2.3.1 Doppelte Wesentlichkeitsanalyse - Assessment erstellen & starten

Um nach den Anforderungen des "European Sustainability Reporting Standard" die Doppelten Wesentlichkeitsanalyse zu erfüllen, muss der Assessor auch in BIC GRC ein Assessment zu der "Doppelten Wesentlichkeitsanalyse" erstellen.

Schritt 1: Navigation zu Assessment

Der Assessor erstellt ein Assessment des Typs "Doppelte Wesentlichkeitsanalyse" über die Menüleiste **Assessment >> Doppelte Wesentlichkeitsanalyse >> "Erstellen"**oder **Assets >> Auswahl einer Unternehmenseinheit >> Links >> Öffnen des Reiters "Doppelte Wesentlichkeitsanalyse" >> "Erstellen"**.



> Assessments dieses Typen können nur auf einer "Organisationseinheit" durchgeführt werden.

Schritt 2: Assessment Details hinterlegen

1. **Asset**: Über einen Wizzard muss der Assessor zunächst ein Asset auswählen, für das er ein Assessment des Types "Doppelte Wesentlichkeitsanalyse" erstellen möchte.

   Sobald ein Asset mittels ausgewählt wurde kann zu dem nächsten Schritt navigiert werden.
2. **Name**: Als nächster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Assessment* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Assessment* einzigartig.
3. **Zeitraum**: Das Assessment braucht ein Start- und ein Enddatum, um anzugeben, in welchem Zeitraum das Assessment gültig ist.

   > Das Enddatum wird von einem Scheduler herangezogen, um ein Mail automatisch an den Assessor zu schicken.
4. **Verantwortliche Person**: Der Assessor hat einen "Assessor" zu nominieren, der die Bewertung des *Assessments* durchführt.

   > Sollte der Assessor gleichzeitig der Ersteller sein kann er sich selber eintragen.
5. **Stakeholder**: Es können zusätzliche Benutzer, die in BIC GRC hinterlegt sind, hinzugefügt werden. Des weiteren können auch Stakeholder manuell im Textfeld eingetragen werden.
6. **Speichern**: Anschließen kann das Assessment zum ersten Mal gespeichert werden.

Schritt 3: GRC Framework Element Zuordnungen kontrollieren

Bevor das Assessment gestartet wird wird empfohlen die hinterlegten Angaben bzw. bisher zugelinkten GRC Framework Elemente zu überprüfen.

Die aktivierten GRC Framework Elemente kommen aus einer Vorauswahl am GRC Framework. Dort wurde von einer berechtigten Person eine Vorauswahl der zutreffenden Elemente vorgenommen. Diese Vorauswahl wird für alle neu erstellten Assessments herangezogen.

Dafür klickt der Assessor auf die drei Punkte links von der Element ID  auf "  GRC Framework Elemente zuordnen". Als nächsten Schritt überprüft er die Assessment Phase "Identifikation der Auswirkung" auf Richtigkeit bzw. ob Ergänzungen zu den bisherigen Selektionen notwendig sind bevor er auf "Speichern" klickt.

> Sollte der Assessor später noch GRC Framework Elemente hinzufügen, z.B. wenn schon die Bewertung der Phase begonnen hat, werden die neu hinzugefügten GRC Framework Elemente automatisch aktiviert und können im Rahmen des aktuell laufenden Assessments mitbewertet werden.

> Sollte der Assessor GRC Framework Elemente abwählen werden die bisherigen Bewertungen zu dem spezifischen Element gelöscht.

Schritt 4: Assessment starten

Nachdem das Assessment erstellt und die GRC Framework Elemente kontrolliert wurden kann das Assessment gestartet werden. Dafür klickt der Assessor auf das Icon  .

> Die weiteren Schritte findet der Assessor unter Assessor - Bewertung durchführen & bewerten.

2.3.2 Doppelte Wesentlichkeitsanalyse - Bewertung durchführen & bewerten

Nachdem der Assessor das Assessment zu "Doppelte Wesentlichkeitsanalyse" für ein bestimmtes Asset gestartet hat kann er die Phase "Identifikation der Auswirkung" starten.

Schritt 1: Übersicht über Assessment-Schirm

Der Assessor hat drei Abschnitte die für ihn für die Bewertung der Phase relevant sind.

Im linken oberen Abschnitt sieht er einen Kreis (1), der ihm dabei helfen soll den aktuellen Fortschritt über das Assessment mitzuverfolgen. Dabei wird im Rahmen aller Bewertungen ein Progress berechnet der den Fortschritt in Prozent angibt. Daneben findet der Assessor Basisinformationen wie Status und Asset (2).

> Für die Berechnung des Fortschritts werden im Status "In Bewertung" die Eingaben zu den Auswirkungen herangezogen und für den Status "In Überprüfung" braucht es Angaben in der "Expertenschätzung" und der zugehörigen "Beschreibung".

Auf der linken Seite des Fensters findet er den zu bewertenden GRC Framework (3). Im Assessment zu "Themenbezogene ESRS" muss der Assessor alle aktivierten GRC Framework Elemente bewerten. Dabei kann der GRC Framework mittels Klick auf das Icon ▸ geöffnet werden.

> **Der Assessor kann in der Phase zu dem GRC Framework "Themenbezogene ESRS" nur die untersten Elemente des GRC Frameworks bewerten.**

Zu bewertende GRC Framework Elemente haben das Icon , Bewertungen die sich in der Überprüfung befinden haben das Icon und abgeschlossene GRC Framework Elemente das Icon .

Auf der rechten Seite des Fensters findet der Assessor die Hauptmaske, die es zu bewerten gilt. Diese wird in den nächsten Schritten genauer beschrieben.

Schritt 2: Assessment Details hinterlegen

1. **Panel - Beschreibung**: Als erstes sieht der Assessor eine Beschreibung die aus dem GRC Framework "Themenbezogene ESRS" übernommen wurde. Dabei handelt es sich um die Beschreibung die am GRC Framework direkt hinterlegt wurde.

   > Die Beschreibung kann und soll vom Assessor nicht bearbeitet werden, sondern soll diesen zusätzliche Informationen für dieses GRC Framework Element zu Verfügung stellen.

   Anschließend fährt der Assessor im "Panel - Bewertung" fort.

2. **Unternehmensweite Informationen**: In diesem Textfeld werden Informationen aus dem GRC Framework übernommen die dort von berechtigten Benutzern vorab hinterlegt wurden.

   > Diese Beschreibung unterscheidet sich von der Panel-Beschreibung dementsprechend, dass die Beschreibung aus dem Panel vom ESRS direkt kommt und die "Unternehmensweiten Informationen" vom eigenen Unternehmen eingetragen worden sind, um Assessoren bei der Bewertung zu unterstützen.

3. **Informationen zur Auswirkung**: Der Assessor hat im nächsten Schritt zu bewerten, ob sein Asset durch dieses GRC Framework Element eine Auswirkung durch die Umwelt spürt, oder weiß, dass sein Unternehmen zu diesem Thema eine Auswirkung auf die Umwelt ausübt.

   Für die Bewertung stehen ihm zwei verschiedene "Ja/Nein" Heatmaps zu Verfügung. Wählt der Assessor "Ja" bei einem der beiden Fragen aus, werden im jeweils direkt darunter die Punkte 4 & 5 angezeigt. Wenn er "Nein" auswählt werden die Punkte 4 & 5 nicht angezeigt.

   Sollte der Assessor bei beiden Fragen "Nein" auswählen darf er direkt einen Statusübergang in den Status "Abgeschlossen" für seine Bewertung durchführen.

   > Sollte sich der Assessor nicht sicher sein, ob auf dem Asset zu diesem GRC Framework Element passende Auswirkungen zu finden wären, kann er in dem Burger-Menü rechts im Bild auf den Menüpunkt "Passende Templates" gehen. Klickt er auf diesen

Punkt bekommt er eine Liste an allen IRO Templates angezeigt, die von einem berechtigten Freigeber DS erstellt wurden zu diesem spezifischen "Themenbezogene ESRS".

4. **Beschreibung**: Anschließend kann der Assessor noch eine zusätzliche Beschreibung hinterlegen, warum und wo er eine Auswirkung sieht.
5. **Bewertung Auswirkung**: Wenn bei einem der beiden Auswirkungen "Ja" ausgewählt wurde muss verpflichtend ein Work Item des Typen *Auswirkungs-Wesentlichkeit* oder *Finanzielle Auswirkung* erstellt oder verlinkt werden.

Bei der Verlinkung kann der Assessor nur *Auswirkungs-Wesentlichkeit* und *Finanzielle Auswirkung* verlinken, die auch an diesem Asset liegen.

In diesem Assessment gibt es eine besondere Funktion: Sollte ein *IRO Template* passen und möchte der Assessor die Informationen des *IRO Templates* für sein Bewertung nutzen, kann er mittels des Icons + nicht nur ein neues Work Item der Typen *Auswirkungs-Wesentlichkeit* oder *Finanzielle Auswirkung* erstellen (1. Option), sondern auch aus den bestehenden *IRO Templates* ein passendes Template als Vorlage für die *Auswirkungs-Wesentlichkeit* oder *Finanzielle Auswirkung* verwenden (2.Option).

Mehr Informationen zu der Erstellung von Finanzielle Wesentlichkeit ableiten & erstellen/Auswirkungs- Wesentlichkeit ableiten & erstellen oder Finanzielle Wesentlichkeit kopieren & erstellen/Auswirkungs-Wesentlichkeit kopieren & erstellen.

6. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "In Überprüfung" durchgeführt.

   Es ist notwendig für den Statusübergang, dass die "Informationen zur Auswirkung" einen Wert haben und zusätzlich bei der Wahl von "Ja" mindestens ein Work Item verlinkt oder erstellt wurde. Zudem müssen sich die erstellten oder verlinkten Work Items zumindest im Status "In Überprüfung" befinden.

   Sobald der Statusübergang erfolgt ist können die bisherigen Angaben nicht mehr verändert werden.

Weitere Schritte sind unter Assessor - Bewertung abschließen & überprüfen zu finden.

2.3.3 Finanzielle Wesentlichkeit ableiten & erstellen

Bei der *Finanziellen Wesentlichkeit* wird betrachtet, ob und in welchem Ausmaß die Umwelt eine Auswirkung auf das Unternehmen hat.

Schritt 1: Finanzielle Wesentlichkeit erstellen

Eine *Finanzielle Wesentlichkeit* kann nur aus einem Assessment des Typs "Doppelte Wesentlichkeitsanalyse" erstellt werden.

Für die Erstellung wird während der Bewertung durch das Icon ✚ (1.Option) eine neue *Finanzielle Wesentlichkeit* erstellt.

> Das *Finanzielle Wesentlichkeit* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil der Bewertung.

Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Finanzielle Wesentlichkeit* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Finanzielle Wesentlichkeit* einzigartig.
2. **Beschreibung**: Die *Finanzielle Wesentlichkeit* sollte so genau wie möglich beschrieben und definiert werden, um Benutzern, die im Workflow nachgelagert sind, einen Überblick über die Aufgabe der *Finanzielle Wesentlichkeit* zu gewähren.
3. **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Finanzielle Wesentlichkeit* erstmalig gespeichert werden.

Schritt 3: Weitere Details hinterlegen

1. **Verantwortlichkeiten**: Der Assessor wird automatisch im Attribut "Assessor" eingetragen und kann nicht mehr verändert werden. Zusätzlich kann vom Assessor ein "Bearbeiter" eingetragen werden. Dieser Bearbeiter ist für die Bewertung im nächsten Status verantwortlich.

   > Trägt der Assessor keinen Bearbeiter ein und macht einen Statusübergang zu "In Bewertung" wird der Assessor automatisch als "Bearbeiter" hinterlegt und muss die Bewertung selber vornehmen.

2. **Scope**: Der "Scope" ist das Asset an dem das Assessment durchgeführt wurde. Er wird automatisch nach dem ersten Speichervorgang gesetzt.

   > *Finanzielle Wesentlichkeiten* mit dem Scope vom Assessment können auch in anderen Bewertungen im Assessment verlinkt werden.

3. **ESRS Topic**: Der "ESRS Topic" ist das GRC Framework Element für den diese *Finanzielle Wesentlichkeit* gilt. Er wird automatisch nach dem ersten Speichervorgang gesetzt.

   Sollte die *Finanzielle Wesentlichkeit* mehrmals im selben Assessment verlinkt werden, dann werden alle GRC Framework Elemente zu denen es einen Bezug gibt additiativ angeführt.

4. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Bewertung" durchgeführt.

   Mehr Informationen über die Bewertung unter Bearbeiter DS - Finanzielle Wesentlichkeit definieren & bewerten

Zurück zu dem Schritt Assessor - Bewertung durchführen & bewerten.

2.3.4 Finanzielle Wesentlichkeit kopieren & erstellen

Bei der *Finanziellen Wesentlichkeit* wird betrachtet, ob und in welchem Ausmaß die Umwelt eine Auswirkung auf das Unternehmen hat.

Schritt 1: Finanzielle Wesentlichkeit kopieren

Eine *Finanzielle Wesentlichkeit* kann nur aus einem Assessment des Typen "Doppelte Wesentlichkeitsanalyse" erstellt werden.

Für das Kopieren wird während der Bewertung durch das Icon + (2.Option) eine neue *Finanzielle Wesentlichkeit* erstellt.

> Die *Finanzielle Wesentlichkeit* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil der Bewertung.

Schritt 2: IRO Template auswählen

Der Assessor bekommt nachdem er die 2. Option - Finanzielle Wesentlichkeit - IRO Template - gewählt hat eine Liste an passenden *IRO Templates* angezeigt.

Aus dieser Liste kann er ein passendes Template wählen und auf "OK" im unteren rechten Fenster klicken.

Sobald der Assessor dies gemacht hat werden alle Informationen wie Name, Beschreibung und die hinterlegten Werte der Bewertung aus dem Template in das Work Item *Finanzielle Wesentlichkeit* übernommen.

Der Assessor ist nach dem Kopieren direkt im Status "In Bewertung". Dort kann er die übernommen Werte aus dem *IRO Template* bei Bedarf noch einmal anpassen.

> Es werden dem Assessor nur *IRO Templates* vorgeschlagen die den Auswirkungstypen "Finanzielle Wesentlichkeit" hinterlegt haben.

Optional -Schritt 3: Nachhaltigkeitsstrategie hinterlegen

Der Bearbeiter kann im Tab "*Nachhaltigkeitsstrategie*" zusätzliche Links hinterlegen.

1. **Strategie**: Der Link "Strategie" führt zu dem Work Item *Dokumentierte Informationen*. Es können dabei keine neuen *Dokumentierte Informationen* erstellt, sondern nur verlinkt werden.

   > Da nur Benutzer mit dem spezifischen Profil Dokumenteneigner *Dokumentierte Informationen* erstellen dürfen, kann der Bearbeiter bei der Notwendigkeit einer noch nicht vorhandenen "Strategie" eine Diskussion im "*Diskussions*"-Tab beginnen.

2. **Maßnahme**: Neben der "Strategie" sollten auch *Maßnahmen* gesetzt und hinterlegt werden. Sie sollen dazu beitragen die aktuelle *Finanzielle Wesentlichkeit* zu reduzieren oder zu optimieren.
3. **Ziele**: Zuletzt kann es Sinn machen nicht nur Maßnahmen zu definieren, sondern sich auch Ziele zu setzen, wie mit der *Finanzielle Wesentlichkeit* in Zukunft umgegangen werden soll.
4. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Überprüfung" durchgeführt.

Zurück zu dem Schritt Assessor - Bewertung durchführen & bewerten oder weiter mit Assessor - Finanzielle Wesentlichkeit überprüfen & freigeben.

2.3.5 Finanzielle Wesentlichkeit ableiten & erstellen

Dabei wird betrachtet, wie die Umwelt eine Auswirkung auf das Unternehmen hat.

Schritt 1: Finanzielle Wesentlichkeit erstellen

Eine *Finanzielle Wesentlichkeit* kann nur aus einem Assessment des Typen "Doppelte Wesentlichkeitsanalyse" erstellt werden.

Für die Erstellung wird während der Bewertung durch das Icon + (1.Option) eine neue *Finanzielle Wesentlichkeit* erstellt.

> Das *Finanzielle Wesentlichkeit* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil der Bewertung.

Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Finanzielle Wesentlichkeit*erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Finanzielle Wesentlichkeit* einzigartig.
2. **Beschreibung**: Die *Finanzielle Wesentlichkeit* sollte so genau wie möglich beschrieben und definiert werden, um Benutzern, die im Workflow nachgelagert sind, einen Überblick über die Aufgabe der *Finanzielle Wesentlichkeit* zu gewähren.
3. **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Finanzielle Wesentlichkeit* erstmalig gespeichert werden.

Schritt 3: Weitere Details hinterlegen

1. **Verantwortlichkeiten**: Der Assessor wird automatisch in dem Attribut "Assessor" eingetragen und kann nicht mehr verändert werden. Zusätzlich kann vom Assessor ein "Bearbeiter" eingetragen werden. Dieser Bearbeiter ist für die Bewertung im nächsten Status verantwortlich.

> Trägt der Assessor keinen Bearbeiter ein und macht einen Statusübergang zu "In "Bewertung" wird der Assessor automatisch als "Bearbeiter" hinterlegt und muss die Bewertung selber vornehmen.

2. **Scope**: Der "Scope" ist das Asset an dem das Assessment durchgeführt wurde. Er wird automatisch nach dem ersten Speichervorgang gesetzt.

> *Finanzielle Wesentlichkeiten* mit dem Scope vom Assessment können auch in anderen Bewertungen im Assessment verlinkt werden.

3. **ESRS Topic**: Der "ESRS Topic" ist das GRC Framwework Element für den diese *Finanzielle Wesentlichkeit* gilt. Er wird automatisch nach dem ersten Speichervorgang gesetzt.

   Sollte die *Finanzielle Wesentlichkeit* mehrmals im selben Assessment verlinkt werden, dann werden alle GRC Framework Elemente zu denen es einen Bezug gibt additiativ angeführt.

4. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Bewertung" durchgeführt.

   Mehr Informationen über die Bewertung unter Bearbeiter DS - Finanzielle Wesentlichkeit definieren & bewerten

Zurück zu dem Schritt Assessor - Bewertung durchführen & bewerten.

2.3.6 Auswirkungs-Wesentlichkeit kopieren & erstellen

Bei der *Auswirkungs-Wesentlichkeit* wird betrachtet, ob und in welchem Ausmaß die Umwelt eine Auswirkung auf das Unternehmen hat.

Schritt 1: Auswirkungs-Wesentlichkeit kopieren

Eine *Auswirkungs- Wesentlichkeit* kann nur aus einem Assessment des Typen "Doppelte Wesentlichkeitsanalyse" erstellt werden.

Für das Kopieren wird während der Bewertung durch das Icon + (2.Option) eine neue *Auswirkungs-Wesentlichkeit* erstellt.

> Die *Auswirkungs-Wesentlichkeit* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil der Bewertung.

Schritt 2: IRO Template auswählen

Der Assessor bekommt nachdem er die 2. Option - Auswirkungs-Wesentlichkeit - IRO Template - gewählt hat eine Liste an passenden *IRO Templates* angezeigt.

Aus dieser Liste kann er ein passendes Template wählen und auf "OK" im unteren rechten Fenster klicken.

Sobald der Assessor dies gemacht hat werden alle Informationen wie Name, Beschreibung und die hinterlegten Werte der Bewertung aus dem Template in das Work Item *Auswirkungs-Wesentlichkeit* übernommen.

Der Assessor ist nach dem Kopieren direkt im Status "In Bewertung". Dort kann er die übernommen Werte aus dem *IRO Template* bei Bedarf noch einmal übersteuern.

> Es werden dem Assessor nur *IRO Templates* vorgeschlagen die den Auswirkungstypen "Finanzielle Wesentlichkeit" hinterlegt haben.

Optional -Schritt 3: Nachhaltigkeitsstrategie hinterlegen

Der Bearbeiter kann im Tab "*Nachhaltigkeitsstrategie*" zusätzliche Links hinterlegen.

1. **Strategie**: Der Link "Strategie" führt zu dem Work Item *Dokumentierte Informationen*. Es können dabei keine neuen *Dokumentierte Informationen* erstellt, sondern nur verlinkt werden.

   > Da nur Benutzer mit dem spezifischen Profil Dokumenteneigner *Dokumentierte Informationen* erstellen dürfen, kann der Bearbeiter bei der Notwendigkeit einer noch nicht vorhandenen "Strategie" eine Diskussion im "*Diskussions*"-Tab beginnen.

2. **Maßnahme**: Neben der "Strategie" sollten auch *Maßnahmen* gesetzt und hinterlegt werden. Sie sollen dazu beitragen die aktuelle *Auswirkungs-Wesentlichkeit* zu reduzieren oder zu optimieren.
3. **Ziele**: Zuletzt kann es Sinn machen nicht nur Maßnahmen zu definieren, sondern sich auch Ziele zu setzen, wie mit der *Auswirkungs-Wesentlichkeit* in Zukunft umgegangen werden soll.
4. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Überprüfung" durchgeführt.

Zurück zu dem Schritt Assessor - Bewertung durchführen & bewerten oder weiter mit Assessor - Auswirkungs-Wesentlichkeit überprüfen & freigeben.

2.3.7 Doppelte Wesentlichkeitsanalyse - Bewertung abschließen & überprüfen

Doppelte Wesentlichkeitsanalyse - Bewertung abschließen & überprüfen

Nachdem der Assessor das Assessment "Doppelte Wesentlichkeitsanalyse" für ein Asset gestartet und im Assessment zu den einzelnen GRC Framework Elementen Bewertungen durchgeführt hat wird er für jede Bewertung noch eine Überprüfung durchführen.

Schritt 1: Work Items in Bewertung in richtigen Status bringen

Der Assessor hat im Rahmen der Bewertung einzelner GRC Framework Elemente zu entscheiden, ob das Unternehmen auf die Umwelt wirkt oder die Umwelt auf das Unternehmen.

Sollte zumindest eines der beiden Fragen mit "Ja" beantwortet worden sein muss verpflichtend ein Work Item entweder des Typen *Finanzielle Wesentlichkeit* und/oder *Auswirkungs-Wesentlichkeit* erstellt werden.

Sobald die *Finanzielle Wesentlichkeit* und/oder *Auswirkungs-Wesentlichkeit* sich jeweils im Status "In Überprüfung" befinden kann ein Statusübergang in der Bewertung des Assessments in "In Überprüfung" vorgenommen werden.

Schritt 2: Bewertung überprüfen

Der Assessor hat nach dem erfolgreichen Statusübergang in "In Überprüfung" zwei Angaben zu hinterlegen.

Dem Assessor wird eine Heatmap (standardmäßig 5x5 Größe) angezeigt. Dabei wird ihm mittels eines Icons für das Ergebnis (R) angezeigt, wie die durchschnittlichen Ergebnisse für die nicht-finanzielle und finanzielle Auswirkung für das Asset im Zusammenhang mit einem GRC Framework Element ausgegangen ist.

> Für die Berechnung werden jeweils aus allen Work Items von z.B. *Finanzielle Wesentlichkeit* die Ergebnisse herangezogen und ein Mittwelwert in der Y-Achse der Heatmap eingetragen. Dasselbe Verhalten ist bei der nicht-finanziellen Auswirkung hinterlegt.

Sollte dieser berechnete Vorschlag von BIC GRC nicht mit der Realität übereinstimmen muss der Assessor mittels des zweiten Icons für die Expertenschätzung (E) (1) eine Übersteuerung zu einem anderen Punkt in der Heatmap vornehmen oder er setzt den gleichen Wert wie das Ergebnis ausgefallen ist. Jedenfalls muss der Assessor das Icon (E) setzen, um die Bewertung abschließen zu können. Weiter muss er eine "Beschreibung der Endeinschätzung" (2) angeben.

> Die Angaben sind notwendig, um den Fortschritt des ganzen Assessments nachverfolgen zu können.

Schritt 3: Überprüfung abschließen

Diesen Vorgang muss er für jedes Element des GRC Framworks wiederholen, bis alle Bewertungen auf der linken Seite das Icon  vorweisen können.

In BIC GRC gibt es ein Dashboard für die Auswertung der Bewertungen unter dem Menüpunkt **Dashboards >> Doppelte Wesentlichkeitsanalyse**.

Wenn alle Überprüfungen abgeschlossen wurden kann der Assessor mit dem nächsten Schritt Assessor - Assessment abschließen & auswerten fortfahren.

2.3.8 Doppelte Wesentlichkeitsanalyse - Assessment abschließen & auswerten

Doppelte Wesentlichkeitsanalyse - Assessment abschließen & auswerten

Nachdem der Assessor das Assessment "Doppelte Wesentlichkeitsanalyse" für ein Asset gestartet sowie alle Bewertungen überprüft und abgeschlossen wurden kann mit dem letzten Schritt begonnen werden - das Assessment abschließen.

Schritt 1: Assessment abschließen

Um das Assessment abschließen zu können müssen alle Bewertungen der Phase "Identifikation der Auswirkung" abgeschlossen sein. Eine gutes Merkmal um das zu erkennen ist, wenn alle GRC Framework Elemente links das Icon haben.

> Das Assessment schließen kann dabei nur der Assessor.

Das Assessment kann über zwei Wege abgeschlossen werden.

1. Abschluss in der Phase

Der Assessor kann direkt in der Phase einen Statuswechsel vornehmen.

> Der Status wird nur angezeigt, wenn die Phase abgeschlossen ist. Ansonsten ist der Status Read Only.

2. Abschluss im Assessment Typen

Neben der Phase kann der Assessor auch über den Assessment Typen das Assessment schließen. Über das Icon in der Liste kann der Assessor den Assessment Typen öffnen und den Statusübergang vornehmen.

Schritt 2: Ergebnisse auswerten

In BIC GRC gibt es ein Dashboard für die Auswertung der Bewertungen zur "Doppelte Wesentlichkeitsanalyse" unter dem Menüpunkt **Dashboards >> Doppelte Wesentlichkeitsanalyse**.

Schritt 3: Weiteres Vorgehen

Das Assessment kann jederzeit wieder geöffnet werden vom Assessor. Anschließend muss manuell auch wieder die Phase geöffnet werden, um sie überprüfen zu können.

> Der Assessor automatisch mittels Scheduler informiert, wenn eine neue Bewertung erforderlich ist.

2.3.9 Doppelte Wesentlichkeitsanalyse - Assessment überprüfen & neubewerten

Doppelte Wesentlichkeitsanalyse - Assessment überprüfen & neubewerten

Nachdem das Enddatum eines Assessments erreicht ist bekommt der Assessor eine Notifikation zugesendet, dass eine Überprüfung notwendig ist.

Schritt 1: Navigation zu spezifischen Assessment

1. Öffnen über Notifikation

Der Assessor bekommt automatisch von BIC GRC eine E- Mail zugesendet, sobald eine Überprüfung des Assessments *Doppelte Wesentlichkeitsanalyse*auf einem Assets durchgeführt werden muss. Der Link zu dem spezifischen Assessment befindet sich in der Notifikation.

2. Öffnen über Assessment Ansicht

Der Assessor navigiert zu einem Assessment des Types "Doppelte Wesentlichkeitsanalyse" über die Menüleiste **Assessment >> Doppelte Wesentlichkeitsanalyse**.

Schritt 2: Assessment öffnen

2. Öffnen im Assessment Typen

Neben der Phase kann der Assessor über den Assessment Typen das Assessment öffnen. Über das Icon in der Liste kann der Assessor den Assessment Typen öffnen und den Statusübergang vornehmen.

1. Öffnen in der Phase

Der Assessor kann direkt in der Phase einen Statuswechsel des "Gesamtstatus" des Assessments vornehmen.

Schritt 3: Assessment öffnen

Wenn das Assessment geöffnet wird wechselt der Status der Phase von Abgeschlossen in "In Überprüfung.

Wenn sich die Phase im Status "In Überprüfung" befindet erscheinen dem Assessor zwei neue Attribute. Im ersten hat er anzugeben, ob sich etwas an der Bewertung für das GRC Framework Element in Kontext des Assets verändert hat. Im zweiten wird ein Datum automatisch von BIC GRC gesetzt, wenn ein Statusübergang gemacht wird.

Schritt 4: Weiteres Vorgehen

Sollte eine Bewertung wieder neu geöffnet werden müssen, weil die Bewertung nicht mehr dem aktuellen Stand entspricht, kann der Assessor einen Statusübergang der Bewertung zu in "In Bewertung" durchführen. Anschließend kann er Änderungen wie bei der Erstbewertung vornehmen. Der Workflow beginnt von neuem. Siehe mehr unter Assessor - Bewertung durchführen & bewerten.

Sollte es für eine spezifische Bewertung keine Änderungen geben kann er einen Statusübergang in "Abgeschlossen" durchgeführt werden.

> Bevor das Assessment wieder in den Status "Abgeschlossen" geschalten werden kann muss noch im Assessments Typen ein neues Enddatum gesetzt werden.

2.3.10 Finanzielle Wesentlichkeit überprüfen & freigeben

Der Assessor wird nach der Bewertung einer *Finanzielle Wesentlichkeit* mittels Notifikation informiert.

> Sollte der Assessor die Bewertung selber durchgeführt haben kann er die nachfolgenden Schritte überspringen und direkt den Statusübergang zu in "Aktiv" durchführen.

Schritt 1: Navigation zu Finanzielle Wesentlichkeit

Der Assessor bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Finanzielle Wesentlichkeit* erstellt wurde und ein Statusübergang erfolgt ist. Der Link zu der spezifischen *Finanzielle Wesentlichkeit* befindet sich in der Notifikation.

Schritt 2: Finanzielle Wesentlichkeit überprüfen

Der Assessor hat in der bewerteten *Finanzielle Wesentlichkeit* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Finanzielle Wesentlichkeit* in Bezug auf Bewertung und optional Nachhaltigkeitsstrategie richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss der *Finanzielle Wesentlichkeit* aus Sicht des Assessors erneut bewertet werden, kann der Assessor einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "In Bewertung" durchführen.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben des Bearbeiter DS passen, kann der Assessor weiter in den Status "Aktiv" schalten.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.3.11 Auswirkungs-Wesentllichkeit überprüfen & freigeben

Der Assessor wird nach der Bewertung einer *Auswirkungs-Wesentlichkeit* mittels Notifikation informiert.

> Sollte der Assessor die Bewertung selber durchgeführt haben kann er die nachfolgenden Schritte überspringen und direkt den Statusübergang zu in "Aktiv" durchführen.

Schritt 1: Navigation zu Auswirkungs-Wesentllichkeit

Der Assessor bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Auswirkungs-Wesentlichkeit* erstellt wurde und ein Statusübergang erfolgt ist. Der Link zu der spezifischen *Auswirkungs-Wesentlichkeit* befindet sich in der Notifikation.

Schritt 2: Auswirkungs-Wesentlichkeit überprüfen

Der Assessor hat in der bewerteten *Auswirkungs-Wesentlichkeit* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Auswirkungs-Wesentlichkeit* in Bezug auf Bewertung und optional Nachhaltigkeitsstrategie richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss der *Auswirkungs-Wesentlichkeit* aus Sicht des Assessors erneut bewertet werden, kann der Assessor einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "In Bewertung" durchführen.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben des Bearbeiter DS passen, kann der Assessor weiter in den Status "Aktiv" schalten.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.4 Bearbeiter Risiko

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

Folgende vorbereitende Aufgaben hat der Bearbeiter Risiko:

- Bedrohung identifizieren & erstellen
- Schwachstelle identifizieren & erstellen
- Risikoszenario herleiten & erstellen
- Ziel definieren & erstellen
  - Zwischenziel definieren & erstellen

Folgende laufende Aufgaben hat ein Bearbeiter Risiko in BIC GRC:

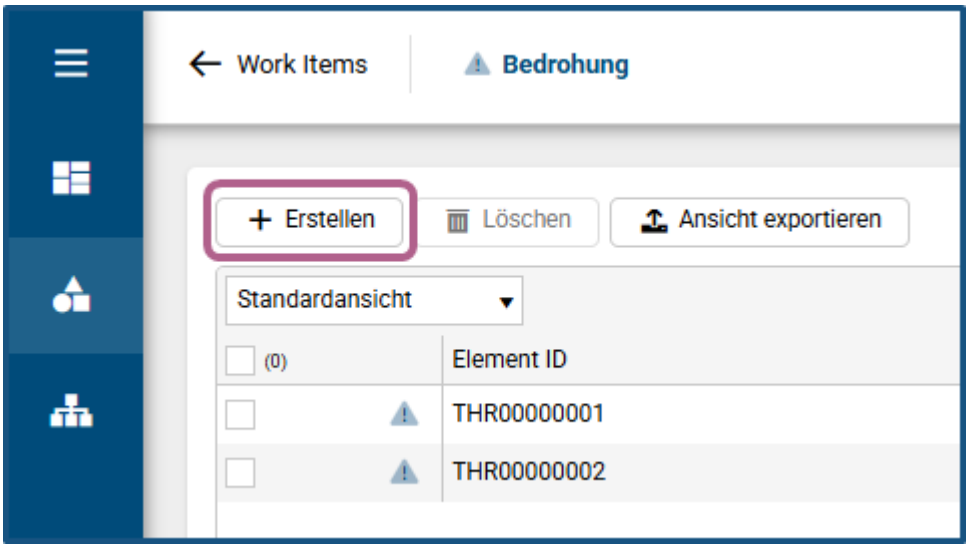
- Nachhaltigkeitsrisiko identifizieren & erstellen
- Nachhaltigkeitsrisiko ergänzen & analysieren
- Nachhaltigkeitsrisiko beurteilen & bewerten
- Abhängige Risiken herleiten & erstellen
- Maßnahmenbewertung ableiten & erstellen
- Maßnahmen identifizieren & erstellen
- Kontrolle ableiten & erstellen
- Ziel umsetzen & überprüfen

2.4.1 Bedrohung identifizieren & erstellen

Für die Herleitung eines *Risikoszenarios* sollte vorab eine passende *Bedrohung* erstellt werden.

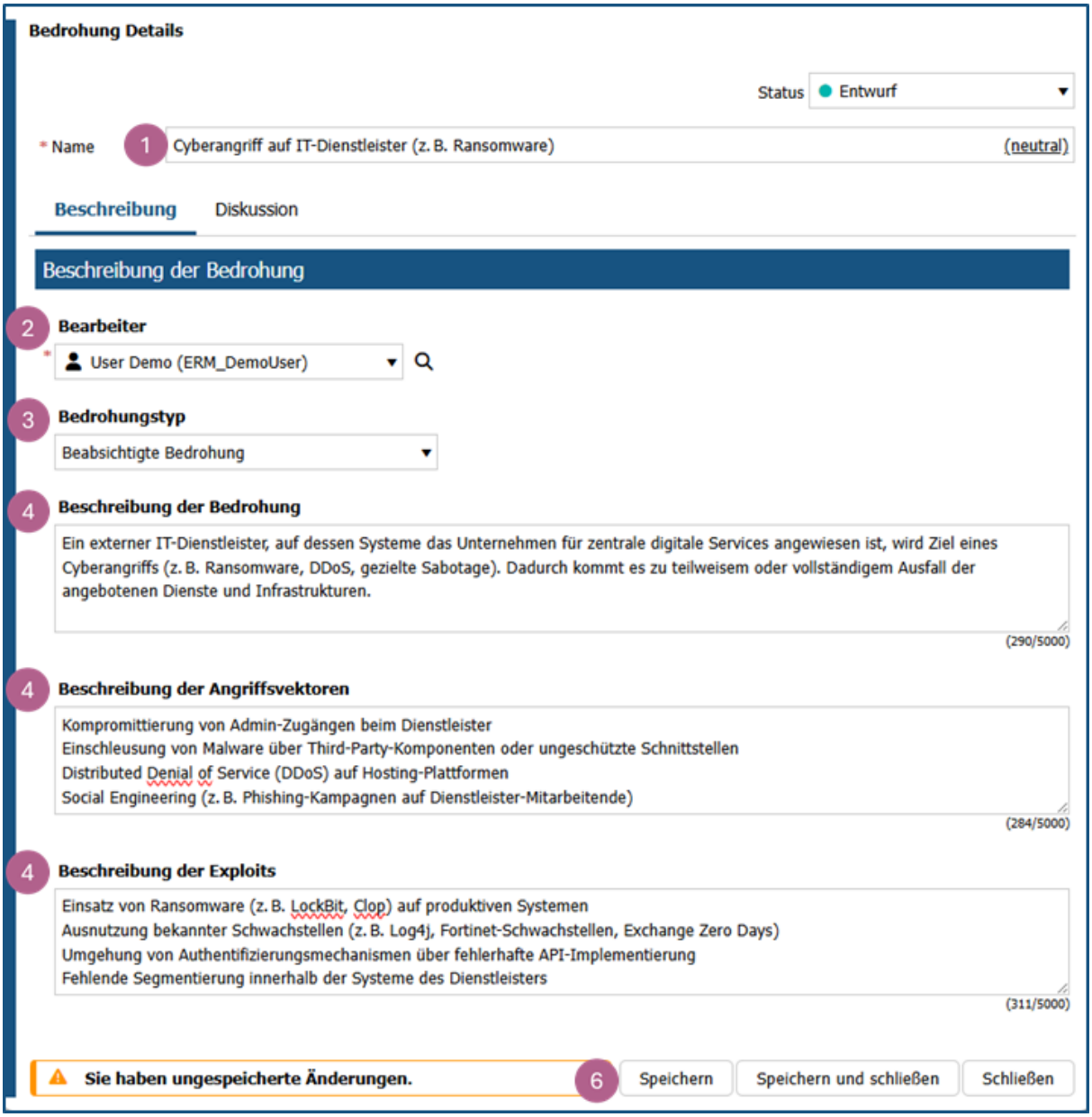
Schritt 1: Bedrohung erstellen

Der Bearbeiter Risiko navigiert über die Menüleiste zu **Work Items >> Bedrohung >> "Erstellen"**.



Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: Details hinterlegen



1 **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Bedrohung* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht den *Bedrohung* einzigartig.

2 **Bearbeiter**: Es muss ein Bearbeiter eingetragen werden, der für die Bearbeitung der *Bedrohung* verantwortlich ist.

> Es werden unabhängig von der Perspektive nur Benutzer mit dem Benutzerprofil "Bearbeiter Risiko" vorgeschlagen.

> Wenn ein anderer Benutzer eingetragen wird, wird dieser mittels einer Notifikation benachrichtigt.

3 **Bedrohungstyp**: Der Bearbeiter kann zwischen drei Bedrohungstypen wählen:

- Natürliche Bedrohung
- Unabsichtliche Bedrohung
- Beabsichtigte Bedrohung

4 **Beschreibungen**: Nach der Einordnung kann die *Bedrohung* beschrieben werden. Dem Bearbeiter stehen drei verschiedene Beschreibungsfelder zur Verfügung, um die *Bedrohung* so ausführlich wie möglich zu beschreiben.

Anschließend sollte der Bearbeiter Risiko das Work Item zum ersten Mal speichern.

5 **Dokumente**: Sobald der Bearbeiter Risiko erstmalig gespeichert hat kann er bei Bedarf Dokumente ergänzen.

> Handelt es sich um eine Datei kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend automatisch im Attributsfeld verlinkt.

6 **Statuswechsel**: Nachdem der Bearbeiter alle Eingaben vorgenommen hat kann er einen Statusübergang zu in "Aktiv" vornehmen.

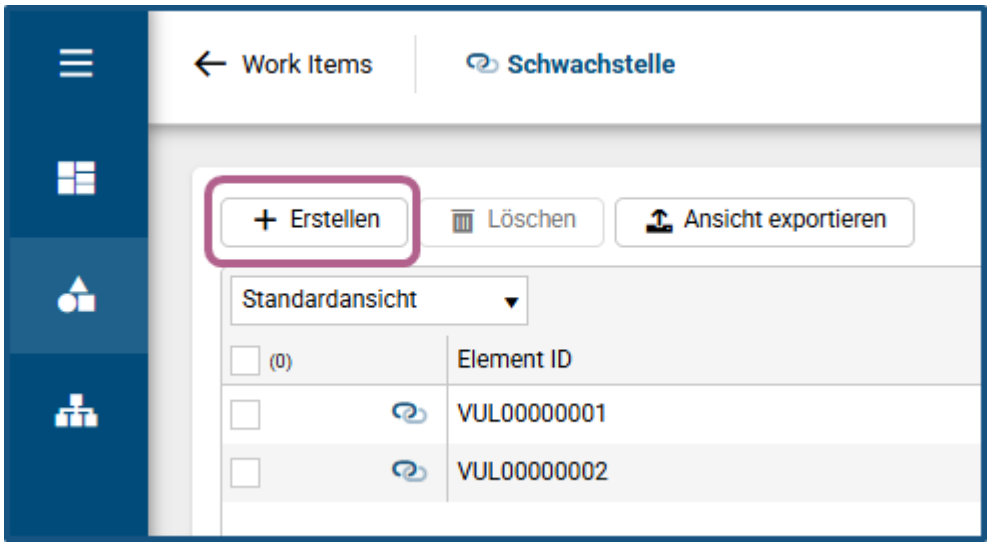
> Es wird niemand über die Erstellung und "Aktivierung" der *Bedrohung* informiert.

2.4.2 Schwachstelle identifizieren & erstellen

Für die Herleitung eines *Risikoszenarios* sollte vorab - neben einer *Bedrohung* - eine *Schwachstelle* erstellt werden.

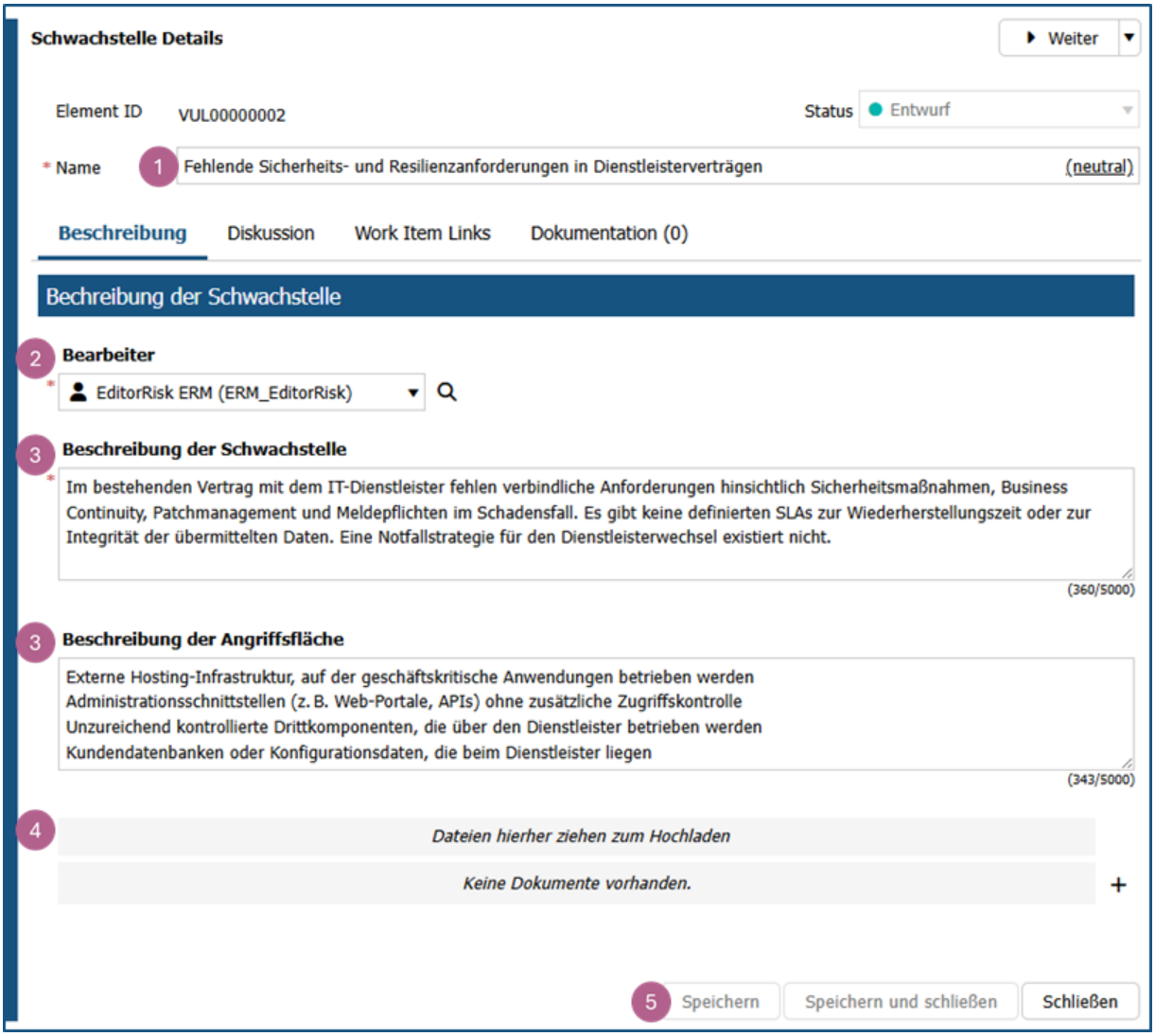
Schritt 1: Schwachstelle erstellen

Der Bearbeiter Risiko navigiert über die Menüleiste zu **Work Items >> Schwachstelle >> "Erstellen"**.



Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: Details hinterlegen



1 **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Schwachstelle* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht die *Schwachstelle*einzigartig.

2 **Bearbeiter**: Es muss ein Bearbeiter eingetragen werden, der für die Bearbeitung der *Schwachstelle* verantwortlich ist.

> Es werden unabhängig von der Perspektive nur Benutzer mit dem Benutzerprofil "Bearbeiter Risiko" vorgeschlagen.

> Wenn ein anderer Benutzer eingetragen wird, wird dieser mittels einer Notifikation benachrichtigt.

3 **Beschreibungen**: Nach der Einordnung kann die *Schwachstelle* beschrieben werden. Dem Bearbeiter stehen zwei verschiedene Beschreibungsfelder zur Verfügung, um die *Schwachstelle* so ausführlich wie möglich zu beschreiben.

4. Anschließend sollte der Bearbeiter Risiko das Work Item zum ersten Mal speichern.

   Dokumente: Sobald der Bearbeiter Risiko erstmalig gespeichert hat kann er bei Bedarf Dokumente ergänzen.

   > Handelt es sich um eine Datei kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend automatisch im Attributsfeld verlinkt.

5. **Statuswechsel**: Nachdem der Bearbeiter alle Eingaben vorgenommen hat kann er einen Statusübergang zu in "Aktiv" vornehmen.

   > Es wird niemand über die Erstellung und "Aktivierung" der *Schwachstelle* informiert.

2.4.3 Risikoszenario herleiten & erstellen

In BIC GRC ist es möglich Risiken herzuleiten. Hierzu kann der Bearbeiter Risiko das Work Item *Risikoszenario* einsetzen.

Schritt 1: Risikoszenario erstellen

Der Bearbeiter kann in BIC GRC an mehreren Stellen *Risikoszenarien* erstellen.

1. Erstellen über Dashboard "Gesamtübersicht Risikoszenario"

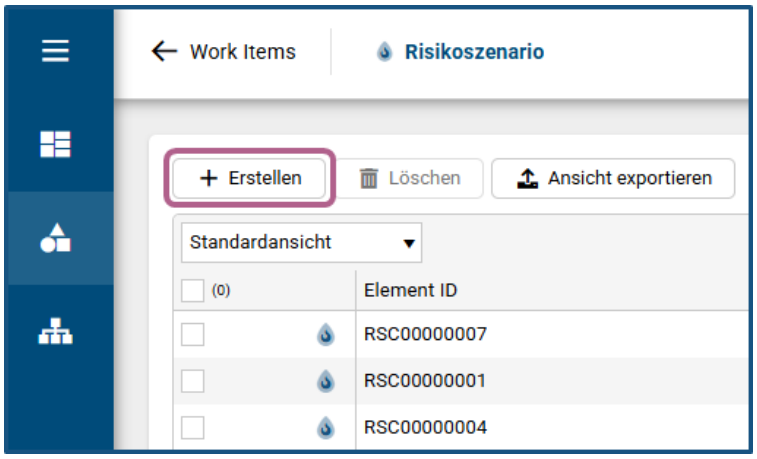
Der Bearbeiter Risiko navigiert über die Menüleiste zu **Dashboards >> Gesamtübersicht Risikoszenarien >> "Neues Risikoszenario"** .

Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Risikoszenario >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Risikoszenario* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht das *Risikoszenario* einzigartig.
2. **GRC Perspektive**: Der Bearbeiter kann ein oder mehrere GRC Perspektiven auswählen, die von diesem generischen *Risikoszenario* betroffen sein können.

> Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.

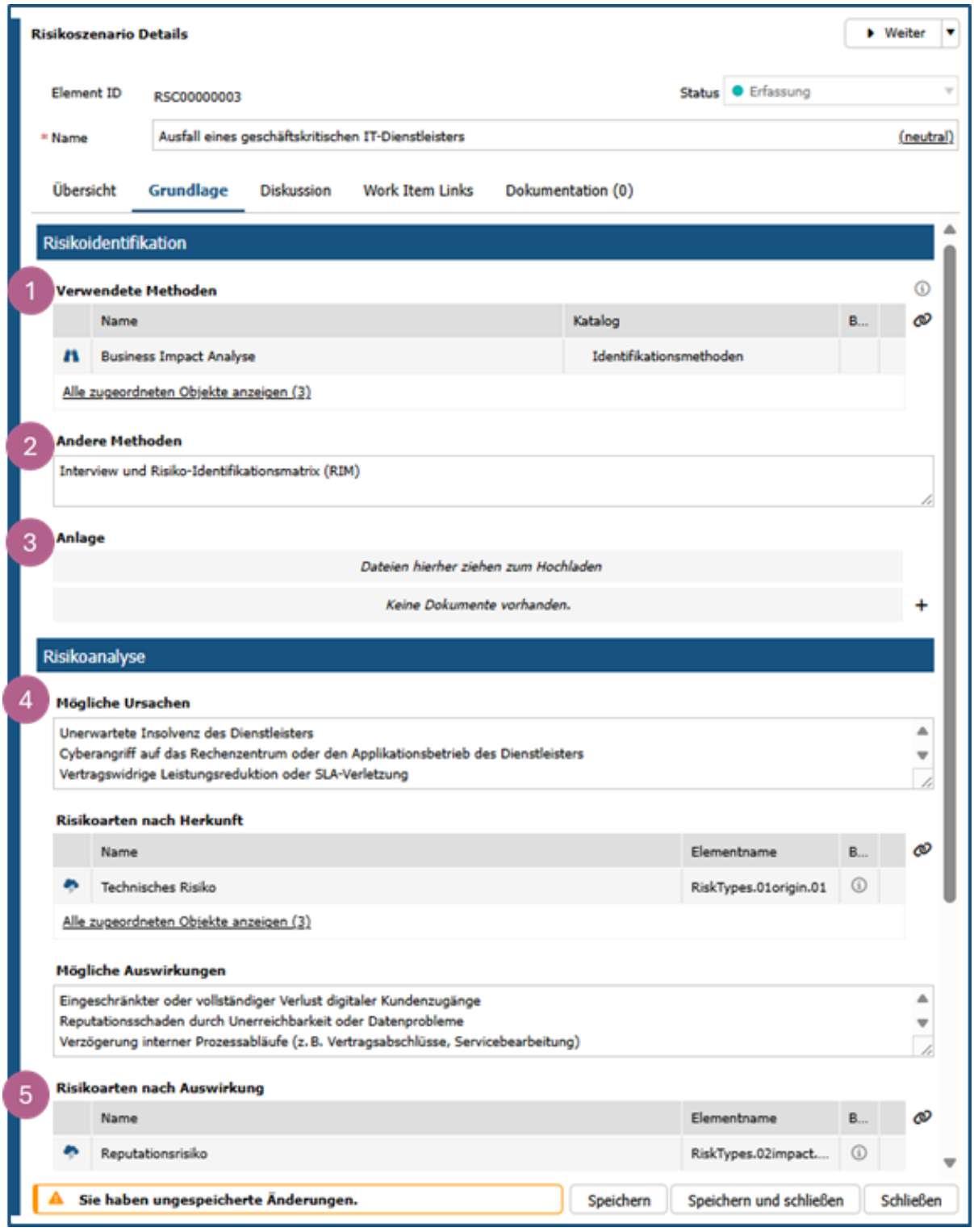
> Es ist möglich, dass durch die Aktivierung unterschiedlicher Module ergänzende Attribute angezeigt werden.

3. **Szenariobeschreibung**: Das *Risikoszenario* sollte so ausführlich wie möglich dokumentiert und beschrieben werden, sodass auch andere Perspektiven einen Zusammenhang erkennen können.
4. **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen kann das *Risikoszenario* erstmalig gespeichert werden

> Beim Speichervorgang wird der Ersteller automatisch in das Benutzerfeld "Bearbeiter" eingetragen.

Schritt 3: Grundlagen festlegen

Als nächsten Schritt sollte der Bearbeiter in den Tab "*Grundlagen*" wechseln, um weitere Informationen zu hinterlegen.



1 **Verwendete Methode**: Der Bearbeiter kann aus einem vorgegebenen GRC Framework wählen, mittels welcher Methode er das *Risikoszenario* hergeleitet hat.

> Zumeist werden *Risikoszenarien* durch gängige Identifikationsmethoden hergeleitet. Für eine bessere Übersicht, welche Methode die meisten oder wichtigsten *Risikoszenarien* hervorgebracht hat, kann diese Verknüpfung zwischen *Risikoszenario*

und GRC Framework hergestellt werden, die später auf beispielsweise Dashboards ausgewertet werden können.

2 **Andere Methode**: Falls in dem gepflegten GRC Framework keine geeignete Identifikationsmethode gefunden werden konnte, kann eine Methode im Textform angegeben werden.

3 **Anlage**: Als zusätzliche Information können an dieser Stelle beispielsweise Dokumente oder Memos hinterlegt werden.

Zum Beispiel die Meeting Minutes eines vorangegangenen Workshops.

4 **Ursache/Herkunft**: In der Risikoanalyse kann des Weiteren angegeben werden, welche Ursachen zu dem Risiko führen können. Dabei kann sowohl eine schriftliche Herleitung erfolgen, als auch eine Zuteilung mittels Link zu einem GRC Framework.

5 **Auswirkung**: Neben der Herkunft kann auch die Auswirkung des *Risikoszenarios* angegeben werden.

Dem Bearbeiter werden beim Verlinken zu den beiden passenden GRC Frameworks nur die Elemente des Frameworks angezeigt, wo der GRC Framework den passenden Tag zur GRC Perspektive hat.

Die Informationen der Ursache und Auswirkung (sowohl Text, als auch Verlinkung) kann von BIC GRC in ein aus dem *Risikoszenario* heraus erstelltes *Nachhaltigkeitsrisiko* übernommen werden. Die Informationen werden übernommen und angezeigt, wenn mittels der Konfiguration die Anzeige der Risikoanalyse im *Nachhaltigkeitsrisiko* erlaubt ist.

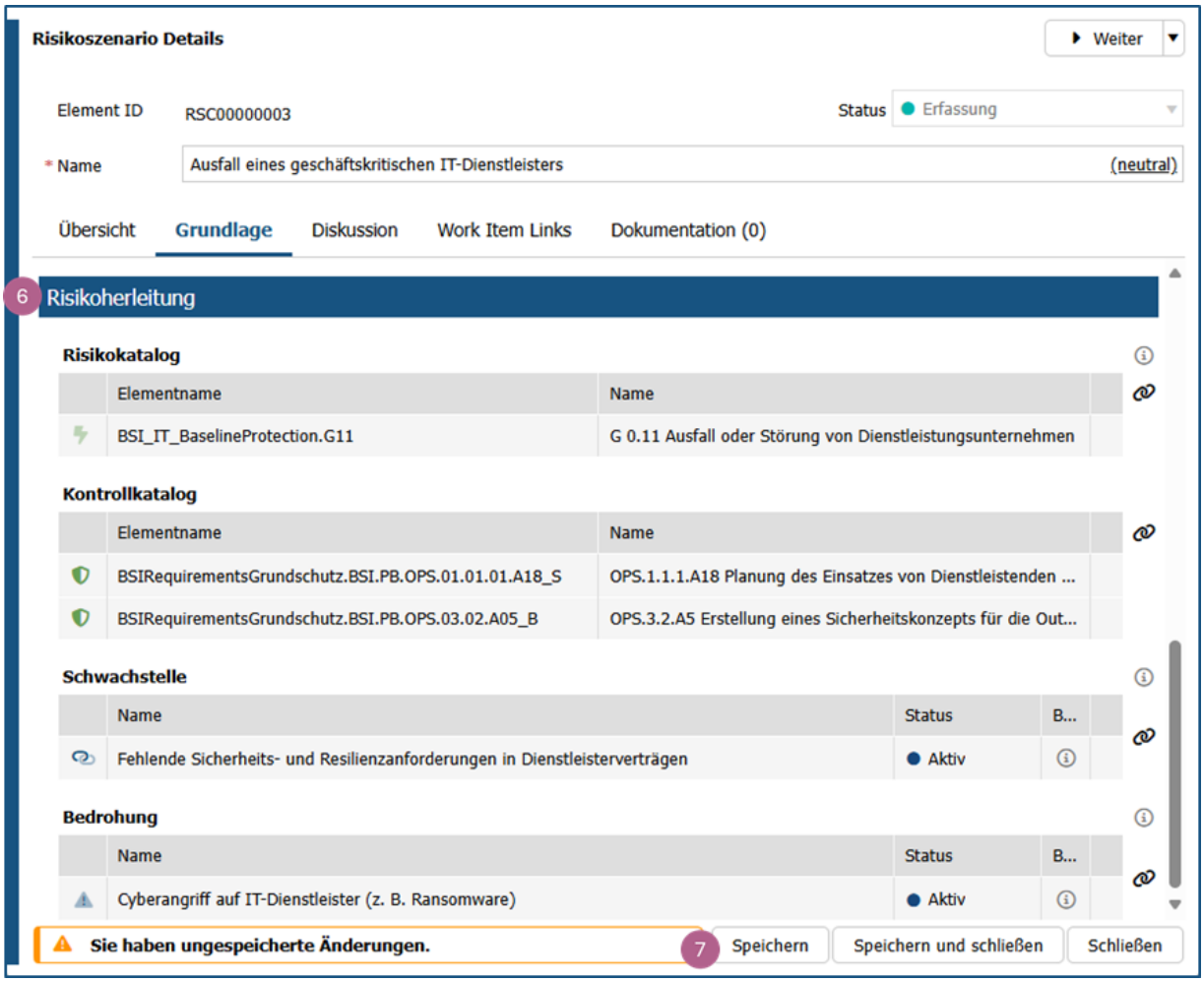
6 **Risikoherleitung**: Schlussendlich kann noch eine Zuordnung zu

- einem Risikokatalog oder
- einer Bedrohung und einer Schwachstelle

angegeben werden.

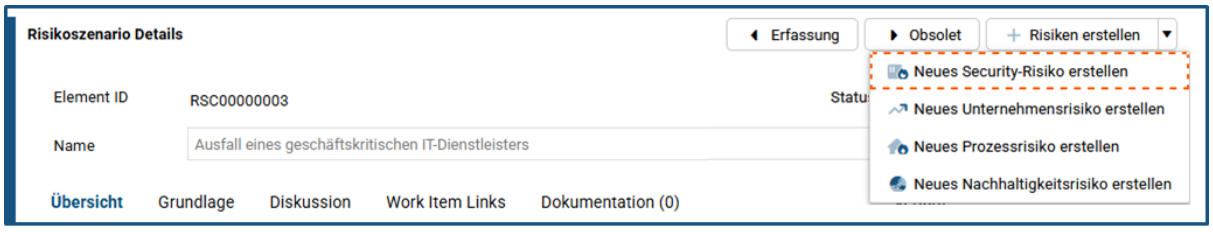
7 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

Es wird niemand über die Erstellung und "Aktivierung" des *Risikoszenarios* informiert.



Schritt 4: Weiteres Vorgehen

Sowohl Benutzer des Benutzerprofils Bearbeiter Risiko als auch Freigeber Risiko aus anderen GRC Perspektiven haben Zugang zu dem *Risikoszenario*. Alle Benutzer außer dem Bearbeiter Risiko haben nur Leserechte und keine Bearbeitungsrechte.



Sollten Anpassungen bzw. Ergänzungen für die jeweilige Perspektive notwendig sein kann dies mittels des "Diskussions"-Tabs besprochen werden.

Das *Risikoszenario* kann nach der Aktivierung von *Nachhaltigkeitsrisiken* verlinkt werden.

> Zusätzlich haben Bearbeiter und Freigeber anderer Perspektiven/Modulen die Möglichkeit, direkt aus dem *Risikoszenario* andere Risikotypen wie z.B. *Unternehmensrisiko-Risiko* zu erstellen. Für die Anzeige der Erstellung im rechten oberen Fenster muss allerdings die

Perspektive im *Risikoszenario* passen.

2.4.4 Ziel definieren & erstellen

In BIC GRC ist es möglich *Ziele* zu definieren und in unterschiedlichen Kontexten zu verknüpfen.

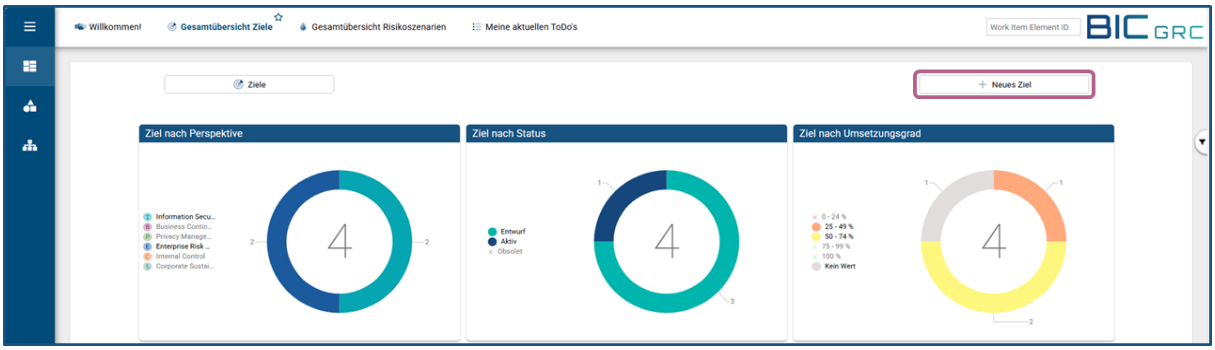
Hierzu kann der Bearbeiter Risiko das Work Item *Ziel* erstellen.

Schritt 1: Ziel erstellen

Der Bearbeiter kann in BIC GRC an mehreren Stellen *Ziele* erstellen.

1. Erstellen über Dashboard "Gesamtübersicht Ziele"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Gesamtübersicht Ziele >> "Neues Ziel"**.



Die Erstellung eines neuen *Ziels* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

2. Erstellen über Nachhaltigkeitsrisiko

Der Bearbeiter Risiko kann aus dem *Nachhaltigkeitsrisiko* heraus ein *Ziel*erstellen. Die Option wird ihm im Status "Entwurf", "Bewertung" und "Behandlung" im rechten oberen Fenster angezeigt.

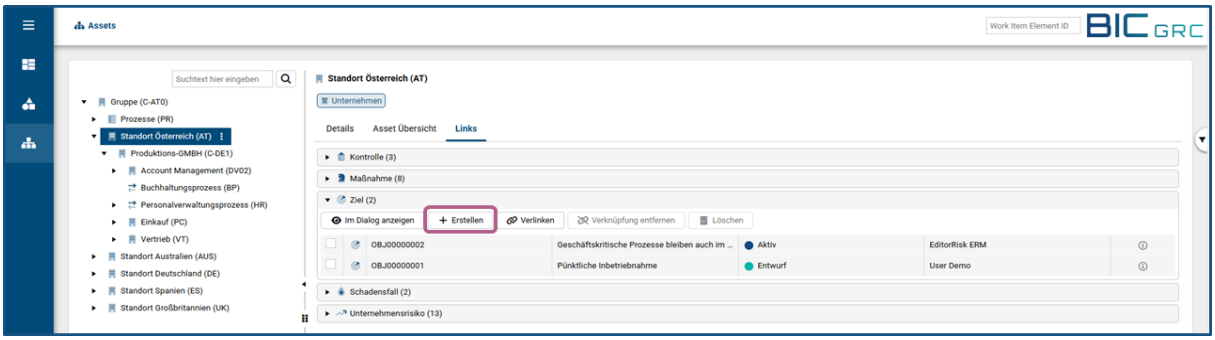
Ein neues Fenster öffnet sich anschließend automatisch.

Ein neues Fenster öffnet sich anschließend automatisch.

3. Erstellen über Asset Übersicht "Links"

Der Bearbeiter navigiert über die Menüleiste zu **Assets >> Auswahl einer Unternehmenseinheit >> Links >> Öffnen des Reiters "Ziel" >> "Erstellen"**

Die Erstellung eines neuen *Ziels* wird durch einen Button "Erstellen" in der Mitte des Fensters durchgeführt.

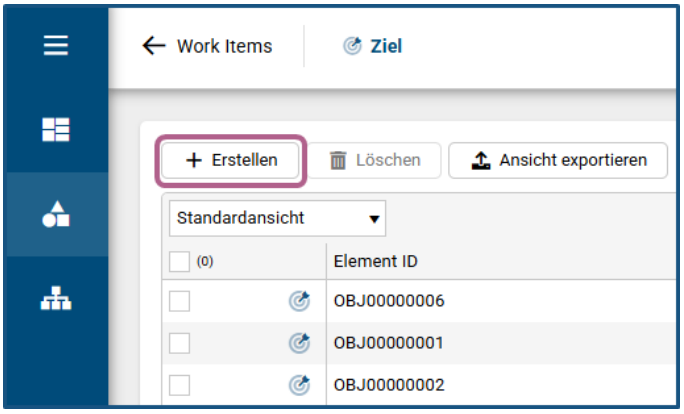


Ein neues Fenster öffnet sich anschließend automatisch.

4. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Ziel >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Zielsetzung definieren

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Ziel* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht das *Ziel* einzigartig.
2. **GRC Perspektive**: Der Bearbeiter kann ein oder mehrere GRC Perspektiven auswählen, in denen er eine Berechtigung für die Erstellung besitzt.

> Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.

3. **Beschreibung**: Das *Ziel* sollte so ausführlich wie möglich dokumentiert und beschrieben werden, sodass auch andere Perspektiven einen Kontext bzw. Zusammenhang erkennen können.
4. **Scope**: Das *Ziel* muss einem Scope zugewiesen werden.

> Dabei darf der Scope nur eine Organisationseinheit oder ein Primary Asset sein.

> Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer keine Rolle auf dem Asset zugewiesen, das er verlinken möchte. Mittels des Work Items

Berechtigungsanfrage kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

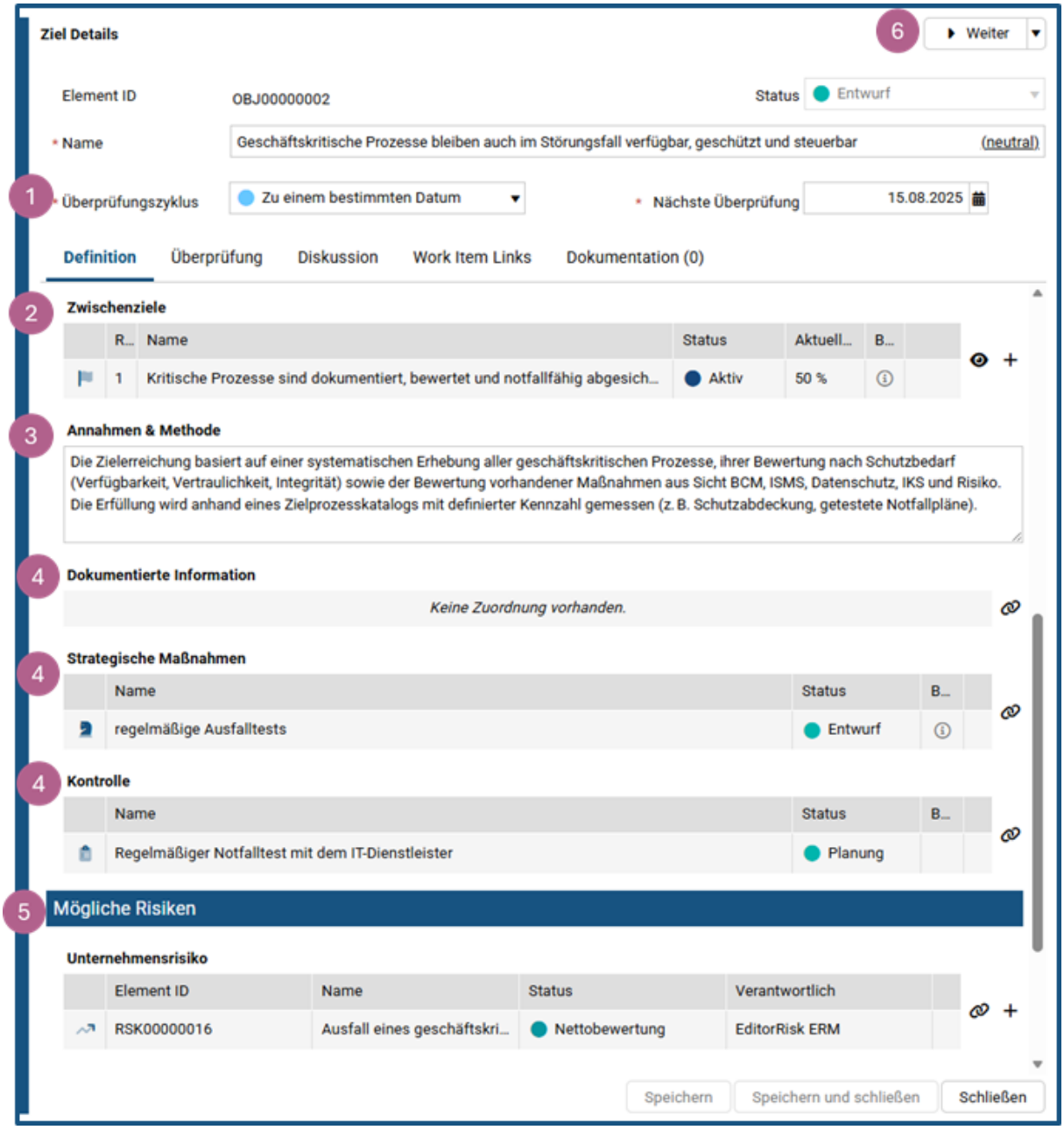
5 SMART: Der Bearbeiter kann das Ziel nach der SMART- Definition erstellen. Alle Komponenten sind im Tab vorhanden und wie folgt zu interpretieren:

- Spezifisch: Wird mittels dem Textfeld "Beschreibung" festgelegt
- Messbar: Wird mittels der passenden Attribute mit einer konkreter "Kennzahl" sowie einem "Zielwert" festgelegt
- Angemessen: Wird mittels der Checkbox "Zielsetzung ist angemessen und realistisch" festgestellt
- Realistisch: Wird mittels der Checkbox "Zielsetzung ist angemessen und realistisch" festgestellt
- Terminiert: Wird mittels des "Zieldatums" festgelegt

6 Speichervorgang: Nach der Hinterlegung der notwendigen Informationen, kann das *Ziel* erstmalig gespeichert werden

Beim Speichervorgang wird der Ersteller automatisch als "Verantwortlicher" eingetragen.

Schritt 3: Weitere Informationen hinterlegen



1 **Überprüfungszyklus**: Der Bearbeiter muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft ein *Ziel* zurück in den Status "Entwurf" geschalten wird, um das *Ziel* in regelmäßigen Zeitabständen zu evaluieren.

> Das Attributsfeld "Datum der Überprüfung" wird automatisch von BIC GRC gesetzt.

2 **Zwischenziele**: Der Bearbeiter kann mittels des passenden Work Items *Zwischenziele* definieren.

> Diese *Zwischenziele* sollen dem Benutzer helfen das *Ziel* besser zu strukturieren und

auch Zwischenergebnisse vorweisen zu können.

Mehr Informationen unter Bearbeiter Risiko - Zwischenziel definieren & erstellen.

3. **Annahmen & Methode**: Es können zusätzliche Informationen hinterlegt werden, die für den Werdegang und die zugrundeliegende Methode des *Ziels* interessant sind.
4. **Kontext**: Der Bearbeiter kann einen Kontext zu *Dokumentierten Informationen*, (Strategischen) *Maßnahmen* und *Kontrollen* herstellen.

> Sowohl *Dokumentierte Informationen*, als auch (Strategische) *Maßnahmen* und *Kontrollen* können nur verlinkt und nicht aus einem *Ziel* erstellt werden.

5. **Mögliche Risiken**: Es kann ein Bezug zu Risiken in BIC GRC hergestellt werden.

> Wenn aus einem Risikotyp ein *Ziel* erstellt wird, wird der Link zu dem jeweiligen Risiko automatisch befüllt.

> Es werden nur Verlinkungen zu Risiken angezeigt, deren Typ mittels der Modulaktivierung verfügbar sind.

6. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

> Die Freigabe eines Zieles ist nicht vorgesehen.

Schritt 4: Update durchführen

Der Bearbeiter sollte das *Ziel* regelmäßig dahingehend überprüfen, ob das *Ziel*in seiner Art und Weise noch realistisch und korrekt ist.

Um dies in regelmäßigen Abschnitten zu überprüfen, unterstützt das Feld "Nächste Überprüfung". Zwei Wochen vor dem erreichen des Datums bekommt der Bearbeiter eine Notifikation automatisch zugesendet, die ihn an eine bevorstehende Überprüfung erinnert.

An dem Tag der "Nächsten Überprüfung" wird das *Ziel* im Status "Aktiv" in den Status "Entwurf" geschalten und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.

> Das Datum wird nach dem Statuswechsel automatisch neu gesetzt abhängig von der Zeitangabe in "Überprüfungszyklus".

> Wenn das *Ziel* einer der Überprüfungszyklen "Alle ... Tage", "Anlassbezogen", "Täglich" oder "Wöchentlich" hat, wird der Status nicht automatisch zurückgesetzt und der Bearbeiter wird nicht über einen Statusübergang mittels Notifikation benachrichtigt.

2.4.5 Zwischenziel definieren & erstellen

Häufig kommt es vor, dass *Ziele* nicht in einem Schritt oder einem Jahr abgehandelt und erreicht werden können. Daher macht es Sinn *Ziele* mittels *Zwischenzielen* zu strukturieren und einzelne Schritte zu setzen, um schlussendlich das Gesamtziel zu erreichen.

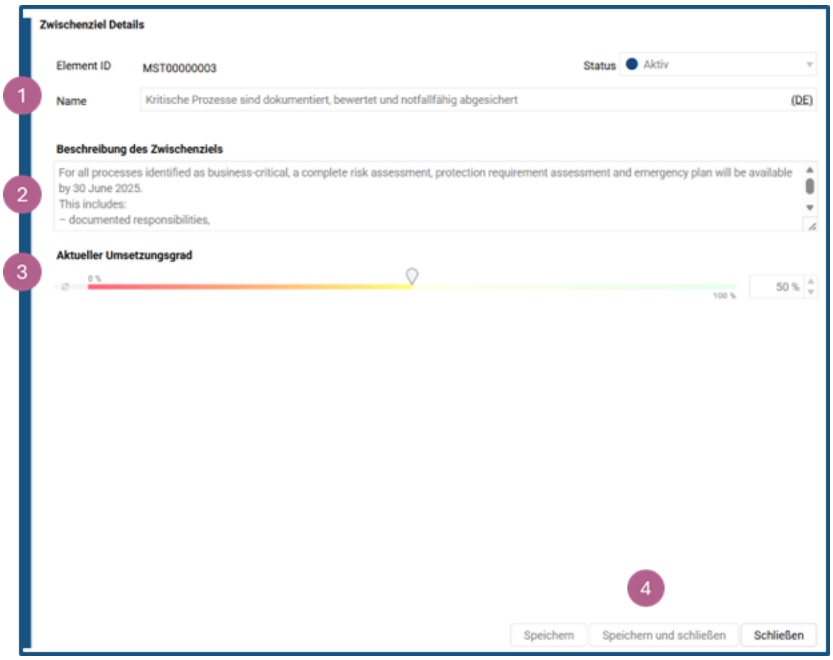
Schritt 1: Zwischenziel erstellen

Ein *Zwischenziel* kann nur mittels Erstellung aus dem Work Item *Ziel* durch den verantwortlichen Bearbeiter erfolgen.

Für die Erstellung wird im Tab "*Definition*" im Abschnitt *Zielsetzung* durch das Icon + ein neues *Zwischenziel* erstellt.

> Das *Zwischenziel* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des Work Items *Ziels*.

Schritt 2: Zwischenziel definieren



1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Zwischenziel*erfolgen.
2. **Beschreibung des Zwischenziels**: Der Bearbeiter sollte das *Zwischenziel* so ausführlich wie möglich beschrieben. Dafür kann jede Information hilfreich sein, die sicherstellt, dass das *Zwischenziel* für die Erreichung des Ziels sachdienlich ist.
3. **Aktueller Umsetzungsgrad**: Mittels Slider oder direkter Eingabe kann der Bearbeiter festlegen, wie weit das *Zwischenziel* in der Umsetzung ist.

> Der Wert kann zwischen 0 - 100% liegen.

> Bei jeder Änderung im *Zwischenziel* wird das *Ziel* automatisch geupdated, sodass keine redundanten Informationen zwischen den Work Items sind.

4 **Speichern & Schließen**: Nach dem Klick auf den Button "Speichern" muss der Bearbeiter einen Rang angeben. Dieser Rang bestimmt in welcher Reihenfolge die einzelnen *Zwischenziele* im Ablauf abgearbeitet werden sollen, sodass sich einzelne Schritte nicht zuvorkommen.

> Sollte sich der Rang später ändern oder ein neues *Zwischenziele* hinzukommen, berechnet BIC GRC die Reihenfolge neu, abhängig davon wo der neue Rang eingegeben worden ist.

Nach dem ersten Speichervorgang landet der Bearbeiter automatisch im Status "Aktiv".

> Anders als in anderen "Aktiv"- Status kann der Bearbeiter noch Änderungen vornehmen.

> Sollte das *Ziel* in den Status "Obsolet" geschalten werden wird auch das *Zwischenziel* automatisch in den Status "Obsolet" gesetzt.

> **Nach dem Speichervorgang kann der Bearbeiter das Work Item schließen und mit Ziel definieren & erstellen fortfahren.**

2.4.6 Nachhaltigkeitsrisiko identifizieren & erstellen

Nachdem ein Risiko in dem Modul Corporate Sustainability identifiziert wurde kann ein neues Work Item *Nachhaltigkeitsrisiko* vom Bearbeiter Risiko erstellt werden.

Schritt 1: Nachhaltigkeitsrisiko erstellen

Der Bearbeiter kann in BIC GRC an mehreren Stellen *Nachhaltigkeitsrisiken* erstellen.

1. Erstellen über Dashboard "Nachhaltigkeitsrisiko "

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Nachhaltigkeitsrisiko >> "Neues Nachhaltigkeitsrisiko "**

Die Erstellung eines neuen *Nachhaltigkeitsrisikos* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Nachhaltigkeitsrisiko >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Nachhaltigkeitsrisiko* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Nachhaltigkeitsrisiko* einzigartig.
2. **Risikozuordnung**: Verpflichtende Eingaben sind unter dem Abschnitt "Risikozuordnung" zu machen: Einerseits ist eine Verlinkung mittels des Icons  zu einer "Organisationseinheit" notwendig, wobei vorselektiert Organisationseinheiten angezeigt werden, bei denen der Bearbeiter Berechtigungen hat.

   > Wird das *Nachhaltigkeitsrisiko* über "2. Erstellen über Asset Übersicht Links" erstellt, wird der Link zur Organisationseinheit automatisch gesetzt von BIC GRC.

   > Durch einen hinterlegten Filter müssen der Bearbeiter als auch der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

   Zusätzlich muss eine Zuordnung  zu einer Kategorie des "ESRS Topics" vorgenommen werden.

   > Es wird zusätzlich noch ein Link "Prozessrisiko" angezeigt, aus dem aber keine Work Items erstellt oder verlinkt werden können. Dieser Link würde sich nur automatisch befüllen, wenn der Zentrale Risikomanager aus dem *Prozessrisiko* ein *Nachhaltigkeitsrisiko* erstellt.
3. **Risikobeschreibung**: Anschließend ist eine Beschreibung des *Nachhaltigkeitsrisikos* zu hinterlegen, wobei auch Informationen zu Ursache und Wirkung interessant sein können. Alle User, die im Workflow des *Nachhaltigkeitsrisikos* nachgelagert sind, orientieren sich an dieser Beschreibung, daher sollte sie so viele notwendige Informationen und Daten wie möglich enthalten.
4. **Risikoszenario**: Wird das *Nachhaltigkeitsrisiko* aus einem Szenario abgeleitet wird dieser Link automatisch bei der Erstellung aus dem Work Item *Risikoszenario* übernommen. Andernfalls kann der Bearbeiter auch ohne direkte Herleitung ein *Risikoszenario* verlinken.

   > Es ist nicht vorgesehen *Risikoszenarien* aus einem *Nachhaltigkeitsrisiko* zu erstellen. *Risikoszenarien* sollten schon feststehen.

5 **Verantwortliche Personen**: Der Bearbeiter hat einen "Bearbeiter Risiko" zu nominieren, der die Bewertung des *Nachhaltigkeitsrisikos* durchführt, und einen "Freigeber Risiko", der für die Freigabe des *Nachhaltigkeitsrisikos* verantwortlich ist.

> Sollte der Bearbeiter gleichzeitig der Ersteller sein, kann er sich selber eintragen. Dadurch, dass ein *Nachhaltigkeitsrisiko* allerdings auch von anderen Usern erstellt werden kann, ist dieses Attribut nicht vorausgefüllt.

> Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer keine Rolle auf dem Asset zugewiesen, das er verlinken möchte. Mittels des Work Items *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

> Sollte der Bearbeiter einen anderen Benutzer als sich selber auswählen verliert er nach dem ersten Speichervorgang weitere Bearbeitungsrechte.

> Damit auf einen Blick erkennbar ist, von wem das *Nachhaltigkeitsrisiko* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

6 **Bewertungszyklus**: Der Bearbeiter muss einen "Bewertungszyklus" hinterlegen. Der Bewertungszyklus gibt an, wie oft ein *Nachhaltigkeitsrisiko* zurück in den Status "In Nettobewertung" geschickt wird, um das *Nachhaltigkeitsrisiko* in regelmäßigen Zeitabständen zu evaluieren. Das Attributsfeld "Nächste Bewertung am" wird automatisch von BIC GRC gesetzt.

7 **Speichern**: Sobald die Informationen angegeben sind kann der Bearbeiter Risiko speichern.

Schritt 3: Zuordnung finalisieren

Der Bearbeiter sollte das *Nachhaltigkeitsrisiko* regelmäßig dahingehend überprüfen, ob das *Nachhaltigkeitsrisiko* in seiner Art und Weise noch aktuell und korrekt ist.

Um dies in regelmäßigen Abschnitten zu überprüfen, unterstützt das Feld "Nächste Bewertung". Zwei Wochen vor dem erreichen des Datums bekommt der Bearbeiter eine Notifikation automatisch zugesendet, die ihn an eine bevorstehende Neubewertung erinnert.

An dem Tag der "Nächsten Bewertung" wird das *Nachhaltigkeitsrisiko* im Status "Aktiv" in den Status "Nettobewertung" geschalten und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.

> **Das Datum wird nach dem Statuswechsel automatisch neu gesetzt abhängig von der Zeitangabe in "Bewertungszyklus".**

Wenn das *Nachhaltigkeitsrisiko* einer der Überprüfungszyklen "Alle ... Tage", "Anlassbezogen", "Täglich" oder "Wöchentlich" hat, wird der Status nicht automatisch zurückgesetzt und der Bearbeiter wird nicht über einen Statusübergang mittels Notifikation benachrichtigt.

Der Bearbeiter kann anschließend mit dem nächsten Schritt Nachhaltigkeitsrisiko ergänzen & analysieren fortfahren.

2.4.7 Nachhaltigkeitsrisiko ergänzen & analysieren

Ein *Nachhaltigkeitsrisiko* kann von mehreren Benutzern identifiziert & erstellt werden.

Wenn der Ersteller und der Bearbeiter unterschiedliche Benutzer sind, wird der Bearbeiter gesondert mittels Notifikation über das neues *Nachhaltigkeitsrisiko* informiert. Die folgenden Schritte 1 & 2 beziehen sich auf die Schritte nach der Erstellung durch einen anderen Benutzer.

Optional Schritt 1: Navigation zu spezifischem Nachhaltigkeitsrisiko nach Fremderstellung

Der Bearbeiter hat zwei Möglichkeiten, ein zu bearbeitendes *Nachhaltigkeitsrisiko* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "NEW" abgeschlossen hat. Der Link zu dem spezifischen *Nachhaltigkeitsrisiko* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine ToDo`s"

Im oberen Teil des Dashboards "Meine ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter noch eine Aufgabe zu erledigen hat.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Nachhaltigkeitsrisiko* automatisch. Der Bearbeiter steigt direkt in den Tab *"Kontext"* des *Nachhaltigkeitsrisikos* ein.

Optional Schritt 2: Überprüfung der Eingaben des Erstellers

Wenn der Ersteller und der Bearbeiter nicht derselbe Benutzer sind, empfiehlt es sich, als ersten Schritt im Work Item *Nachhaltigkeitsrisiko* zu dem Tab *"Kontext"* zu gehen, um die Detaileingaben des Erstellers einzusehen.

Sollten die Eingaben des Erstellers nicht richtig oder unvollständig sein, kann der Bearbeiter einen Beitrag im Tab

"Diskussion" hinterlassen. Der Ersteller wird anschließend über den Beitrag mittels Notifikation informiert.

> Der Bearbeiter kann anschließend mit dem nächsten Schritt Nachhaltigkeitsrisiko beurteilen & bewerten fortfahren.

Optional - Schritt 3: Risikoanalyse durchführen

Das Management hat die Möglichkeit, den Benutzern/Bearbeitern Risiko einen Tab "*Risikoanalyse*" anzeigen zu lassen. Die Anzeige ist dabei nicht individuell pro *Security-Risiko*, sondern zentral für alle *Nachhaltigkeitsrisiken* einzustellen.

1. **Mögliche Ursache bzw. Auswirkung**: Um das *Nachhaltigkeitsrisiko* besser einschätzen und bewerten zu können, macht es Sinn vorab eine Risikoanalyse durchzuführen.

   Mittels der beiden Textfelder zu "Mögliche Ursache" und Mögliche Auswirkung" hat der Bearbeiter die Möglichkeit anderen Benutzern einen besseren Einblick und EIndruck zu vermitteln.

2. **Risikoart nach Herkunft bzw. Auswirkung**: Die beiden Links zu "Risikoart nach Herkunft" und "Risikoart nach Auswirkung" sollen den Bearbeiter zusätzlich unterstützen eine Einordnung des *Nachhaltigkeitsrisikos* zu ermöglichen.

   > Es werden nur GRC Framework-Elemente angezeigt die auch einen passenden Tag zu der Perspektive besitzen.

   > Sollte es ein passendes *Risikoszenario* geben, dass diese beiden Links ausgefüllt hat, werden diese bei einem Speichervorgang nach der Hinterlegung des *Risikoszenarios* automatisch übernommen. Wurde im *Nachhaltigkeitsrisiko* schon eine Verlinkung vorgenommen, werden die bestehenden Eingaben von "Risikoart nach Herkunft" und "Risikoart nach Auswirkung" nicht überschrieben.

3. **Betroffene Stakeholder**: Bei den "Betroffenen Stakeholdern" kann in ein Textfeld eingetragen werden, welche Stakeholder laut dem Bearbeiter von diesem *Nachhaltigkeitsrisiko* betroffenen sein werden.

   > Dadurch, dass es sich um ein Textfeld handelt dient dieser Eintrag rein als Information am *Nachhaltigkeitsrisiko* und kann nicht auf beispielsweise Dashboards ausgewertet werden.

2.4.8 Nachhaltigkeitsrisiko beurteilen & bewerten

Ein *Nachhaltigkeitsrisiko* wird von einem Ersteller identifiziert & erstellt und von einem Bearbeiter Risiko ergänzt & analysiert, bevor der Bearbeiter Risiko mit der Bewertung des Risikos beginnen kann.

Schritt 1: Bewertung durchführen

Sobald sich das *Nachhaltigkeitsrisiko* im Status *"Brottobewertung*" befindet, kann mit der Bewertung des *Nachhaltigkeitsrisiko* in dem Tab *"Bruttobewertung"* begonnen werden.

Im ersten Schritt hat der Bearbeiter die passende Bewertungsmethode zu wählen. Dabei ist zwischen zwei Bewertungsmöglichkeiten zu wählen.

Folgende Bewertungsmethoden stehen zu Verfügung:

- (a) Qualitativ
- (b) Quantitativ (Multi-Period)

Im Sinne der Lesbarkeit werden "Schritt 3: Bruttobewertung durchführen" und "Schritt 4: Nettobewertung durchführen" abhängig von der Bewertungsmethode beschrieben.

Schritt 2a: Qualitative Bruttobewertung durchführen

Bei einer qualitativen Risikobewertung wird eine deskriptive und keine monetäre Bewertung durchgeführt. In BIC GRC erfolgt dies in Form einer 4x4, 5x5 oder 6x6-Heatmap (auch Risikomatrix genannt). Die Größe der Heatmap wird vorab vom Management bestimmt.

1. **Optional - Was wurde identifiziert:** Wenn vom Management die Option freigeschalten wurde auch Chancen zu bewerten, wird diese Auswahl angezeigt.

   Abhängig von der Auswahl wird das Format der Heatmap gewählt. Die Heatmap erscheint dabei erst nach dem erstmaligen speichern.

   Wenn es sich wie im Beispielbild um ein reines Risiko handelt, wird ein Farbverlauf von grün bis rot vorgegeben. Wurde eine Chance identifiziert spiegelt sich die Heatmap und der Farbverlauf ist blau. Für den Fall, dass sich ein *Nachhaltigkeitsrisiko* im Verluaf ändert von negativ zu positiv bzw. vice versa - sogenannte Mixed Cases - werden beide Heatmaps - Risiko und Chance - gleichzeitig angezeigt.

2. **Bruttobewertung**: Der Bearbeiter hinterlegt per Klick in der Heatmap ein Icon, in dessen Wertebereich sich das *Nachhaltigkeitsrisiko* seiner Meinung nach ohne Steuerung, also ohne *Maßnahme,* befindet.

> Für die bessere Einschätzung werden dem Bearbeiter die unternehmensweiten Schwellenwerte angezeigt.

3. **Begründung der Bewertung**: Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu dieser Bewertung gekommen ist.
4. **Bewertung nach Zeithorizont**: Da *Nachhaltigkeitsrisiken* in unteschiedlichen Zeithorizonten betrachtet werden müssen, kann der Bearbeiter angeben, wie sich das *Nachhaltigkeitsrisiko* möglicherweise im Zeitablauf verändern wird.

   Dafür wird ihm eine eigene Heatmap angezeigt, in der er die Werte Kurzfristig (S), Mittelfristig (M) und Langfristig (L) hinterlegen muss
5. **Abhängige Risiken**: Der Bearbeiter kann einen Bezug zu anderen *Nachhaltigkeitsrisiken* herstellen, indem er ein *Abhängiges Risiko* Work Item erstellt.

   Weitere Informationen unter Abhängige Risiken herleiten & erstellen.

> Da die Verbindung zwischen zwei *Nachhaltigkeitsrisiken* einzigartig ist, können *Abhängige Risiken* immer nur aus einem (Parent-) Risiko erstellt und nicht verlinkt werden.

> Es wird stark empfohlen, mit der Möglichkeit von Abhängigkeiten zwischen *Nachhaltigkeitsrisiken* zu arbeiten, da auch im tatsächlichen Alltag Risiken nicht alleine stehen, sondern Interdependenzen vorhanden sind.

6. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang " Nettobewertung" durchgeführt.

Beim Statusübergang wird der Bearbeiter automatisch in den Tab "*Nettobewertung*" weitergeleitet.

Schritt 2a: Nettobewertung durchführen

7. **Soll-Bewertung**: Der Bearbeiter hinterlegt per Klick in der Heatmap ein Icon (T=Target) für den gewünschten Soll- Zustand, in dem sich das *Nachhaltigkeitsrisiko* nach geplanten *Maßnahmen* befinden sollte.
8. **Risikosteuerung**:

   Anschließend entscheidet der Bearbeiter, mit welcher Risikosteuerung er dieses Ziel erreichen möchte.

   - Vermeiden: Durch die Wahl alternativer Lösungsansätze wird versucht, die Ursache zu umgehen, z.B. Verzicht auf Geschäftsbeziehungen in Regionen mit instabilen Governance-Strukturen.
   - Vermindern: Das Risiko wird durch Maßnahmen vermindert, die sowohl auf die Ursache als auch auf die Wirkung Einfluss nehmen, z.B. Schulungen für Mitarbeiter zu menschenrechtlichen Risiken in Lieferketten.
   - Transferieren: Durch Abwälzung der Haftung oder eingetretener Schäden auf eine Dritte Partei kann ein Risiko transferiert werden, z.B. auf ein Versicherungsunternehmen.

- Akzeptieren: Können für ein Risiko keine Maßnahmen gefunden werden, die das Nachhaltigkeitsrisiko effizient oder effektiv vermeiden, vermindern oder transferieren, muss das Restrisiko akzeptiert werden.

Zudem kann der Bearbeiter freiwillig Kontrollen ableiten & erstellen.

> Für die Mitigation des *Nachhaltigkeitsrisikos* können mehrere *Maßnahmenbewertungen* aus dem *Nachhaltigkeitsrisiko* heraus erstellt werden.

Der Bearbeiter kann ein *Nachhaltigkeitsrisiko* erst "Akzeptieren", wenn es sich unter dem vom Management vorgegebenen Risikoschwellenwert befindet. Dieser Schwellenwert kann im Risikowertbalken abgelesen werden.

Sollte der Bearbeiter sich für "Akzeptieren" entscheiden, wird ein Beschreibungsfeld sichtbar. Es sind keine Maßnahmen oder Kontrollen mehr verlinkbar, sondern nur noch bisherige Verlinkungen lesbar.

Mehr zu der Erstellung von Maßnahmenbewertungen.

9 **Ist- Bewertung**: Nachdem alle *Maßnahmenbewertungen* hinterlegt sind, kann in der Heatmap mittels des Icons (C) manuell der aktuelle Ist-Zustand des *Nachhaltigkeitsrisiko* eingeordnet werden, unter der Beachtung der aktuellen *Maßnahmen* und ihres Umsetzungsgrad zum aktuellen Zeitpunkt.

10 **Risikowertbalken**: Sobald eine Ist- Bewertung erfolgt ist wird ein Risikowertbalken angezeigt.

11 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu " Freigabe" durchgeführt.

Quantitativ - Mehrjahressimulation

> **Bei der Risikobewertung Quantitativ- Mehrperioden- Simulation wird eine monetäre Bewertung durchgeführt. Die Bewertung erfolgt dabei mittels einer 3-Punkte-Bewertung für bis zu fünf Jahre in die Zukunft.**

Schritt 1d: Bruttobewertung durchführen

1 **Zusätzliche Feedbackschleife:** Bei der Wahl der Bewertungsmethode "Mehrperioden-Simulation" kann der Bearbeiter freiwillig einen Simulationsanalysten mittels hinterlegen. Dieser kann die Eingaben der Bewertung und der Simulationsresultate auf Plausibilität überprüfen, bevor es dem Freigeber zur Freigabe weitergegeben wird.

2 Der Bearbeiter muss Voreinstellungen für die Mehrjahresbewertung machen, indem er zwei Attributsfelder ausfüllt.

Anzahl der Jahre: Zuerst wird bestimmt, für wie viele Jahre in die Zukunft die Risikobewertung vorgenommenen werden kann. Abhängig von der Eingabe, werden die Jahre, die nicht in den Zeitraum fallen, ausgegraut und können nicht vom Bearbeiter bearbeitet werden.

3 **Langfristiges Risikoverhalten:** Als zweite Information muss hinterlegt werden, ob das *Nachhaltigkeitsrisiko* abhängig von der Eingabe der zu bewertenden Jahre noch bestehen bleibt. Sollte das *Nachhaltigkeitsrisiko* darüber hinaus noch bestehen, wobei aber keine passenden Informationen für die Eingabe vorliegen, so werden die Eingaben des zuletzt bewerteten Jahres übernommen und als Basis für die Simulation herangezogen. Besteht das *Nachhaltigkeitsrisiko* nach der gewählten Jahresangabe nicht mehr, werden die ausgegrauten Attributsfelder automatisch mit dem Wert 0 befüllt und nicht weiter beachtet.

> Die angezeigten Jahreszahlen sind dynamisch und passen sich automatisch an das aktuelle Jahr bei Jahreswechsel an. Mittels eines Rollforwards können die Werte bei einer Mehrjahresbewertung ein Jahr vorgerückt werden.

4 **Eintrittswahrscheinlichkeit**: Als nächsten Schritt hat der Bearbeiter die Häufigkeit zu bestimmen, mit der das *Nachhaltigkeitsrisiko* auftreten kann. Dabei kann er sich entscheiden, ob das *Nachhaltigkeitsrisiko* nur einmal eintritt oder mehrfach, beziehungsweise wie oft es (z.B. pro Jahr) auftreten kann.

> Anhand der Häufigkeit wird automatisch eine Eintrittswahrscheinlichkeit im Hintergrund berechnet, die unter der Eingabe der Häufigkeit abgebildet wird. Bei Fragen hierzu kann ein GBTEC Consultant konsolidiert werden.

5 **Schadenshöhe**: Nach der Eintrittswahrscheinlichkeit hat der Bearbeiter die Schadenshöhe zu hinterlegen. Die Schadenshöhe ist für drei Werte zu bestimmen:

- Bester Fall
- Wahrscheinlichster Fall
- Schlimmster Fall

> Im weiteren Verlauf der Nettobewertung werden alle Schätzungen zum Risikoeintritt entsprechend ihrer Wahrscheinlichkeit bewertet.

6 **Optional - Shape Parameter**: Der Shape-Parameter wird auch als Gleichgewichtsfaktor bezeichnet und kann als vierter Parameter neben der 3-Punkte-Bewertung gesehen werden.

Er gibt an, wie gesichert die Schätzung der Schadenshöhe ist und verändert gegebenfalls die Form der PERT-Verteilung.

> Zum Beispiel können manche Werte anhand von Erfahrungen als sehr sicher angegeben werden. Andere Werte wie z.B. solche im Zusammenhang mit Reputationsschäden können nur grob geschätzt werden.

Dem Bearbeiter stehen fünf Stufen für die Einschätzung der Sicherheit zur Verfügung.

> Der Shape-Parameter ist optional und kann vom Management dahingehend übersteuert werden, das er von dem Bearbeiter nicht ausgewählt werden kann.

> Wenn der Shape-Parameter nicht eingegeben werden kann, bleibt er bei seinem Standardwert von 4. Ist die Option vom Management freigegeben, den Shape-Parameter zu nutzen, bekommt der User durch die 5-Stufen eine Auswahl zwischen den Werten 4-20 (4 ist sicher, 20 ist unsicher). Daher empfiehlt GBTEC seine Verwendung für genauere Simulationsergebnisse.

7 **Begründung**: Es muss eine Begründung angegeben werden, wie der Bearbeiter zu der Bewertung gekommen ist.

8 **Abhängige Risiken**: Der Bearbeiter kann einen Bezug zu anderen *Nachhaltigkeitsrisiken* herstellen, indem er ein *Abhängiges Risiko* Work Item erstellt.

Weitere Informationen unter Abhängige Risiken herleiten & erstellen.

> Da die Verbindung zwischen zwei *Nachhaltigkeitsrisiken* einzigartig ist, können *Abhängige Risiken* immer nur aus einem (Parent-) Risiko erstellt und nicht verlinkt werden.

> Es wird stark empfohlen, mit der Möglichkeit von Abhängigkeiten zwischen *Nachhaltigkeitsrisiken* zu arbeiten, da auch im tatsächlichen Alltag Risiken nicht alleine stehen, sondern Interdependenzen vorhanden sind.

9 **Statuswechsel**: Ein Statusübergang kann erst durchgeführt werden, wenn alle Attributsfelder (außer Punkt 1) ausgefüllt wurden. Beim Statusübergang wird der Bearbeiter automatisch in den Tab "*Nettobewertung*" weitergeleitet.

Schritt 2d: Nettobewertung durchführen

10 **Soll-Bewertung**: Im Tab "*Nettobewertung*" findet der Bearbeiter eine Tabelle mit der Überschrift "*Soll-Wert*". In dieser Tabelle befinden sich vorerst alle Werte ohne Mitigation - also Maßnahmen - wieder. Die Werte entsprechen den Bruttowerten.

11 **Risikosteuerung**:

Anschließend entscheidet der Bearbeiter, mit welcher Risikosteuerung er dieses Ziel erreichen möchte.

- Vermeiden: Durch die Wahl alternativer Lösungsansätze wird versucht, die Ursache zu umgehen, z.B. Verzicht auf Geschäftsbeziehungen in Regionen mit instabilen Governance-Strukturen.
- Vermindern: Das Risiko wird durch Maßnahmen vermindert, die sowohl auf die Ursache als auch auf die Wirkung Einfluss nehmen, z.B. Schulungen für Mitarbeiter zu menschenrechtlichen Risiken in Lieferketten.
- Transferieren: Durch Abwälzung der Haftung oder eingetretener Schäden auf eine Dritte Partei kann ein Risiko transferiert werden, z.B. auf ein Versicherungsunternehmen.
- Akzeptieren: Können für ein Risiko keine Maßnahmen gefunden werden, die das Nachhaltigkeitsrisiko effizient oder effektiv vermeiden, vermindern oder transferieren, muss das Restrisiko akzeptiert werden.

Zudem kann der Bearbeiter freiwillig Kontrollen ableiten & erstellen.

Für die Mitigation des *Nachhaltigkeitsrisiko s* können mehrere *Maßnahmenbewertungen* aus dem *Nachhaltigkeitsrisiko* heraus erstellt werden. Nach einem Speichervorgang sind die Änderungen durch die *Maßnahme* ersichtlich.

Der Bearbeiter kann ein *Nachhaltigkeitsrisiko* erst "Akzeptieren", wenn es sich unter dem vom Management vorgegebenen Risikoschwellenwert befindet. Dieser Schwellenwert kann im Risikowertbalken abgelesen werden.

Sollte der Bearbeiter sich für "Akzeptieren" entscheiden, wird ein Beschreibungsfeld sichtbar. Es sind keine Maßnahmen oder Kontrollen mehr verlinkbar, sondern nur noch bisherige Verlinkungen lesbar.

Mehr zu der Erstellung von Maßnahmenbewertungen.

Hat der Bearbeiter den Eindruck, dass nach der Hinterlegung der *Maßnahmenbewertung* keine angemessene Veränderung der Werte in der Tabelle vorgenommen wurden, empfehlen wir den Button "Werte updaten" oder mittels der Tastatur-Taste "F5" die Seite neu zu laden.

12 **Werte überschreiben:** Wenn der Bearbeiter der Meinung ist, dass die automatisch berechneten Werte nicht dem tatsächlichen Soll-Wert entsprechen, kann er die Checkbox "Möchten Sie die vorgeschlagenen Werte überschreiben?" verwenden. Durch diese Auswahl werden weitere Attributsfelder sichtbar, die für eine manuelle Übersteuerung verwendet werden können.

13 **Werte kopieren:** Sollte der Bearbeiter nicht alle Attributsfelder manuell eingeben wollen, kann er den Button "Werte kopieren" verwenden. Durch diesen werden alle Werte aus den vorgeschlagenen Werten in die darunter liegenden bearbeitbaren Attributsfelder übertragen. Danach kann der Bearbeiter eine manuelle Adaptierung individueller Attributtsfelder vornehmen, die für die Simulation herangezogen werden.

14 **Ist- Bewertung**: Unter dem Abschnitt "*Risikobehandlung*" befindet sich ein weiterer Abschnitt "*Ist-Wert*". Die Tabelle "*Ist-Wert*" verhält sich wie die Tabelle "*Soll-Wert*" mit der Ausnahme, dass sich die Werte nicht auf zu 100% implementierte Maßnahmen beziehen, sondern auf deren tatsächlichen Umsetzungsgrad, welcher zwischen 0-100% liegen kann. Somit sollten "Ist-Werte" immer gleich sein oder sich zwischen dem Brutto- und dem Soll-Wert befinden, sofern nicht die Risikosteuerung "Akzeptieren" ausgewählt wurde.

Hat der Bearbeiter den Eindruck, dass nach der Hinterlegung der *Maßnahmenbewertung* keine angemessene Veränderung der Werte in der Tabelle vorgenommen wurden, empfehlen wir mittels der Tastatur-Taste "F5" die Seite neu zu laden.

15 **Simulation**:

Wenn alle Attributsfelder in der Tabelle eingetragen sind, wird ein neuer Bereich "*Simulation*" unter dem Abschnitt "*Risikobehandlung*" sichtbar. In diesem werden die Iterationen eingegeben, wobei der Standardwert vom Management vorgegeben wird. Wenn alle Eingaben vollständig sind, kann der Button "Simulation" verwendet werden, um die Simulation zu starten. Nach der erfolgreichen Durchführung der Simulation wird das Attributsfeld "Zeitstempel" automatisch mit den aktuellen Daten befüllt.

Wenn die Simulation erfolgreich durchgeführt wurde erscheinen automatisch neue Tabellen mit den Resultaten der Simulation, aufgegliedert nach Jahren sowie Brutto-, Ist- und Soll-Wert und passenden Plots.

> Der Bearbeiter hat verschiedene Plot- Auswahlmöglichkeiten, um das *Nachhaltigkeitsrisiko* für ein oder mehrere Jahre visuell abzubilden. In der Standardauswahl befinden sich die Typen Boxplot, Histogramm,Dichteplot und ab dem Jahr 1 nach dem aktuellen Jahr die Möglichkeit einer Dynamischen VaR-Grafik.

> Sollte es bei der Simulation zu einem Abbruch gekommen sein, wird neben dem Simulations-Button ein Warning- oder ein Error-Icon angezeigt. Wenn der User mit der Maus über das Icon streicht, werden im zusätzliche Informationen angezeigt.

16 **Statusübergang**: Der Bearbeiter hat nach der Bewertung die Möglichkeit zwischen zwei Statusübergängen zu wählen. Sollte er sich bezüglich der Eingaben der Bewertung unsicher sein, kann er den Status " Expertenüberprüfung" wählen. Hierbei wird der eingetragene Simulationsanalyst benachrichtigt und um eine Überprüfung der Eingaben und Simulationsresultate gebeten.

> Wurde kein Simulationsanalyst in der Brutto-Bewertung eingetragen, erscheint der Status " Expertenüberprüfung" nicht, auch wenn es sich um die Bewertungsmethode "Mehrperioden-Simulation" handelt.

Wenn die Eingaben keine Überprüfung erfordert oder vom Management der Status " Expertenüberprüfung" nicht zur Verfügung gestellt wird, kann der Bearbeiter direkt zum Status " Freigabe" wechseln, wobei der Freigeber über diesen Statuswechsel benachrichtigt wird.

> Der Statusübergang ist nur möglich, wenn ein Zeitstempel gesetzt wurde von der Simulation. Dabei wird der Zeitstempel automatisch gesetzt von BIC GRC und auch nur bei einem erfolgreichen Simulationsdurchlauf.

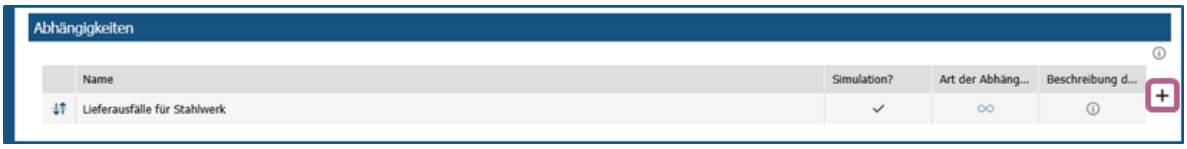
2.4.9 Abhängige Risiken herleiten & erstellen

In der Unternehmenspraxis beeinflussen Risiken einander und sind keine Silo-Risiken. Um diesen Einfluss aufeinander bzw. Abhängigkeiten herzustellen, kann der Bearbeiter eines Risikos aus seinem *Nachhaltigkeitsrisiko* ein Work Item *Abhängiges Risiko* erstellen, dass eine Verbindung zwischen zwei *Nachhaltigkeitsrisiken* (Parent-Child) herstellt.

Schritt 1: Abhängiges Risiko erstellen

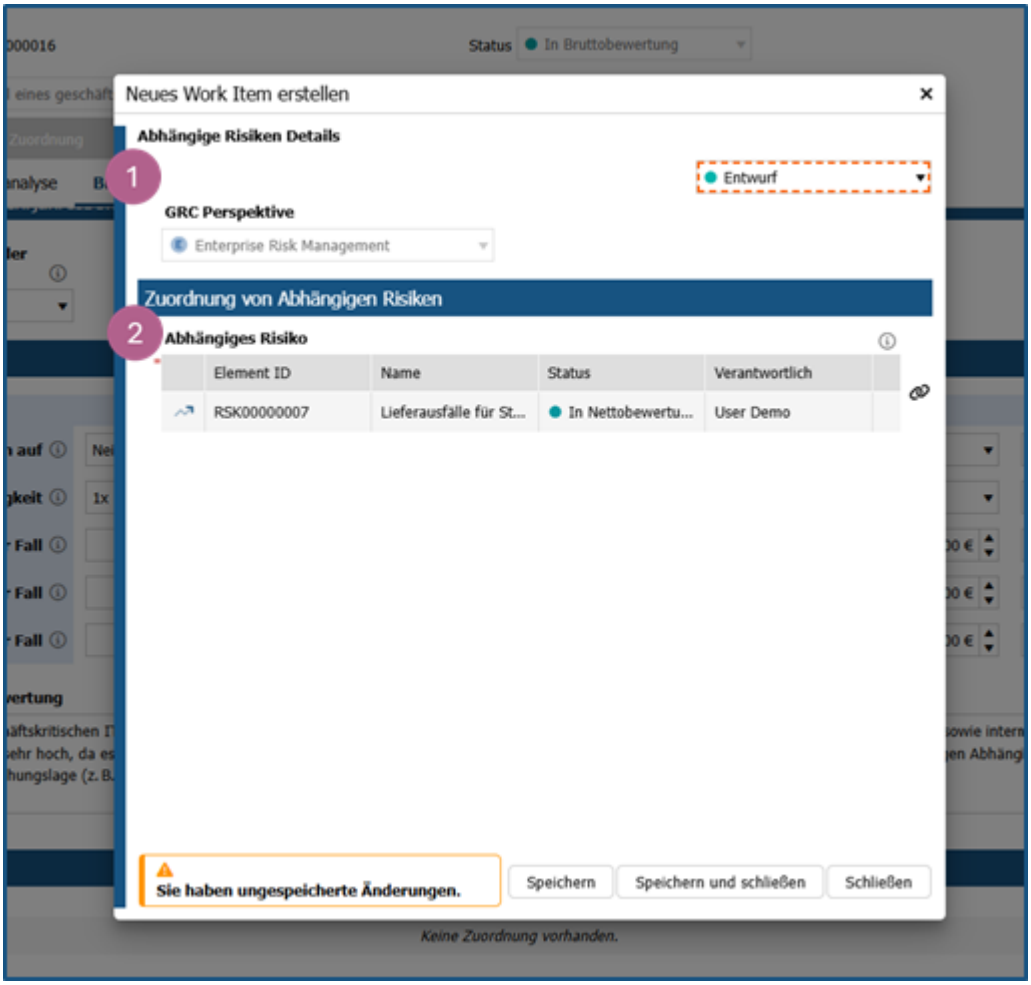
Ein *Abhängige Risiko* kann nur mittels Erstellung aus dem Work Item *Nachhaltigkeitsrisiko* durch den verantwortlichen Bearbeiter erfolgen.

Für die Erstellung wird im Tab "*Bruttobewertung*" im Abschnitt zum *Abhängigen Risiko* durch das Icon + ein neues *Abhängiges Risiko* erstellt.



Das *Abhängige Risiko* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des *Nachhaltigkeitsrisikos*.

Schritt 2: Nachhaltigkeitsrisiko zuordnen



1 **GRC Perspektive**: Bei der Erstellung des *Abhängigen Risikos* wird automatisch die GRC Perspektive "Corporate Sustainability" gesetzt und kann nicht verändert werden.

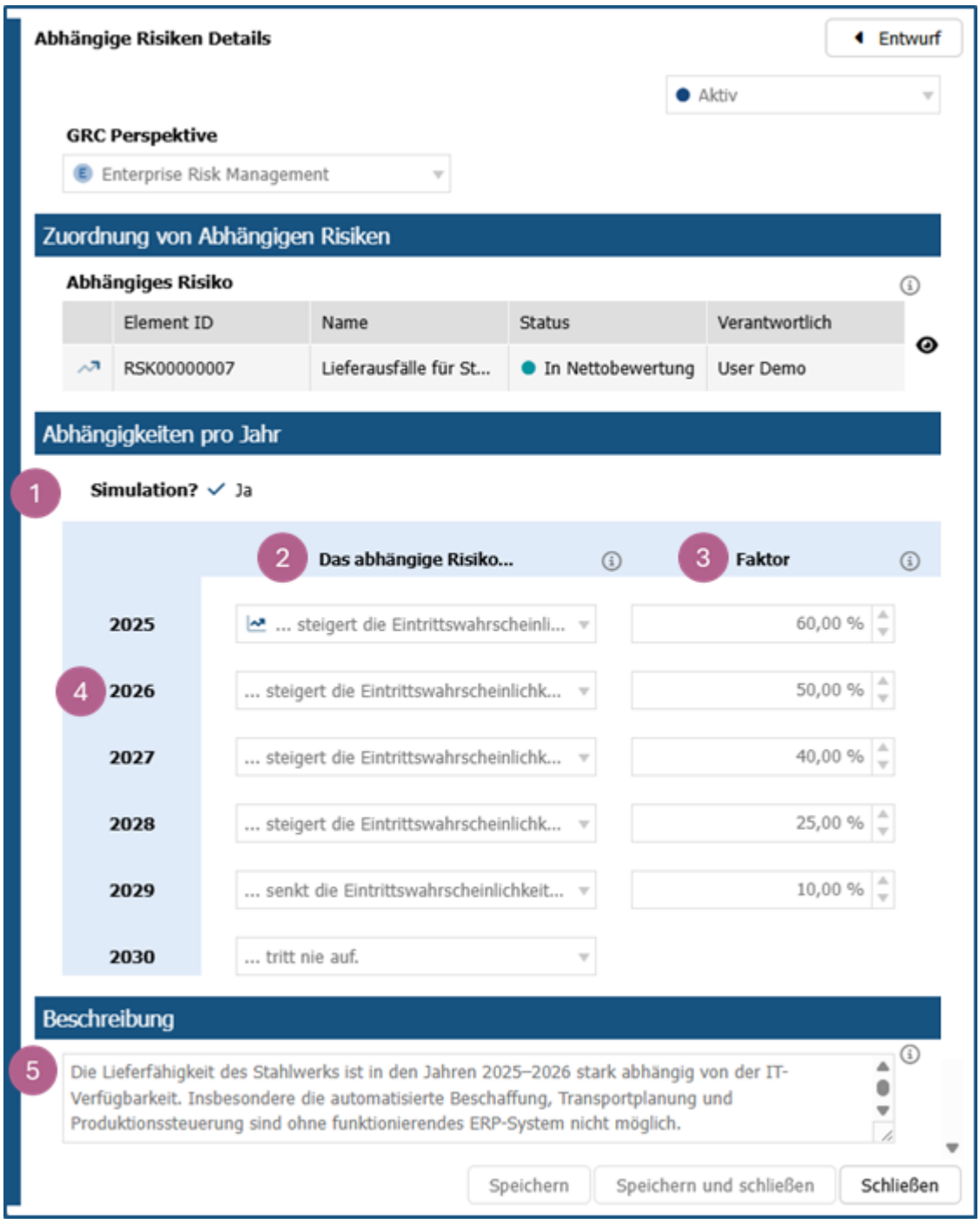
Diese Information ist wichtig, da *Abhängige Risiken* zwischen anderen Risikotypen hergestellt werden können.

2 **Unternehmensrisiko verlinken**: Zuerst muss der Bearbeiter ein *Unternehmensrisiko* verlinken, das von dem (Parent-) *Unternehmensrisiko* beeinflusst werden soll.

Danach sollte der Bearbeiter erstmalig speichern.

Es kann insgesamt nur ein *Unternehmensrisiko*in dem *Abhängigen Risiko*verlinkt werden.

Schritt 3: Abhängigkeit dokumentieren



1. **Simulation**: Von BIC GRC wird automatisch abgeleitet, ob das *Abhängige Risiko* für die Simulation und somit die Work Item Typen *Portfolio Simulation* und *Mehrperioden Portfolio Simulation* verwendet werden kann, oder ob das *Abhängige Risiko* nur als Information zwischen den *Unternehmensrisiken* fungiert.
2. **Das abhängige Risiko...**: Neben der aktuellen Jahreszahl kann der Bearbeiter hinterlegen, inwiefern das (Parent-) *Unternehmensrisiko* das (Child-) *Unternehmensrisiko* beeinflusst.
3. **Faktor**: Sollte der Bearbeiter festlegen, dass die Eintrittswahrscheinlichkeit mittels eines Faktors das (Child-)*Unternehmensrisikos* steigt oder sinkt, kann zusätzlich ein Prozentwert eingegeben werden.

> Bei dieser Information handelt es sich nicht um den Umstand, dass ein (Parent-)*Unternehmensrisiko* ein anderes (Child-)*Unternehmensrisiko* mit einer Wahrscheinlichkeit von über 100 % verursacht, sondern um die Information, dass das Auftreten eines (Child-)*Unternehmensrisikos* um den Faktor erhöht (multipliziert) wird, der höher als 100 % sein kann (man stelle sich das als „Wachstumsfaktor“ vor). Ein Beispiel soll dies verdeutlichen: Ein (Parent-)*Unternehmensrisiko* hängt von einem (Child-)*Unternehmensrisiko* mit einem Faktor von 200% ab. Das (Child-) *Unternehmensrisiko* hat bei seinem Entstehen eine Eintrittswahrscheinlichkeit von 10 %. Das Eintreten des (Parent-) *Unternehmensrisikos* erhöht also die Eintrittswahrscheinlichkeit des (Child-) *Unternehmensrisikos* auf 20% pro Iteration (nicht auf 200%).

4. **Mehrjahressimulation**: Bei der Bewertungsmethode Mehrjahressimulation im *Unternehmensrisiko* hat der Bearbeiter in dem *Abhängigen Risiko* nicht nur die Abhängigkeit für das laufende, sondern auch für die nächsten Jahre zu bestimmen. Die Anzahl der zu befüllenden Jahre ist abhängig von der Angabe im *Unternehemsrisiko*, inwieweit das *Unternehmensrisiko* in die Zukunft bewertet werden kann.
5. **Beschreibung der Abhängigkeiten:** Der Bearbeiter kann bei Bedarf noch die Abhängigkeit zwischen den *Unternehmensrisiken* genauer beschreiben.

Schritt 4: Weiteres Vorgehen

Sobald die Abhängigkeit hinterlegt ist, kann das *Abhängige Risiko*erneut gespeichert und geschlossen werden.

> Sollte das *Abhängige Risiko* entlinkt wird, wird es aus dem gesamten System gelöscht und verbleibt nicht als Waise im System.

> Wenn das (Parent-) *Unternehmensrisiko* in den Status "Obsolet" geschalten wird, wird auch das *Abhängige Risiko* in "Obsolet" gesetzt. Dasselbe Verhalten ergibt sich, wenn das (Child-)*Unternehmensrisiko* in den Status "Obsolet" geschalten wird.

Zurück zu dem Schritt Bearbeiter Risiko - Unternehmensrisiko beurteilen & bewerten.

2.4.10 Maßnahmenbewertung ableiten & erstellen

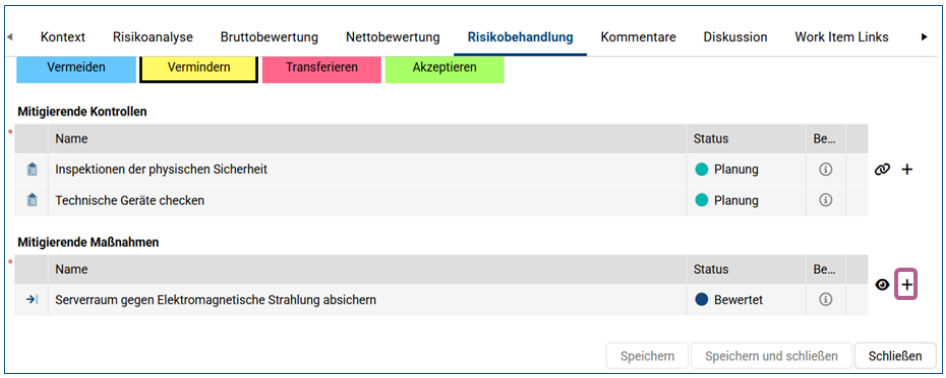
Nach der Erstellung eines *Nachhaltigkeitsrisikos* bedarf es *Maßnahmen*, um das *Nachhaltigkeitsrisiko* zu mitigieren. Um nicht für jedes *Nachhaltigkeitsrisiko* individuelle *Maßnahmen* erstellen zu müssen, die sich dann im System doppelt wiederfinden, besteht die Möglichkeit über *Maßnahmenbewertung* , eine Verbindung zwischen einem *Nachhaltigkeitsrisiko* und mehrfach verwendeten *Maßnahmen* herzustellen.

> Diese *Maßnahmenbewertung* stellt den tatsächlichen Einfluss einer *Maßnahme* auf ein spezifisches *Nachhaltigkeitsrisiko* fest.

Schritt 1: Maßnahmenbewertung erstellen

Die *Maßnahmenbewertung* kann nur mittels Erstellung aus dem Work Item *Nachhaltigkeitsrisiko* durch den verantwortlichen Bearbeiter erfolgen. Dabei wird die Erstellung einer *Maßnahmenbewertung* nur erlaubt, wenn nicht die Risikosteuerung "Akzeptieren" ausgewählt wurde.

Für die Erstellung wird im Tab "*Behandlung*" im Link zur *Maßnahme* durch das Icon + eine neue *Maßnahmenbewertung* erstellt.



> Die *Maßnahmenbewertung* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des *Nachhaltigkeitsrisikos* .

Schritt 2: Maßnahme zuordnen

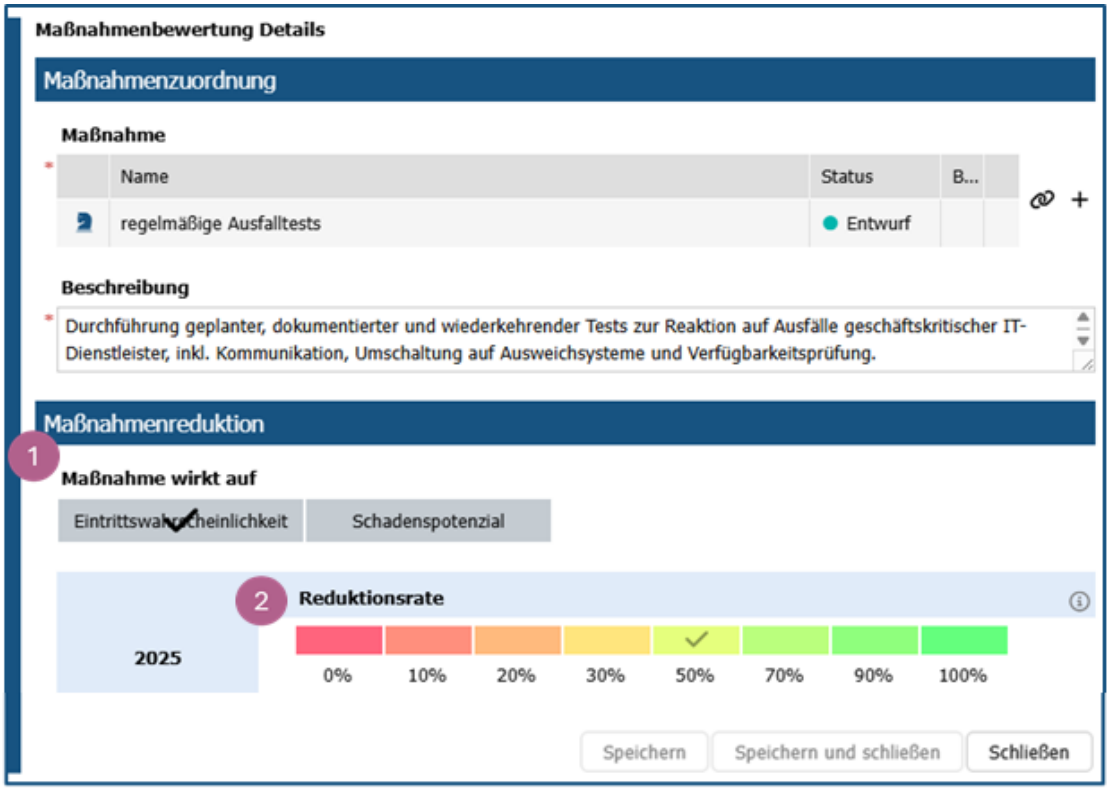
1. **Maßnahme verlinken**: Zuerst muss der Bearbeiter ein Work Item des Typs *Maßnahme* verlinken, die das spezifische *Nachhaltigkeitsrisiko* mitigieren soll.
2. **Maßnahme erstellen**: Sollte eine passende *Maßnahme* noch nicht bestehen, kann diese über das Icon + erstellt werden. Mehr dazu unter Bearbeiter Risiko - Maßnahme definieren &

erstellen.

3. **Beschreibung**: Danach sollte im darunterliegenden Beschreibungsfeld dokumentiert werden, warum und wie die *Maßnahme* auf das *Nachhaltigkeitsrisiko* wirkt.
4. **Speichern**: Anschließend kann die *Maßnahmenbewertung* gespeichert werden, damit weitere Attributsfelder angezeigt werden.

> Es kann insgesamt nur eine *Maßnahme* in der *Maßnahmenbewertung* verlinkt werden.

Schritt 3: Maßnahmenwirkung dokumentieren



1. **Wirkung**: Nachdem eine *Maßnahme* verlinkt wurde, kann der Bearbeiter festlegen, ob die *Maßnahme* auf die "Eintrittswahrscheinlichkeit" oder die "Schadenshöhe" wirkt.
2. **Reduktionsrate**: Sobald die *Maßnahmenbewertung* gespeichert wurde, wird eine Heatmap sichtbar, die sich auf die Reduktion bezieht. Je mehr die spezifische *Maßnahme* auf das *Nachhaltigkeitsrisiko* wirkt, desto höher sollte die Reduktionsrate gewählt werden.

Schritt 4: Weiteres Vorgehen

Sobald die Reduktionsrate hinterlegt ist, kann die *Maßnahmenbewertung* erneut gespeichert und geschlossen werden. Anschließend sollte das *Nachhaltigkeitsrisiko* mittels erneuten Speicherns durch die Tastaturtaste "F5" aktaulisiert werden, um die Informationen aus der *Maßnahmenbewertung* in das *Nachhaltigkeitsrisiko* zu übernehmen.

Sollte die *Maßnahmenbewertung* entlinkt werden, wird direkt sie aus dem gesamten System gelöscht und verbleibt nicht als Waise im System.

Wenn das *Nachhaltigkeitsrisiko* in den Status "Obsolet" geschalten wird, wird auch die *Maßnahmenbewertung* in "Obsolet" gesetzt. Dasselbe Verhalten ergibt sich, wenn die *Maßnahme* in den Status "Obsolet" geschalten wird.

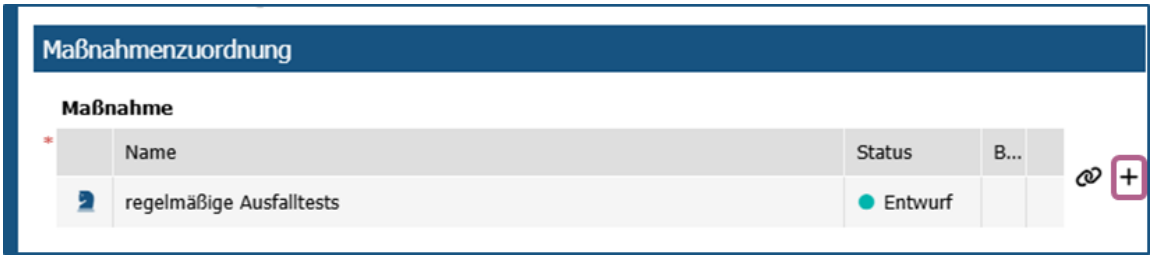
2.4.11 Maßnahme identifizieren & erstellen

Eine *Maßnahme* kann von einem Bearbeiter Risiko erstellt und im Rahmen einer Risikobehandlung eingesetzt werden.

Durch das Erstellen und die Zuordnung zu einem Asset in der Asset Hierarchie kann eine *Maßnahme* von mehreren Domänen in BIC GRC ausgewählt und verlinkt werden. Dadurch wird das Maßnahmenmanagement zu einem eigenen, wesentlichen Bestandteil von BIC GRC.

Schritt 1: Maßnahme erstellen aus Maßnahmenbewertung

Die *Maßnahme* kann von einem Bearbeiter aus einem *Nachhaltigkeitsrisiko* bzw. einer *Maßnahmenbewertung* heraus erstellt werden, indem er im *Nachhaltigkeitsrisiko* und anschließend in der *Maßnahmenbewertung* auf das Icon + klickt.



Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Maßnahme* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Maßnahme* einzigartig.
2. **Bereich**: Um den Bereich der Anzeigeverfügbarkeit der *Maßnahme* einzuschränken, muss es einem Asset in der Asset Hierarchie zugeordnet werden.

   Soll eine *Maßnahme* beispielsweise nur für Standort A und nicht für Standort B gelten, muss der Scope "Standort A" in der Asset-Verlinkung ausgewählt werden. Soll die *Maßnahme* später in BIC GRC erneut verlinkt werden, wird sie nur Usern mit Berechtigungen in Standort A angezeigt und keinen Usern die Assets an Standort B verwalten.

3. **GRC- Perspektive**: Die Perspektive wird automatisch aus der *Maßnahmenbewertung* übernommen und gesetzt. Sie kann nach dem ersten Speichervorgang nicht mehr verändert werden.
4. **Verantwortlichkeiten**: Der Bearbeiter des Risikos hat einen "Bearbeiter Maßnahme" zu hinterlegen, der für die Implementierung der *Maßnahme* verantwortlich sein wird.

   Dieser Benutzer wird durch das  Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

   Weiters ist ein "Freigeber Maßnahme" zu nominieren, der die *Maßnahme* freigibt.

   > Beide Benutzer können erst eingetragen werden, sobald es eine Zuordnung zu einem Asset gibt. Durch einen hinterlegten Filter müssen der Bearbeiter als auch der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

   > Damit auf einen Blick erkennbar ist, von wem die *Maßnahme* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt. Sollte der Bearbeiter gleichzeitig der Ersteller sein kann er sich selber eintragen. Dadurch, dass eine *Maßnahme* allerdings auch von anderen Benutzer erstellt werden kann ist dieses Attribut nicht vorausgefüllt.
5. **Art der Maßnahme**: Mittels der Art der Maßnahme kann der Bearbeiter eine Kategorie für die Maßnahme festlegen.
6. **Einordnung**: Für eine *Maßnahme* ist zu hinterlegen, mit welcher "Priorität" die *Maßnahme* umzusetzen ist und um welche "Art von Maßnahme" es sich handelt. Diese beiden Kriterien können später für die Auswertung auf Dashboards verwendet werden, haben aber keinen weiteren Einfluss auf den Workflow.
7. **Beschreibung**: Die *Maßnahme* sollte so genau wie möglich beschrieben und definiert werden, um Benutzern, die im Workflow nachgelagert sind, einen Überblick über die Aufgabe der *Maßnahme* zu gewähren.
8. **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Maßnahme* gespeichert werden.

   > Nach dem Speichervorgang wird der eingetragene Bearbeiter Maßnahme mittels Notifikation benachrichtigt.

   > Der Ersteller kann nach dem Speichervorgang keine Änderungen mehr an der *Maßnahme* vornehmen. Falls es noch Ergänzungen geben sollte, können diese mittels des "*Diskussion*"-Tabs besprochen werden.

   > Nach dem Speichervorgang kann der Bearbeiter das Work Item schließen und mit Maßnahmenbewertung ableiten & erstellen bzw. Nachhaltigkeitsrisiko beurteilen & bewerten fortfahren.

2.4.12 Kontrolle ableiten & erstellen

Der Bearbeiter Risiko kann in einem *Nachhaltigkeitsrisiko* nicht nur *Maßnahmen* definieren, sondern auch passende *Kontrollen*.

Schritt 1: Kontrolle erstellen aus Nachhaltigkeitsrisiko

Der Bearbeiter Risiko kann aus einem *Nachhaltigkeitsrisiko* im Status "Nettobewertung" direkt eine *Kontrolle* erstellen, indem er im *Nachhaltigkeitsrisiko* auf das Icon + klickt.

Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Kontrolle* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Kontrolle* einzigartig.
2. **Scope**: Um den Bereich der Anzeigeverfügbarkeit der *Kontrolle* einzuschränken, muss es einem Asset in der Asset Hierarchie zugeordnet werden.
3. **GRC- Perspektive**: Die Perspektive wird automatisch aus dem *Nachhaltigkeitsrisiko* übernommen und gesetzt.

   > Sie kann nach dem ersten Speichervorgang nicht mehr verändert werden.

4. **Verantwortliche Personen**: Der Bearbeiter Risiko hat einen "Bearbeiter Kontrolle" zu hinterlegen, und zusätzlich einen "Freigeber Kontrolle", der für die Freigabe der *Kontrolle* verantwortlich ist.

   > Durch einen hinterlegten Filter müssen der Bearbeiter als auch der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

   Dieser Benutzer wird durch das 🔍 Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

   > Damit auf einen Blick erkennbar ist, von wem die *Kontrolle* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt. Sollte der Bearbeiter gleichzeitig der Ersteller sein kann er sich selber eintragen. Dadurch, dass eine *Kontrolle* allerdings auch von anderen Benutzer erstellt werden kann ist dieses Attribut nicht vorausgefüllt.

5. **Kontrollebene**: Die "Kontrollebene" soll angeben, ob die *Kontrolle* vom Management vorgegeben wird oder individuell entstanden ist.
6. **Art der Kontrolle**: Der Bearbeiter Risiko kann bestimmen, ob die *Kontrolle* als "Hauptkontrolle" geführt wird, oder als eine "Unterstützende Kontrolle", wenn z.B. beim

Kontroll-Testing identifiziert wurde, dass die bestehende "Hauptkontrolle" nicht ausreichend ist, um einer Anforderung zu entsprechen.

7 **Beschreibung der Kontrolle**: Der Bearbeiter Risiko sollte in der Beschreibung der *Kontrolle* so gut wie möglich angeben, was er von der *Kontrolle* erwartet und welchem Zweck sie dient.

8 **Speichern**: Sobald alle Informationen eingetragen wurden, kann die *Kontrolle* gespeichert werden.

> Nach dem Speichervorgang wird der eingetragene Bearbeiter Kontrolle mittels Notifikation benachrichtigt.

> Der Ersteller kann nach dem Speichervorgang keine Änderungen mehr an der *Kontrolle* vornehmen. Falls es noch Ergänzungen geben sollte, können diese im "*Diskussion*"-Tab besprochen werden.

> Nach dem Speichervorgang kann der Bearbeiter das Work Item schließen und mit Nachhaltigkeitsrisiko beurteilen & bewerten fortfahren.

2.4.13 Ziel umsetzen & überprüfen

Ziele werden in der Regel nicht innerhalb eines kurzen Zeitraums erreicht, sondern über einen längeren Zeithorizont hinweg verfolgt.

Aus diesem Grund legt der Bearbeiter bei der Erstellung des Work Items *Ziel* einen Überprüfungszyklus fest, zu dem das Ziel erneut auf Aktualität und Fortschritt überprüft wird.

Schritt 1: Navigation zu Ziel

Der Bearbeiter Risiko bekommt automatisch zwei Wochen vor der nächsten Überprüfung von BIC GRC eine Erinnerungs-E-Mail zugesendet.

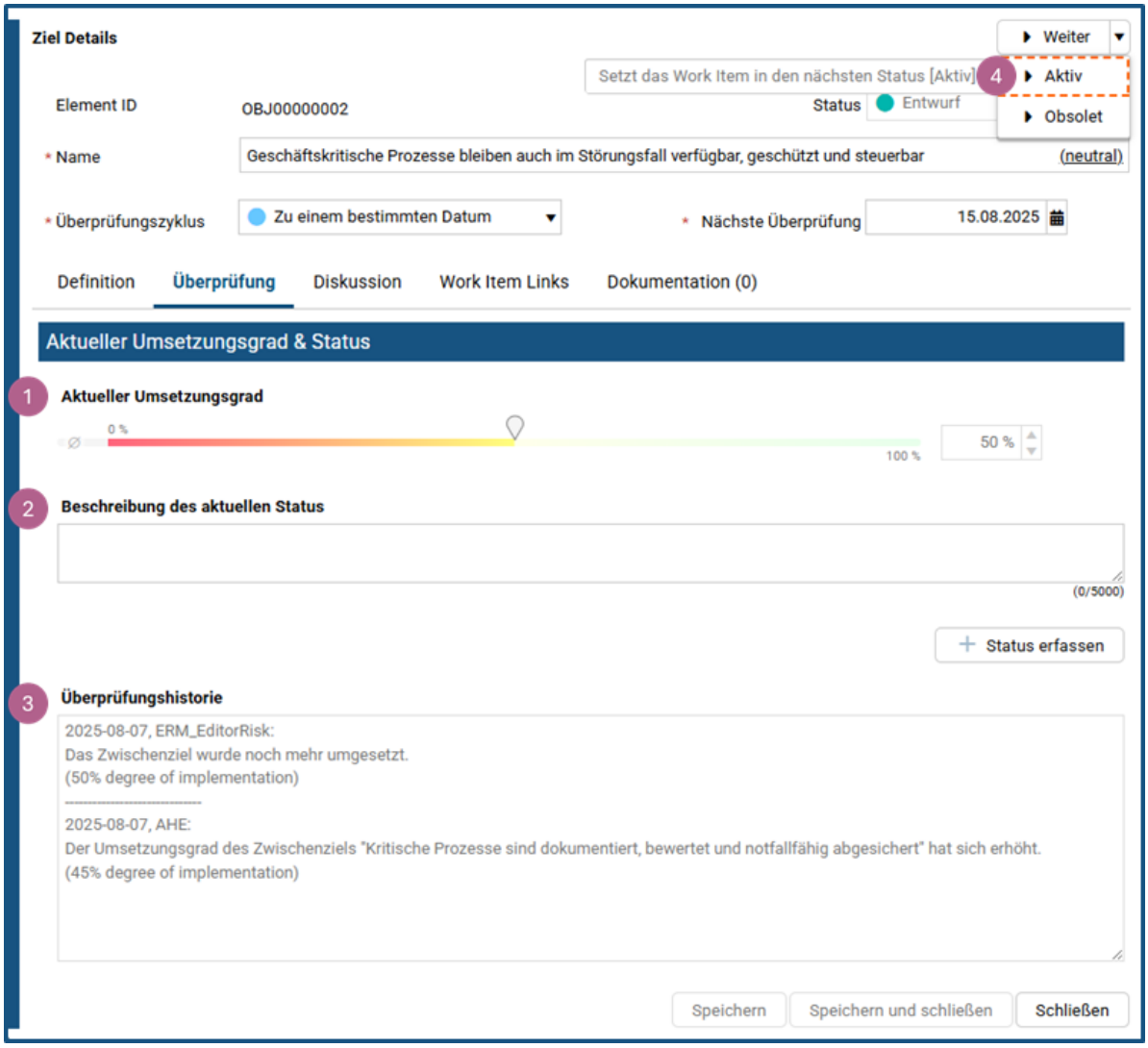
An dem Tag an dem das Datum erreicht wird, wird der Status automatisch zu "Entwurf" gewechselt und der Bearbeiter bekommt erneut eine E-Mail zugesendet. Der Link zu dem spezifischen *Ziel* befindet sich in der Notifikation.

Schritt 2: Zwischenziele evaluieren

Der Bearbeiter sollte bei der Überprüfung mit der Durchsicht der *Zwischenziele* beginnen.

> Der Bearbeiter kann die bisher erstellten *Zwischenziele* bearbeiten und den aktuellen Umsetzungsgrad des *Zwischenziels* hinterlegen.

Schritt 3: Überprüfung durchführen



1. **Aktueller Umsetzungsgrad**: Der aktuelle Umsetzungsgrad wird automatisch als Mittelwert aller *Zwischenziele* ermittelt.
2. **Beschreibung des aktuellen Status**: Um den Fortschritt besser messen zu können kann der Bearbeiter den aktuellen Status erfassen. Mittels des Buttons "Status erfassen" wird der eingetragene Text mit dem aktuellen Datum ergänzt in die "Überprüfungshistorie" übernommen.
3. **Überprüfungshistorie**: Die "Überprüfungshistorie" ist ein Update-Feed, wo der Bearbeiter den aktuellen Status des *Ziels* einträgt und andere berechtigte Personen sich ein Bild über den Fortschritt des *Ziels* machen können.
4. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

2.5 Simulationsanalyst

Bei dem Benutzerprofil Simulationsanalyst handelt es sich um eine unterstützende Rolle, die von Organisationen verwendet werden kann, um ihre Bearbeiter eines Risikos bei der Bewertung von *Nachhaltigkeitsrisiko* mit Simulation zu unterstützen. Dabei kann in *Nachhaltigkeitsrisiken* ein Simulationsanalyst hinterlegt werden, der die Eingaben und Ergebnisse der Simulation überprüft und gesondert freigibt, bevor diese an den Freigeber des Risikos weitergeleitet werden.

Folgende Aufgaben hat ein Simulationsanalyst in BIC GRC:

- Nachhaltigkeitsrisiko überprüfen & freigeben

2.5.1 Nachhaltigkeitsrisiko überprüfen & freigeben

Ein *Nachhaltigkeitsrisiko* wird vom Bearbeiter Risiko erstellt und bewertet. Sollte es sich bei dem *Nachhaltigkeitsrisiko* um ein Risiko mit der Bewertungsmethode "quantitativ - Mehrjahressimulation" handeln - also ein *Nachhaltigkeitsrisiko* mit Simulationskomponenten - kann vom Bearbeiter Risiko optional ein Simulationsanalyst in einem Attributsfeld hinterlegt werden, der die Simulationseingaben und -ergebnisse im Status "Expertenüberprüfung" gemäß eines 4-Augen-Prinzp überprüft. Mehr dazu unter Bearbeiter Risiko - Nachhaltigkeitsrisiko beurteilen & bewerten.

Schritt 1: Navigation zu spezifischem Nachhaltigkeitsrisiko

Der Simulationsanalyst hat zwei Möglichkeiten ein zu überprüfendes *Nachhaltigkeitsrisiko* zu öffnen.

1. Öffnen über Notifikation

Der Simulationsanalyst bekommt eine E-Mail zugesendet, sobald der Bearbeiter Risiko alle Eingaben im Status "Nettobewertung" abgeschlossen und einen optionalen Statusübergang zu "Expertenüberprüfung" durchgeführt hat. Der Link zu dem spezifischen *Nachhaltigkeitsrisiko* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine ToDo`s"

Im oberen Teil des Dashboards "Meine ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Staus anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Simulationsanalyst noch eine Überprüfung durchzuführen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Nachhaltigkeitsrisiko* automatisch.

Schritt 2: Überprüfung durchführen

Der Simulationsanalyst hat in dem bewerteten *Nachhaltigkeitsrisiko* alle Leserechte, um auf Basis aller eingegebenen Informationen zu entscheiden, ob das *Nachhaltigkeitsrisiko* in Bezug auf Brutto- und Nettobewertung richtig eingeordnet und bewertet worden ist.

Sollte dies nicht der Fall sein und muss das *Nachhaltigkeitsrisiko* aus Sicht des Simulationsanalysten erneut bewertet werden, kann der Simulationsanalyst einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "In Bruttobewertung" durchführen.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben weitgehend akzeptabel sein, kann der Simulationsanalyst weiter in den Status "In Freigabe" schalten. Der verantwortliche Freigeber Risiko wird mittels Notifikation über den Statuswechsel benachrichtigt.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.6 Freigeber Risiko

Das Benutzerprofil Freigeber Risiko setzt sich aus allen Freigeber für Risiken zusammen, die unternehmensweit tätig sind. Das Benutzerprofil von Freigeber Risiko ermöglicht es, dass es bei mehreren Organisationseinheiten, Prozessen oder Supporting Assets eines Unternehmens unterschiedliche Freigeber Risiko geben kann, die eigene *Nachhaltigkeitsrisiken* managen müssen.

Folgende Aufgaben hat ein Freigeber Risiko in BIC GRC:

- Nachhaltigkeitsrisiko überprüfen & freigeben

Der Freigeber Risiko kann darüber hinaus noch weitere Work Items erstellen in BIC GRC. Da dies aber nicht seine Hauptaufgabe ist, wird an dieser Stelle nur auf andere Benutzerprofile verwiesen:

- Bedrohung identifizieren & erstellen
- Schwachstelle identifizieren & erstellen
- Risikoszenario herleiten & erstellen
- Ziel definieren & erstellen
  - Zwischenziel definieren & erstellen
- Nachhaltigkeitsrisiko identifizieren & erstellen
- Kontrolle ableiten & erstellen

Bei diesem Vorgang handelt es sich um das reine Erstellen und die Eingabe von den wichtigsten Informationen, um einen Workflow in Gang zu bringen. Sobald der Freigeber Risiko das erste Mal ein Work Item speichert geht das Recht der Bearbeitung auf den eingetragenen Bearbeiter über, der mittels Notifikation automatisch informiert wird. Der Freigeber kann Ergänzungen zu seinen initialen Angaben nur noch im "Diskussions"-Tab hinterlegen.

2.6.1 Nachhaltigkeitsrisiko überprüfen & freigeben

Ein *Nachhaltigkeitsrisiko* wird vom Bearbeiter Risiko erstellt und bewertet. Sobald die Bewertung abgeschlossen und überprüft wurde, kann ein *Nachhaltigkeitsrisiko* dem Freigeber Risiko weitergegeben werden mittels Statusübergang in "In Freigabe".

Schritt 1: Navigation zu spezifischen Nachhaltigkeitsrisiko

Der Freigeber Risiko hat zwei Möglichkeiten ein freizugebendes *Nachhaltigkeitsrisiko* zu öffnen.

1. Öffnen über Notifikation

Der Freigeber Risiko bekommt eine E-Mail zugesendet, sobald der Bearbeiter Risiko alle Eingaben im Status "In Behandlung" abgeschlossen hat. Der Link zu dem spezifischen *Nachhaltigkeitsrisiko* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber Risiko noch eine Freigabe durchzuführen hat.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Nachhaltigkeitsrisiko* automatisch.

Schritt 2: Überprüfung durchführen

Der Freigeber Risiko hat in dem bewerteten *Nachhaltigkeitsrisiko* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob das *Nachhaltigkeitsrisiko* in Bezug auf Brutto- und Nettobewertung richtig eingeordnet, bewertet und behandelt worden ist.

Sollte dies nicht der Fall sein und muss das *Nachhaltigkeitsrisiko* aus Sicht des Freigebers Risiko erneut bewertet werden, kann der Freigeber Risiko einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "In Bruttobewertung" oder "In Nettobewertung" durchführen.

Sollte zudem das *Nachhaltigkeitsrisiko* besonders hoch sein oder das *Nachhaltigkeitsrisiko* an einem z.B. Kernprozess liegen kann der Freigeber Risiko die Checkbox "ERM relevant" im Status "Freigabe" anklicken.

> Die Checkbox wird nur angezeigt, wenn auch das Modul Enterprise Risk aktiv ist. Der ERM Executive wird mittel Notifikation über die Markierung informiert.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzers passen kann der Freigeber Risiko weiter in den Status "Aktiv" schalten, falls vom Management keine explizite "Management Freigabe" durchgeführt werden muss.

> Der Ersteller und Bearbeiter Risiko werden über den Statuswechsel in "Aktiv" mittels Notifikation benachrichtigt.

> Das verantwortliche Management wird mittels Notifikation über den Statuswechsel zu "In Managementfreigabe" benachrichtigt.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.7 Bearbeiter Maßnahme

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.

Folgende Aufgaben hat ein Bearbeiter Maßnahme in BIC GRC:

- Maßnahme definieren & erstellen
- Maßnahme ergänzen & bearbeiten
- Maßnahme aufbauen & planen

- Maßnahme verwalten & umsetzen
- Optional: Maßnahme überprüfen & verbessern
  - Finding identifizieren & erstellen
  - Finding sichten & behandeln

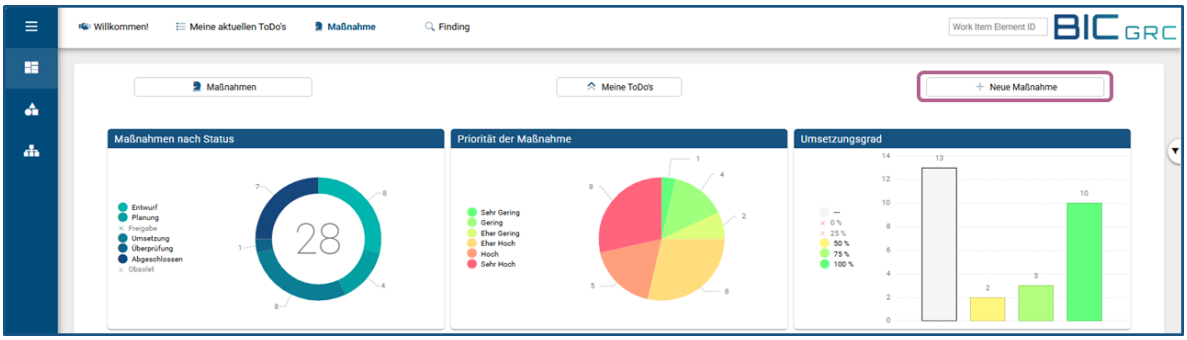
2.7.1 Maßnahme definieren & erstellen

Eine *Maßnahme* kann von mehreren Benutzerprofilen aus unterschiedlichen Modulen und aus verschiedenen Gründen erstellt werden. Durch das Erstellen und die Zuordnung zu einem Asset in der Asset Hierarchie kann eine *Maßnahme* von mehreren Modulen in BIC GRC ausgewählt und verlinkt werden. Dadurch wird das Maßnahmenmanagement zu einem eigenen, wesentlichen Bestandteil von BIC GRC.

Schritt 1: Maßnahme erstellen

1. Erstellung aus Dashboard

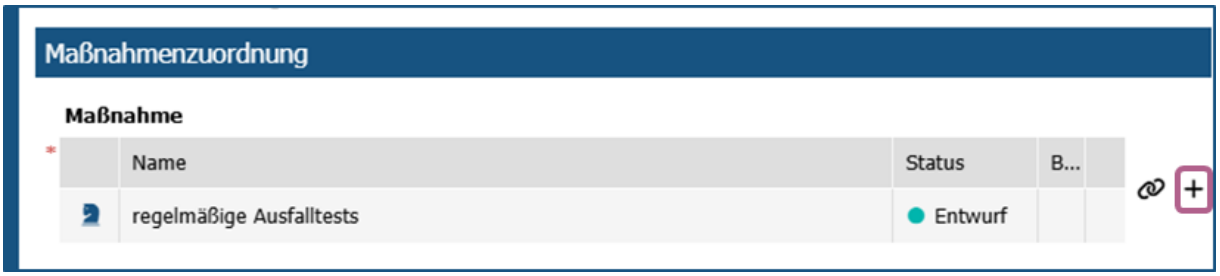
Der Bearbeiter Maßnahme navigiert über die Menüleiste zu **Dashboards >> Übersicht Maßnahme >> "Neue Maßnahme"**



Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung aus anderen Work Items

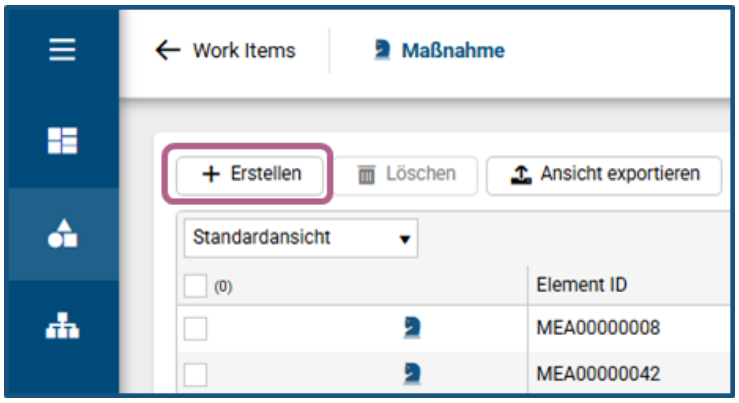
Maßnahmen können aus unterschiedlichen Work Items, wie beispielsweise Risiken, Findings oder Management Reviews resultieren. Erstellt werden sie über einen passenden Link mit Überschrift "Maßnahme" mittels des Icons + oder sie werden verlinkt mittels 🔗.



3. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Maßnahme >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Sowohl bei der Erstellung über Dashboard, als auch bei der Erstellung aus einem anderen Work Item öffnet sich ein neues Fenster des Work Item Types *Maßnahme* .

Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Maßnahme* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Maßnahme* einzigartig.
2. **Scope**: Um den Bereich der Anzeigeverfügbarkeit der *Maßnahme* einzuschränken, muss es einem Asset in der Asset Hierarchie zugeordnet werden.

   Es werden nur Assets des Types "Organisationseinheiten" zugelassen.

   Soll eine *Maßnahme* beispielsweise nur für Standort A und nicht für Standort B gelten, muss der Scope "Standort A" in der Asset-Verlinkung ausgewählt werden. Soll die *Maßnahme* später in BIC GRC erneut verlinkt werden, wird sie nur Benutzern mit Berechtigungen in Standort A angezeigt und keinen Usern die Assets an Standort B verwalten.
3. **GRC Perspektive**: Nach der Auswahl des Scopes wird dem Benutzer die Liste zu den GRC Perspektiven angezeigt.

   Der Bearbeiter kann ein oder mehrere GRC Perspektiven auswählen, in denen er eine Berechtigung für die Erstellung besitzt.

   Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.
4. **Verantwortlichkeiten**: Der Ersteller hat einen "Bearbeiter Maßnahme " zu hinterlegen, der für die Implementierung, Bewertung und Umsetzung der *Maßnahme* verantwortlich ist .

   Weiters ist ein "Freigeber Maßnahme" zu nominieren, der die *Maßnahme* freigibt.

   Dieser Benutzer wird durch das Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

Durch einen hinterlegten Filter müssen der Bearbeiter als auch der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

Es ist zu empfehlen, dass der Ersteller des Work Items *Maßnahme* zugleich der "Bearbeiter Maßnahme " einer *Maßnahme* ist.

5 **Art der Maßnahme**: Die "Art der Maßnahme" kategorisiert sie *Maßnahme*. So kann später ein anderer Benutzer, der die Maßnahme verlinken möchte auf einen Blick sehen, ob die Maßnahme in ihrer Art passt.

Falls keine passende Auswahl dabei ist in der vorgeschlagenen Liste, kann der Benutzer "Sonstige" angeben. Danach erscheint auf der rechten Seite ein Attributsfeld, wo manuell eine "Sonstige Maßnahme" zu schreiben ist.

6 **Priorität**: Für eine *Maßnahme* ist zu hinterlegen, mit welcher "Priorität" die *Maßnahme* umzusetzen ist.

Art und Priorität der *Maßnahme* können später für die Auswertung auf Dashboards verwendet werden, haben aber keinen weiteren Einfluss auf den Workflow.

7 **Beschreibung**: Die *Maßnahme* sollte so genau wie möglich beschrieben und definiert werden, um Benutzer, die im Workflow nachgelagert sind, einen Überblick über die Aufgabe der *Maßnahme* zu gewähren.

8 **Speichern**: Sobald die Informationen angegeben sind kann der Ersteller speichern.

Wenn der Ersteller der *Maßnahme* gleichzeitig der Bearbeiter Maßnahme ist, kann er mit dem nächsten Schritt Bearbeiter Maßnahme - Maßnahme ergänzen & bearbeiten fortfahren.

2.7.2 Maßnahme ergänzen & bearbeiten

Eine *Maßnahme* kann von mehreren Benutzern identifiziert & erstellt werden.

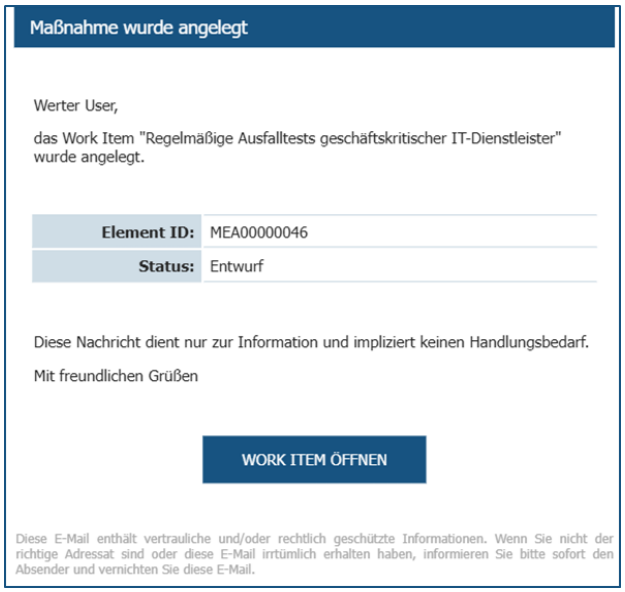
Wenn der Ersteller und der Bearbeiter unterschiedliche Benutzer sind, wird der Bearbeiter gesondert mittels Notifikation über die neue *Maßnahme* informiert. Die folgenden Schritte 1 & 2 beziehen sich auf die Tätigkeiten nach der Erstellung durch einen anderen Benutzer.

Optional Schritt 1: Navigation zu spezifischer Maßnahme nach Fremderstellung

Der Bearbeiter hat zwei Möglichkeiten, eine zu bearbeitende *Maßnahme* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "NEW" abgeschlossen hat. Der Link zu der spezifischen *Maßnahme* befindet sich in der Notifikation.



2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

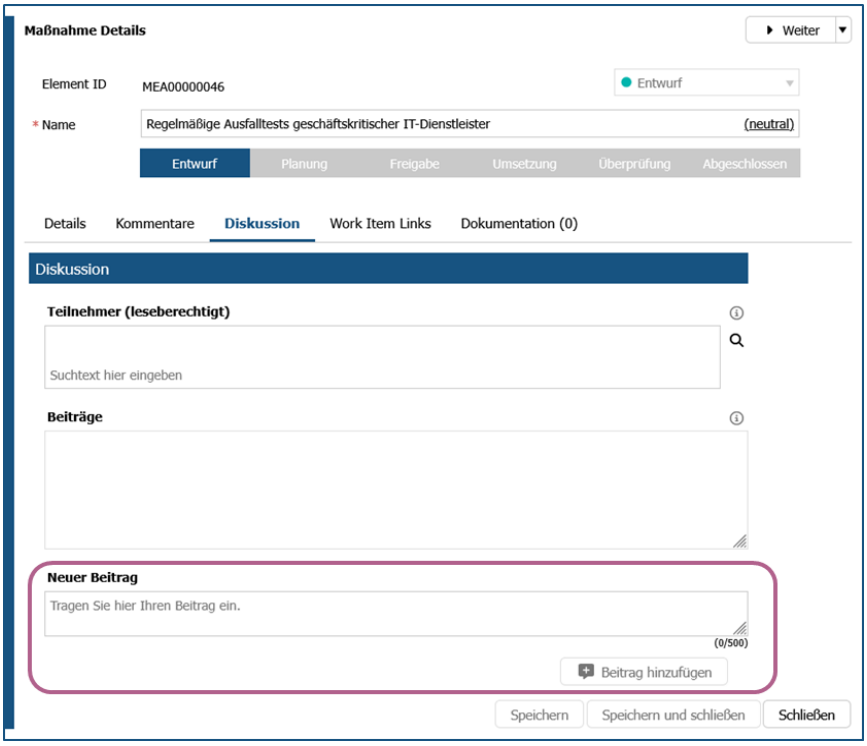
Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter noch eine Aufgabe zu erledigen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Maßnahme* automatisch.

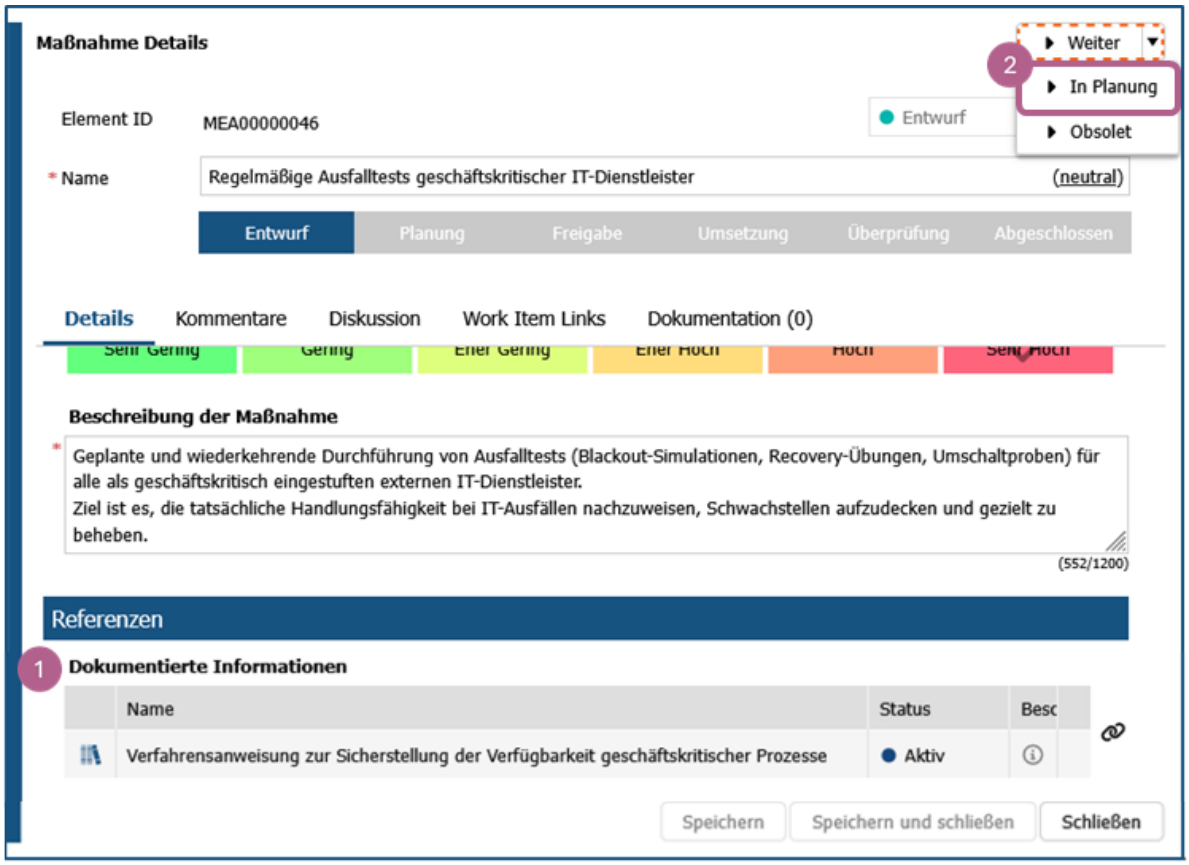
Optional Schritt 2: Überprüfung der Eingaben des Erstellers

Wenn der Ersteller und der Bearbeiter nicht derselbe Benutzer sind, empfiehlt es sich, als ersten Schritt im Work Item *Maßnahme* zu dem Tab *"Details"* zu gehen, um die Detaileingaben des Erstellers einzusehen.

Sollten die Eingaben des Erstellers nicht richtig oder unvollständig sein, kann der Bearbeiter einen Beitrag im Tab *"Diskussion"* hinterlassen. Der Ersteller wird anschließend über den Beitrag mittels Notifikation informiert.



Schritt 3: Eingaben ergänzen



1. **Dokumentierte Informationen**: Der Bearbeiter Maßnahme kann ein oder mehrere *Dokumentierte Informationen* hinterlegen.

> *Dokumentierte Informationen* unterstützen insbesondere im Informationssicherheitsbereich um Effizienz und Nachvollziehbarkeit zu verbessern, können aber auch in anderen Modulen dazu beitragen Transparenz zu schaffen.

2. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Planung" durchgeführt.

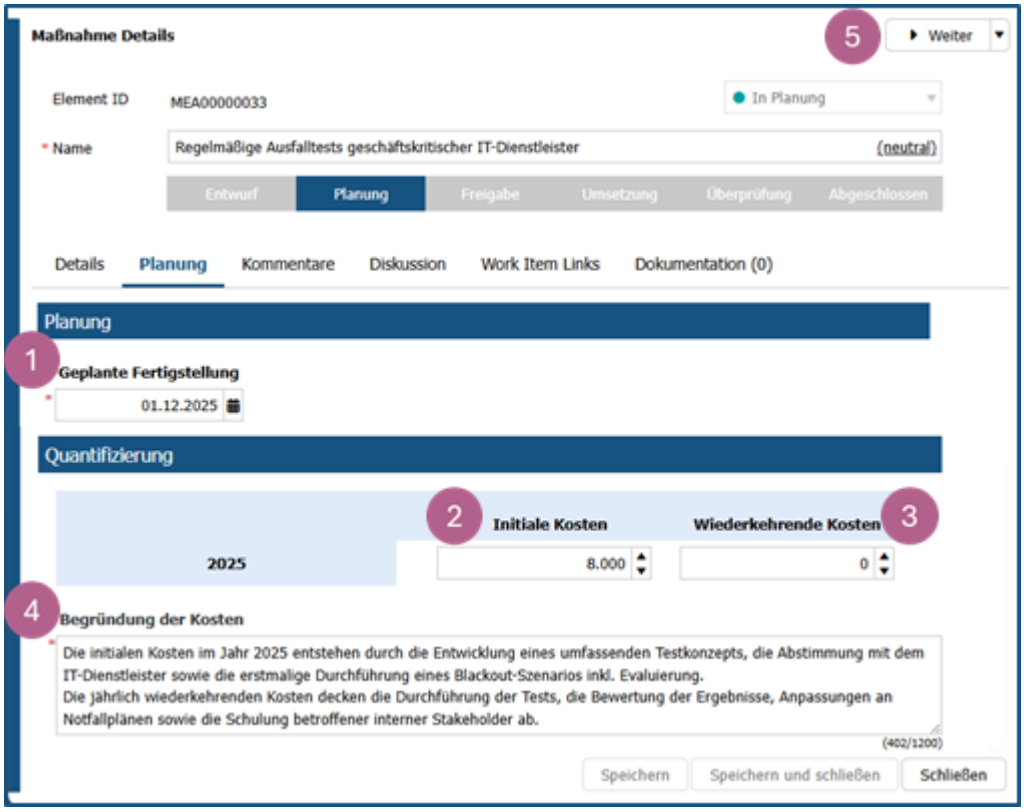
> Der Bearbeiter kann anschließend mit dem nächsten Schritt Maßnahme aufbauen & planen fortfahren.

2.7.3 Maßnahme aufbauen & planen

Der Bearbeiter Maßnahme übernimmt bei einer spezifischen *Maßnahme* die monetäre Bewertung der Kosten und die Verantwortung für die Umsetzung in einem geplanten Zeitraum.

Der Bearbeiter kann direkt nach dem Maßnahme ergänzen & bearbeiten fortfahren oder mittels des **Dashboards >> Meine aktuellen ToDo's** zu der *Maßnahme* navigieren.

Schritt 1: Planung vornehmen



1. **Geplante Fertigstellung**: Der Bearbeiter hinterlegt bis wann die *Maßnahme* ohne Verzögerung fertiggestellt werden sollte. Diese Information ist wichtig für die Umsetzung der Maßnahme.
2. **Initiale Kosten**: Die "Initialen Kosten" geben an, wie hoch die Kosten im Jahr der Anschaffung sind. .
3. **Wiederkehrende Kosten**: Die "Wiederkehrenden Kosten" beschreiben die Kosten, die im Anschluss an die Umsetzung jährlich zu erwarten sind.
4. **Begründung**: Für die Nachvollziehbarkeit der Angaben der Kosten hat der Bearbeiter eine Begründung anzugeben wie die Kosten zustande kommen.

> Wenn es beispielsweise Rechnungen oder andere Dokumentationen dazu gibt, wie sich die Kosten der *Maßnahme* zusammensetzen, kann auch der Tab "*Dokumentation*" verwendet werden, um die Dokumente revisionssicher zu hinterlegen.

5. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Freigabe" durchgeführt.

> Der nächste Status wird von Freigeber Maßnahme - Maßnahme überprüfen & freigeben durchgeführt. Der eingetragene Freigeber Maßnahme wird mittels Notifikation über den Statuswechsel informiert.

Sollten die Eingaben nicht richtig oder unvollständig sein, kann der Freigeber Maßnahme einen Kommentar in dem Tab "*Kommentar*" hinterlassen und die *Maßnahme* erneut in den Status "Planung" setzen. Der Bearbeiter Maßnahme wird über diesen Vorgang mittels Notifikation benachrichtigt.

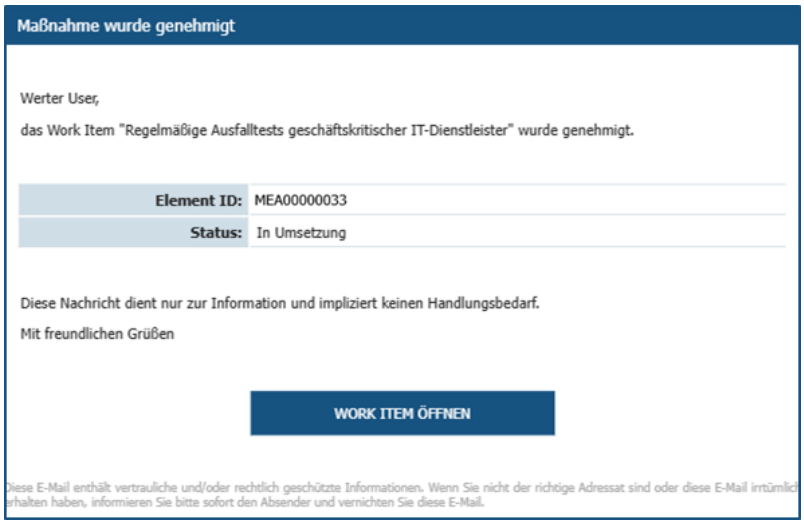
2.7.4 Maßnahme verwalten & umsetzen

Schritt 1: Navigation zu spezifischer Maßnahme

Der Bearbeiter Maßnahme hat zwei Möglichkeiten, eine zu bewertende *Maßnahme* zu öffnen.

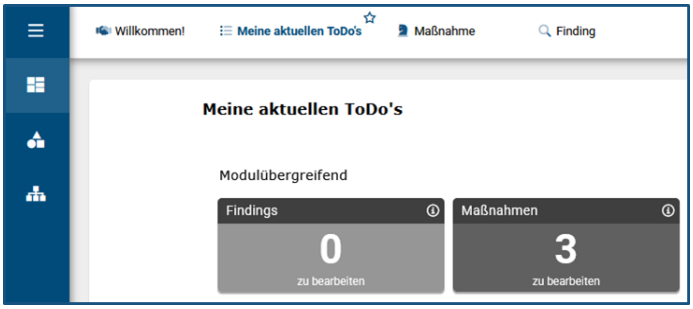
1. Öffnen über Notifikation

Der Bearbeiter Maßnahme bekommt eine E-Mail zugesendet, sobald der Freigeber freigegeben und einen Statusübergang zu "Umsetzung" durchgeführt hat. Der Link zu der spezifischen *Maßnahme* befindet sich in der Notifikation.



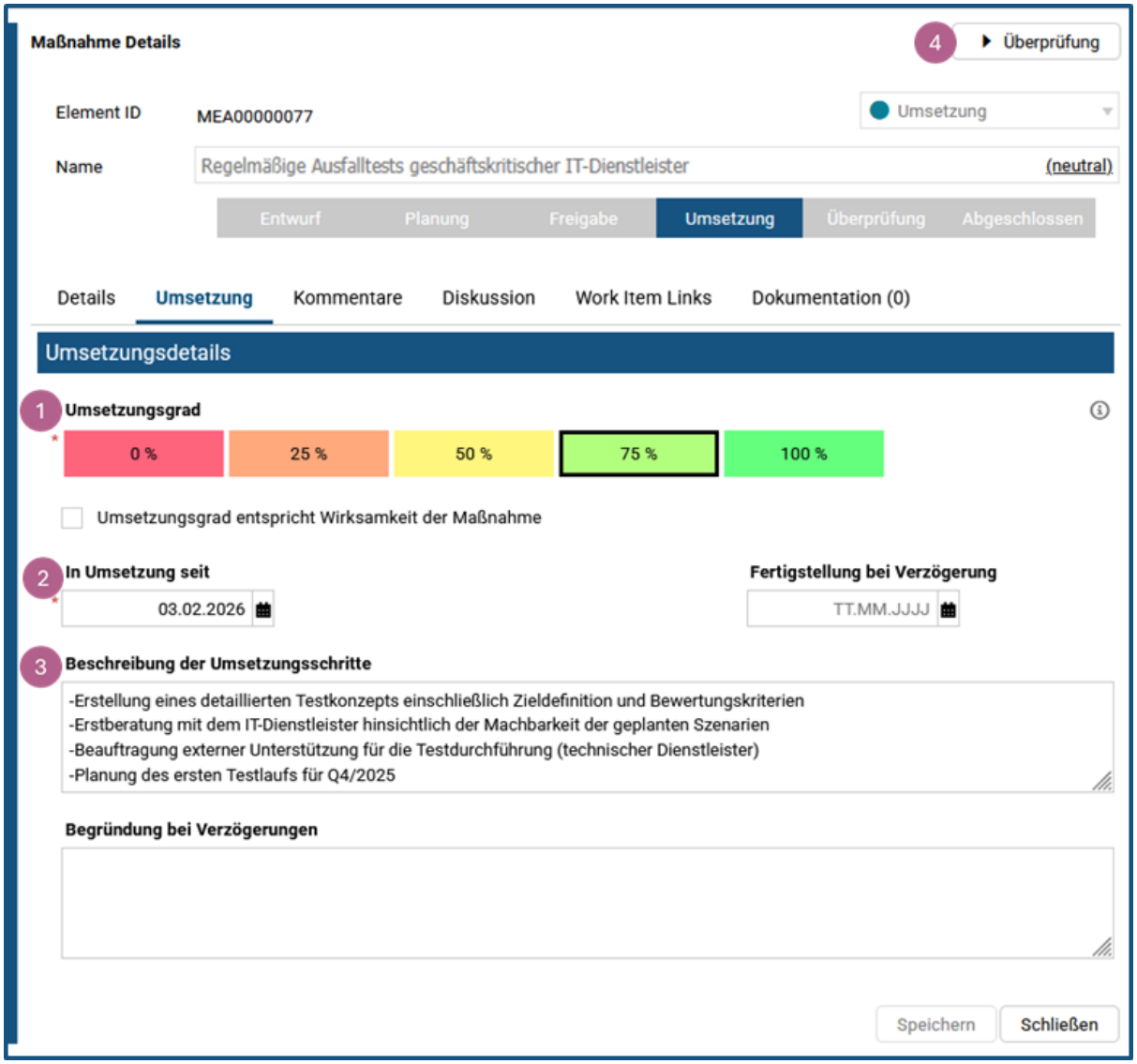
2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter Maßnahme noch eine Umsetzung durchzuführen hat.



Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die "Maßnahme" automatisch. Der Bearbeiter Maßnahme steigt direkt in den Tab "*Umsetzung*" ein.

Schritt 2: Umsetzung dokumentieren



1 **Umsetzungsgrad und -wirksamkeit**: Der Bearbeiter Maßnahme kann den Grad der Umsetzung in 5 -Stufen bewerten, abhängig vom Reifegrad der *Maßnahme*. Weiters hat er die Möglichkeit, durch das Anklicken einer Checkbox anzugeben, ob die *Maßnahme* erst bei vollständiger Implementation wirkt oder schon Zwischenergebnisse wirksam sind.

> So ist beispielsweise eine Versicherung erst bei Unterschrift zu 100% wirksam, bei der Installation von 75% aller geplanter Feuerlöscher sind diese aber auch schon ohne 100%ige Implementierung teilweise wirksam.

2 **Daten**: Das Datumsattribut „In Umsetzung seit“ wird von BIC GRC automatisch gesetzt, wenn der Freigeber Maßnahme den Statusübergang der *Maßnahme* von „In Freigabe“ zu „In Umsetzung“ weiterschaltet. Das „Fertigstellungsdatum“ ist gleich dem „Geplanten Fertigstellungsdatum“, das vom Bearbeiter Maßnahme hinterlegt wurde.

> Ist das „Fertigstellungsdatum“ bereits überschritten und die Maßnahme noch nicht

final umgesetzt, wird ein neues Datumsattribut "Fertigstellung bei Verzögerung" sichtbar. Dieses neue Datum ist verpflichtend einzutragen.

Das Fertigstellungsdatum ergibt sich bei Überschreitung des heutigen Datums aus dem Maximum aus "Geplanten Fertigstellungsdatum" und "Fertigstellung bei Verzögerung".

3 **Beschreibung der Umsetzungsschritte**: Für die Nachvollziehbarkeit der Angaben der einzelnen Umsetzungsschritte hat der Bearbeiter eine detaillierte Beschreibung zu hinterlegen.

Falls das geplante "Fertigstellungsdatum" nicht eingehalten werden kann, muss der Bearbeiter nicht nur ein neues, realistisches Datum angeben, sondern auch eine Begründung, warum das ursprüngliche Datum nicht eingehalten werden konnte.

4 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Überprüfung" oder "Abgeschlossen" durchgeführt.

Der Bearbeiter kann anschließend mit dem optionalen Schritt Optional: Bearbeiter Maßnahme - Maßnahme überprüfen & verbessern fortfahren.

Sollte die *Maßnahme* ohne Überprüfung in den Status "Abgeschlossen" wechselt, wird der Freigeber der *Maßnahme* mittels Notifikation benachrichtigt.

2.7.5 Optional: Maßnahme überprüfen & verbessern

Das Management kann auf eine Überprüfung der Maßnahme mittels eines zusätzlichen Workflow Status bestehen. Dafür ist der Bearbeiter Maßnahme nach Abschluss der Umsetzung verantwortlich.

Schritt 1: Navigation zur Maßnahme

Der Bearbeiter Maßnahme hat zwei Möglichkeiten, eine *Maßnahme* zu bearbeiten/öffnen.

1. Direkter Anschluss an Maßnahmenumsetzung

Der Bearbeiter Maßnahme ist bereits in der *Maßnahme*, da er gerade den Status "Umsetzung" abgeschlossen hat.

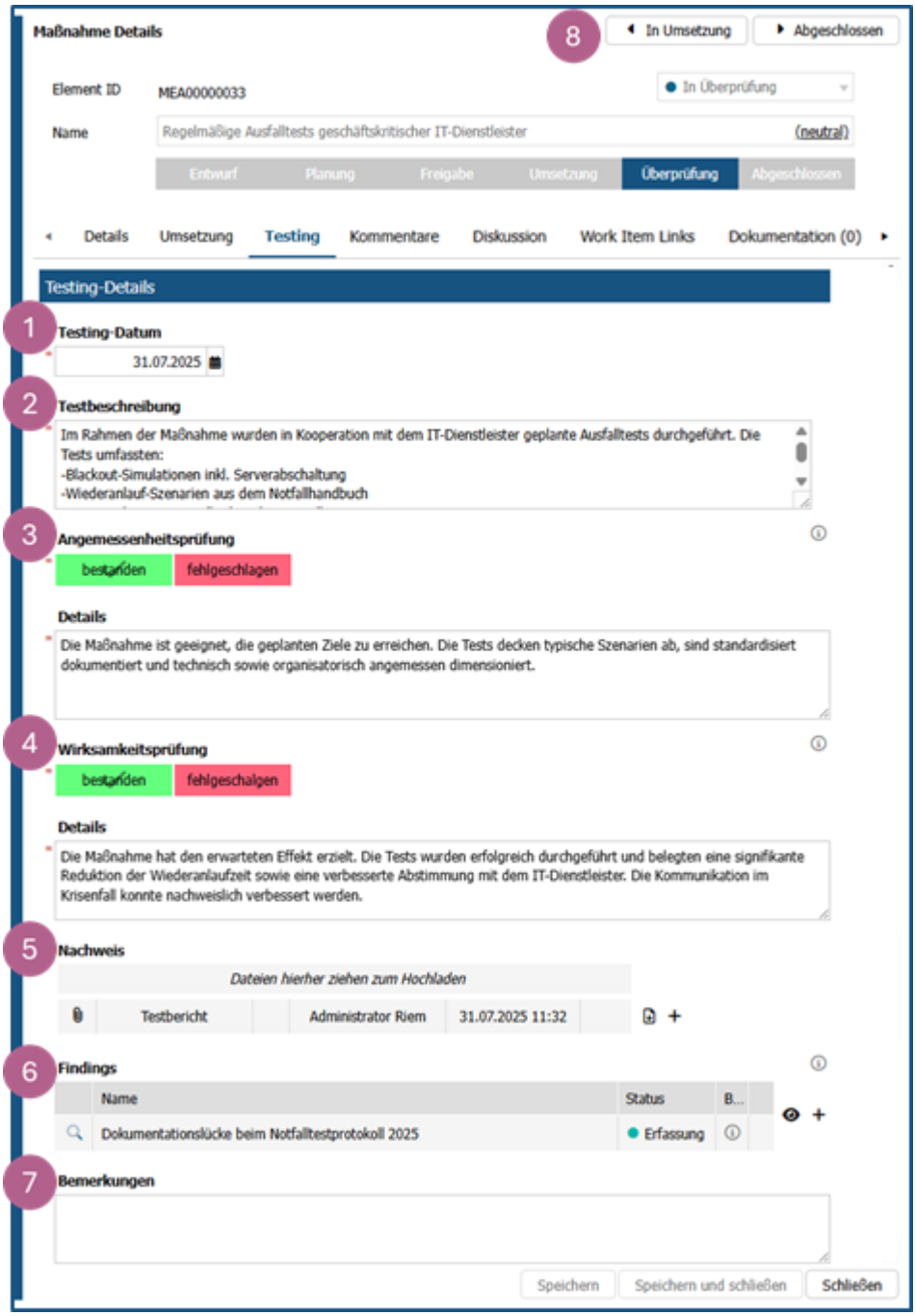
2. Öffnen über Dashboard "Meine ToDo`s"

Im oberen Teil des Dashboards "Meine ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigt. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter Maßnahme eine Überprüfung durchzuführen hat.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Maßnahme* automatisch.

Schritt 2: Überprüfung durchführen

Der Bearbeiter Maßnahme hat in der erstellten, bewerteten und umgesetzten *Maßnahme* optional die Aufgabe zu entscheiden, ob die Maßnahme Angemessen und Effektiv ist.



1. **Testing Datum**: Hier hat der Bearbeiter anzugeben, an welchem Tag er das Testing der *Maßnahme* durchgeführt hat.
2. **Testbeschreibung**: Der Bearbeiter sollte in wenigen Worten beschreiben, was er getestet und überprüft hat, um nachvollziehen zu können auf welcher Grundlage das Testing erfolgt ist.
3. **Angemessenheitsprüfung**: Der Bearbeiter kann im Rahmen des *Maßnahmen-Testings* die Angemessenheit der *Maßnahme* feststellen und mittels "Bestanden" oder "Fehlgeschlagen" einordnen.
4. **Wirksamkeitsprüfung**: Neben der Angemessenheit muss der Bearbeiter überprüfen, ob die *Maßnahme* in ihrer Art und Beschaffenheit wirksam ist. Die Einordnung erfolgt hier mittels "Bestanden" oder "Fehlgeschlagen".

> Der Test der Wirksamkeit wird erst angezeigt, wenn die Angemessenheitsprüfung erfolgreich war.

5 **Nachweis Dokumentation**: An dieser Stelle können Dokumente als Link, Memo oder Datei verlinkt werden. Es sollen alle Informationen hinterlegt werden, die als Nachweis gelten.

> Handelt es sich um eine Datei, kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend im Attributsfeld verlinkt.

6 **Finding**: Der Link, um ein *Finding* zu hinterlegen, ist immer sichtbar. Sollte allerdings die "Angemessenheitsprüfung" oder der "Wirksamkeitsnachweis" fehlgeschlagen sein, muss ein *Finding* verpflichtend angegeben werden. Hierfür kann der Bearbeiter über das Icon + ein neues *Finding* erstellen. Mehr dazu unter Bearbeiter Maßnahme - Finding identifizieren & erstellen.

7 **Bemerkung**: Sollte noch etwas in der *Maßnahme* zu ergänzen sein, dass in den anderen Attributsfeldern nicht passend wäre, kann dies hier festgehalten werden.

8 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Abgeschlossen" durchgeführt.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

> Der Freigeber der *Maßnahme* wird über den Statusübergang zu "Abgeschlossen" mittels Notifikation benachrichtigt.

2.7.6 Finding identifizieren & erstellen

Sollte der Bearbeiter Maßnahme während der Überprüfung einer *Maßnahme* zu der Erkenntnis kommen, dass entweder die "Angemessenheitsprüfung" und/oder der "Wirksamkeitsnachweis" mit einem negativen Ergebnis abschließen werden, muss der Bearbeiter Maßnahme ein *Finding* erstellen.

Schritt 1: Finding aus Maßnahme erstellen

Ein *Finding* kann aus einer *Maßnahme* erstellt werden. Sollte das Ergebnis der "Angemessenheitsprüfung" oder der "Wirksamkeitsprüfung" in der *Maßnahme* als "Fehlgeschlagen" eingeordnet werden, muss verpflichtend ein Finding erstellt werden.

Die Erstellung erfolgt durch das Icon + nach dem Abschnitt "Wirksamkeitsnachweis".

> Das *Finding* geht automatisch in der *Maßnahme* auf.

Schritt 2: Finding dokumentieren

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Finding* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Finding* einzigartig.
2. **GRC-Perspektive**: Die Perspektive wird automatisch aus der *Maßnahme* übernommen und gesetzt.
3. **Bearbeiter**: In das Attribut wird bei der Erstellung automatisch der "Bearbeiter Maßnahme" der *Maßnahme* gesetzt.
4. **Datum der Meldung**: Der Bearbeiter Maßnahme muss eingeben, wann er das *Finding* offiziell gemeldet/entdeckt hat. Daher muss das Datum nicht mit dem tagesaktuellen Datum übereinstimmen.
5. **zu behandeln bis**: Unter dem Datum wird jenes Datum verstanden, bis zu dem das *Finding* behoben werden sollte. Es soll einen Hilfestellung sein, um eine Orientierung für im Workflow nachgelagerte User zu geben, bis wann die Behebung des *Findings* wünschenswert wäre.
6. **Art des Findings**: Der Bearbeiter Maßnahme kann im Rahmen von fünf Stufen einordnen, wie bedenklich das *Finding* im Kontext der Angemessenheit oder Wirksamkeit der *Maßnahme* ist.
7. **Finding für dieses Asset**: Das Asset wird automatisch aus dem Work Item übernommen aus dem es erstellt wurde.
8. **Beschreibung des Findings**: Die "Beschreibung des Findings" soll so viele Informationen und Inputs wie möglich enthalten, beispielsweise wie das *Finding* entdeckt wurde. Weiters kann möglicherweise Rückschlüsse auf Ursache und Wirkung entstehen.
9. **Priorität des Findings**: Dem *Finding* kann eine Priorität hinterlegt werden, die später für Auswertungen auf beispielsweise Dashboads verwendet werden kann.
10. **Statuswechsel**: Der Bearbeiter Maßnahme kann abschließend in den Status "Behandlung" schalten. Mehr Informationen zu dem Statuswechsel in Finding sichten & behandeln.

> Anschließend kann der Bearbeiter Maßnahme in die *Maßnahme* zurückkehren und mit der Dokumentation der Überprüfung der *Maßnahme* fortfahren. Bearbeiter_Maßnahme_-_Maßnahme überprüfen & verbessern.

2.7.7 Finding verwalten & behandeln

Ein Bearbeiter bekommt eine Notifikation zugesendet, wenn er als Bearbeiter in einem *Finding* eingetragen wurde. Seine Aufgabe ist es im *Finding* passende Maßnahmen zu definieren, um das *Finding* angemessen zu behandeln.

Schritt 1: Navigation zu spezifischem Finding nach Fremderstellung

Der Bearbeiter hat zwei Möglichkeiten ein zu bearbeitendes *Finding* zu öffnen.

1. Öffnen über Notifikation

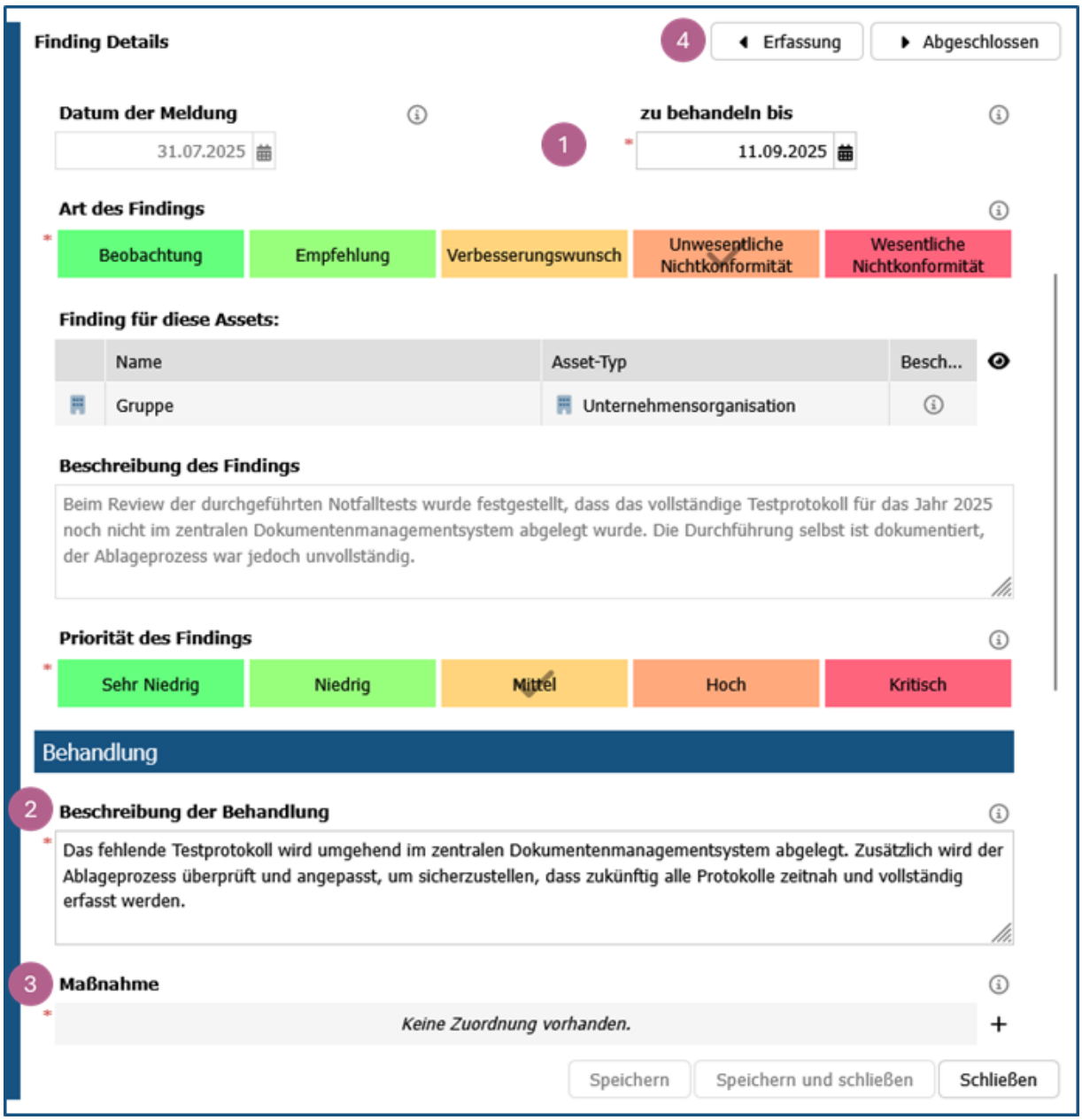
Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "Erfassung" abgeschlossen hat. Der Link zu dem spezifischen *Finding* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen To's"

Der Bearbeiter kann in dem Dashboard seine aktuellen *Findings* sehen.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Finding* automatisch.

Schritt 2: Finding behandeln



1. **Angaben überprüfen**: Als erstes kann der Bearbeiter bei Bedarf die Einschätzungen des Erstellers überarbeiten. So kann er das "zu behandeln bis"-Datum so setzen, dass es für ihn realistisch ist. Zudem kann er die "Art des Findings" und die "Priorität des Findings" neu einschätzen.
2. **Beschreibung der Behandlung**: Danach sollte der Bearbeiter beschreiben wie er das *Finding* behandeln möchte. Dies passiert im ersten Schritt schriftlich, bevor konkrete *Maßnahmen* dazu erstellt werden.
3. **Maßnahme**: Das *Finding* wird durch eine *Maßnahme* behandelt. Mehr Informationen über die Erstellung einer Maßnahme unter Bearbeiter Maßnahme - Maßnahme definieren & erstellen Schritt 2.

> Es ist im *Finding* nur möglich neue *Maßnahmen* zu erstellen und keine bestehenden *Maßnahmen* zu verlinken.

4 **Statuswechsel**: Der Bearbeiter kann abschließend in den Status "Abgeschlossen" weiterschalten.

> Der Ersteller wird über den Statusübergang mittels Notifikation benachrichtigt.

2.8 Freigeber Maßnahme

Benutzer mit dem Benutzerprofil Freigeber Maßnahme haben die Verantwortung für eine oder mehrere spezifische *Maßnahme(n)* in BIC GRC. In einer *Maßnahme* können nur jene Freigeber hinterlegt werden, die auch die entsprechenden Berechtigung für das Asset haben.

Folgende Aufgabe hat der Freigeber Maßnahme in BIC GRC:

- Maßnahme überprüfen & freigeben

Zusätzlich darf er Maßnahmen erstellen und sie nach der Erstellung einem Bearbeiter Maßnahme zuweisen. Informationen zu der Erstellung einer Maßnahme unter Bearbeiter Maßnahme - Maßnahme definieren & erstellen.

2.8.1 Maßnahme überprüfen & freigeben

Nach der Erstellung und Planung einer *Maßnahme* durch einen Erfasser bzw. einen Bearbeiter , muss diese vor der Umsetzung einer Freigabe durch den Freigeber der Maßnahme überprüft werden.

Schritt 1: Navigation zur Maßnahme

Der Freigeber Maßnahme hat zwei Möglichkeiten, eine *Maßnahme* zu öffnen.

1. Öffnen über Notifikation

Der Freigeber Maßnahme bekommt eine E- Mail zugesendet, sobald der Bearbeiter Maßnahme den Status der *Maßnahme* zu "Freigabe" wechselt. Der Link zu der spezifischen *Maßnahme* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

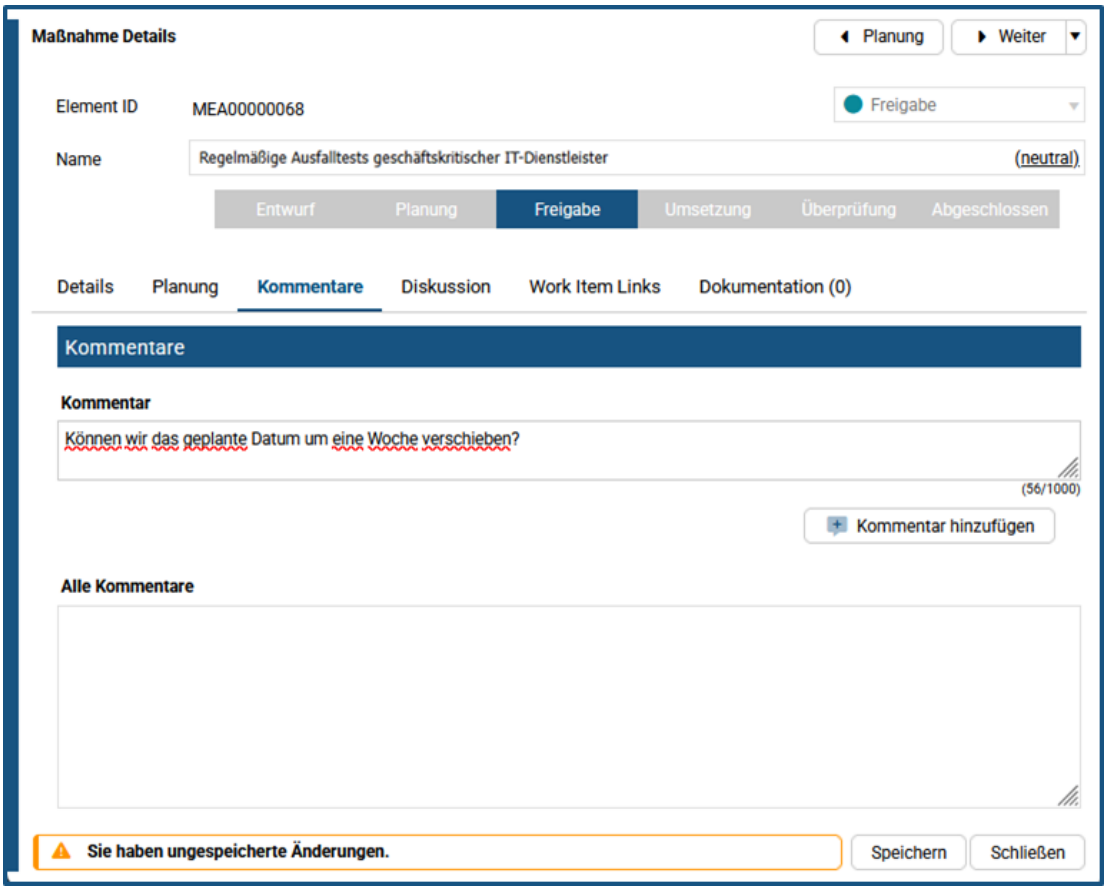
Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigt. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber Maßnahme eine Überprüfung durchzuführen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich automatisch ein neues Fenster für die *Maßnahme*.

Schritt 2: Freigabe durchführen

Der Freigeber Maßnahme hat in der erstellten und geplanten *Maßnahme* alle Leserechte, um auf Basis aller eingegebenen Informationen zu entscheiden, ob die *Maßnahme* in einem ausreichenden Ausmaß beschrieben und geplant wurde. Wenn dies der Fall ist, kann der Freigeber Maßnahme in Status "Umsetzung" weiterschalten.

Sollte dies nicht der Fall sein und muss die *Maßnahme* aus Sicht des Freigebers erneut bewertet werden, kann der Freigeber einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "Planung" durchführen.



Nach dem Statusübergang kann das Fenster geschlossen werden.

Nach dem Speichervorgang wird der eingetragene Bearbeiter Maßnahme mittels Notifikation benachrichtigt.

2.9 Bearbeiter Kontrolle

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.

Folgende Aufgaben hat ein Bearbeiter Kontrolle in BIC GRC:

- Kontrolle ableiten & erstellen
- Kontrolle bearbeiten & prüfen
- Kontroll-Testing einleiten & erstellen
  - Finding sichten & behandeln
- Kontroll-Testing überprüfen & freigeben

Der Bearbeiter Kontrolle kann darüber hinaus noch *Maßnahmen* aus einem *Finding* erstellen in BIC GRC. An dieser Stelle auf das Benutzerprofile "Bearbeiter Maßnahme" verwiesen:

- Maßnahme definieren & erstellen

2.9.1 Kontrolle ableiten & erstellen

In BIC GRC können unterschiedliche Benutzer eine *Kontrolle* erstellen. Dabei kann dies durch Erstellung aus anderen Work Items (z.B. Risiken) oder eine manuelle Einzelerstellung (Bottom-Up) erfolgen.

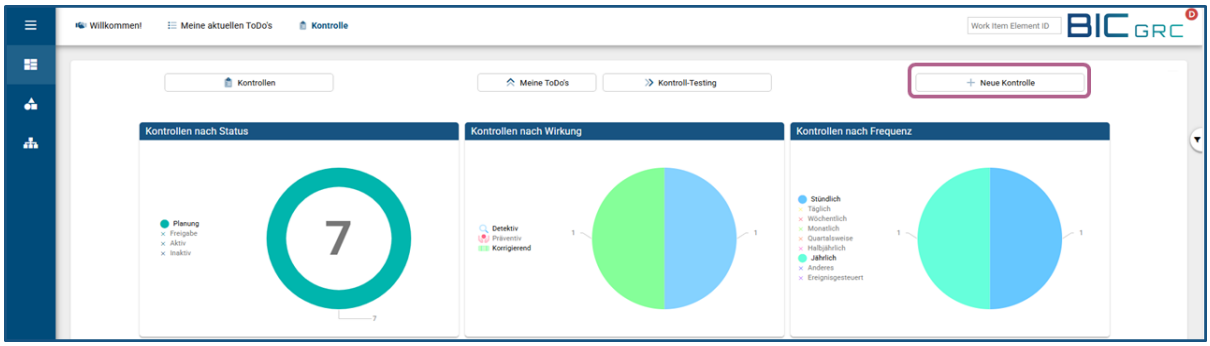
Schritt 1: Kontrolle erstellen

Der Bearbeiter Kontrolle hat zwei Möglichkeiten eine *Kontrolle* zu erstellen.

1. Erstellen über Dashboard "Kontrolle"

Der Bearbeiter Kontrolle navigiert über die Menüleiste zu **Dashboards >> Übersicht Kontrolle >> "Neue Kontrolle"**

Die Erstellung einer neuen *Kontrolle* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

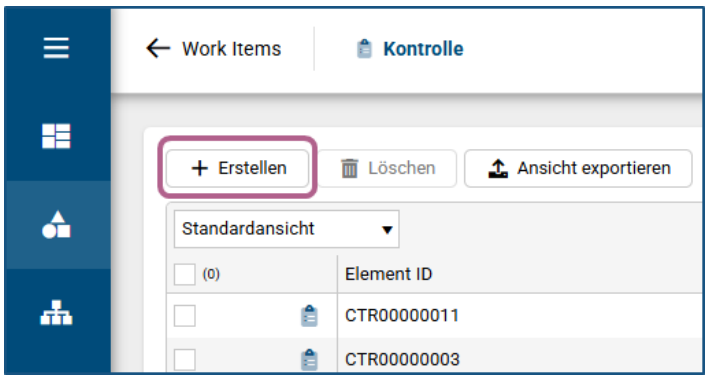


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Kontrolle >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Kontrolle* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Kontrolle* einzigartig.

2. **Scope**: Der Scope gibt an in welchem der Bereich bzw. Prozess die *Kontrolle* angewendet werden soll.

   Im Hintergrund filtert ein Filter auf Assets der Typen "Organisationseinheit" und "Primary Asset".

   Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer keine Rolle auf dem Asset zugewiesen, das er verlinken möchte. Mittels des Work Items *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

3. **GRC Perspektive**: Nach der Auswahl des Scopes wird dem Benutzer die Liste zu den GRC Perspektiven angezeigt.

   Der Bearbeiter kann ein oder mehrere GRC Perspektiven auswählen, in denen er eine Berechtigung für die Erstellung besitzt.

   Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.

4. **Verantwortliche Personen**: Es muss ein Benutzer im Attribut "Bearbeiter" hinterlegt werden und zusätzlich ein "Freigeber" der für die Freigabe der *Kontrolle* verantwortlich ist.

   Durch einen hinterlegten Filter müssen der Bearbeiter als auch der Freigeber einem bestimmten Benutzerprofil am Asset zugeordnet sein, um dem Ersteller angezeigt zu werden.

   Dieser Benutzer wird durch das Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

5. **Kontrollebene**: Die "Kontrollebene" bestimmt, ob eine Kontrolle vom Management (Top-Down) anfordert wird oder ob es sich um eine Bottom-Up erstellte *Kontrolle* handelt.
6. **Art der Kontrolle**: Es kann bestimmt werden, ob die *Kontrolle* als "Hauptkontrolle" zu einem Prozess geführt wird, oder als eine "Unterstützende Kontrolle", wenn z.B. beim *Kontroll-Testing* identifiziert wurde, dass die bestehende "Hauptkontrolle" nicht ausreichend ist.
7. **Beschreibung der Kontrolle**: Die Kontrollbeschreibung soll so viele Informationen und Inputs wie möglich enthalten, sodass der Kontrolldurchführer im Anschluss genau informiert ist, was seine Aufgabe während der *Kontrolldurchführung* ist
8. **Speichern**: Sobald die Informationen angegeben sind kann der Benutzer speichern.

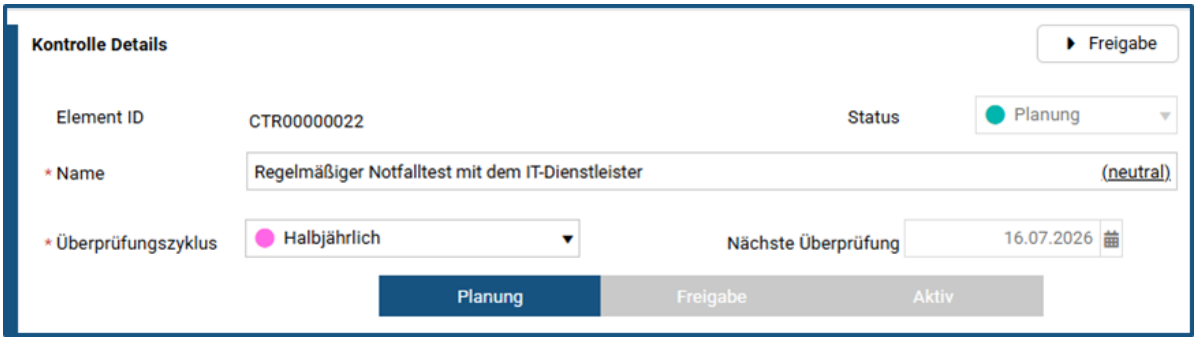
Ansonsten wird der hinterlegte Bearbeiter Kontrolle nach dem Speichervorgang mittels Notifikation über den Statusübergang benachrichtigt.

Schritt 3: Zuordnung finalisieren

Der Bearbeiter sollte die *Kontrolle* regelmäßig dahingehend überprüfen, ob die *Kontrolle* in seiner Art und Weise noch aktuell und korrekt ist.

Um dies in regelmäßigen Abschnitten zu überprüfen, unterstützt das Feld "Nächste Überprüfung". Zwei Wochen vor dem erreichen des Datums bekommt der Bearbeiter eine Notifikation automatisch zugesendet, die ihn an eine bevorstehende Neubewertung erinnert.

An dem Tag der "Nächsten Bewertung" wird die *Kontrolle* im Status "Aktiv" in den Status "Planung" geschalten und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.



Das Datum wird nach dem Statuswechsel automatisch neu gesetzt abhängig von der Zeitangabe im "Überprüfungszyklus".

Wenn die *Kontrolle* einer der Überprüfungszyklen "Alle ... Tage", "Anlassbezogen", "Täglich" oder "Wöchentlich" hat, wird der Status nicht automatisch zurückgesetzt und der Bearbeiter wird nicht über einen Statusübergang mittels Notifikation benachrichtigt.

Wenn der Ersteller der Kontrolle gleichzeitig der Bearbeiter Kontrolle ist, kann er mit dem nächsten Schritt Bearbeiter Kontrolle - Kontrolle ergänzen & bearbeiten fortfahren.

2.9.2 Kontrolle bearbeiten & prüfen

Ein *Kontrolle* kann von mehreren Benutzern identifiziert & erstellt werden.

Wenn der Ersteller und der Bearbeiter unterschiedliche Benutzer sind, wird der Bearbeiter gesondert mittels Notifikation über die neue *Kontrolle* informiert. Die folgenden Schritte 1 & 2 beziehen sich auf die Schritte nach der Erstellung durch einen anderen Benutzer.

Optional Schritt 1: Navigation zu spezifischem Kontrolle nach Fremderstellung

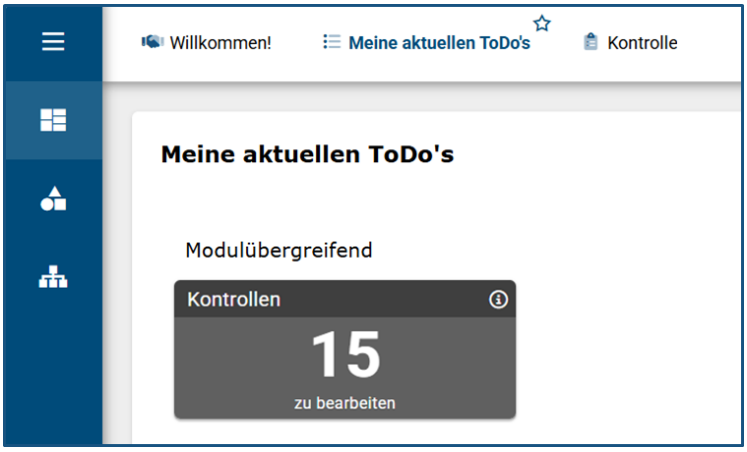
Der Bearbeiter hat zwei Möglichkeiten, ein zu bearbeitendes *Kontrolle* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "NEW" abgeschlossen hat. Der Link zu der spezifischen *Kontrolle* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter noch eine Aufgabe zu erledigen hat.

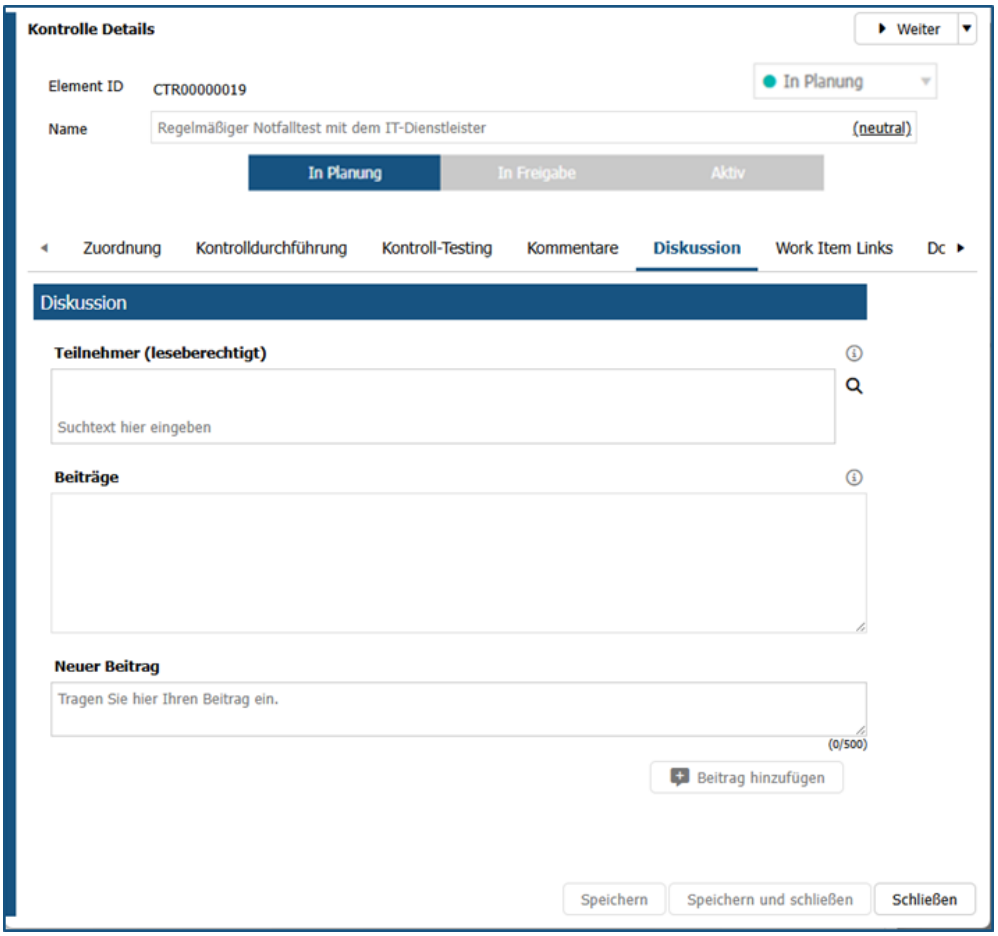


> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontrolle* automatisch. Der Bearbeiter steigt direkt in den Tab *"Zuordnung"* der *Kontrolle* ein.

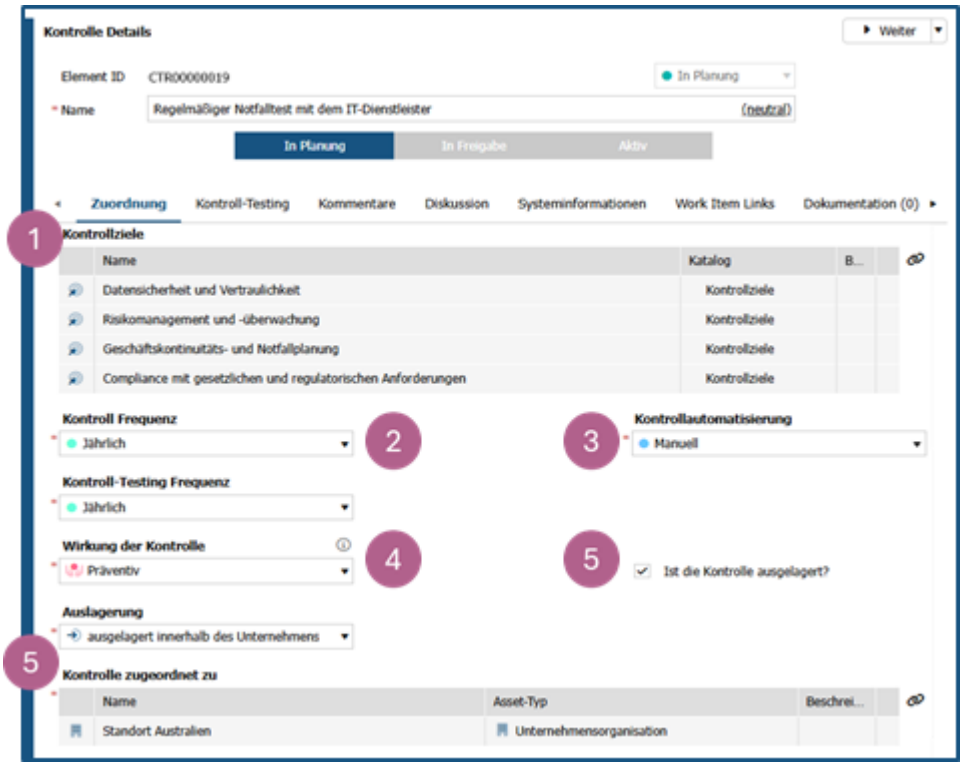
Optional Schritt 2: Überprüfung der Eingaben des Erstellers

Wenn der Ersteller und der Bearbeiter nicht derselbe Benutzer sind, empfiehlt es sich, als ersten Schritt im Work Item *Kontrolle* zu dem Tab *"Zuordnung"* zu gehen, um die Detaileingaben des Erstellers einzusehen.

Sollten die Eingaben des Erstellers nicht richtig oder unvollständig sein, kann der Bearbeiter einen Beitrag im Tab *"Diskussion"* hinterlassen. Der Ersteller wird anschließend über den Beitrag mittels Notifikation informiert.



Schritt 3: Kontrolle ergänzen



1. **Kontrollziel**: Bei dem "Kontrollziel" können aus einem GRC Framework ein oder mehrere passende Ziele verlinkt werden, denen die *Kontrolle* zu Grunde liegt.

> In dem GRC Framework wurden einige Beispiele hinterlegt, wie "Zugriffskontrolle", die vom Management ergänzt werden sollten. Wenn die *Kontrolle* beispielsweise dem Kontrollziel "Zugriffskontrolle" unterliegt, dann soll das Ziel der Kontrolle sein, dass bei einer gut funktionierenden *Kontrolle*, nur berechtigte Personen Zugriff auf z.B. ein System haben.

2. **Frequenzen**: In der *Kontrolle* können zwei Arten von Frequenzen hinterlegt werden:
   - Frequenz der Kontrolle: In welchen zeitlichen Abständen soll die Kontrolle durchgeführt werden.

     > Die Frequenz wird später auch für die *Kontrolldurchführung* herangezogen.

   - Frequenz des Kontroll-Testings: In welchen zeitlichen Abständen soll die Kontrolle auf Angemessenheit und Effiktivität überprüft werden.

     > Die Frequenz wird später auch für das *Kontroll-Testing* herangezogen.

3. **Kontrollautomatisierung**: In diesem Attributsfeld werden die drei gängigsten Angaben "Manuell", "Halbautomatisch" oder "Automatisch" angezeigt.

> Abhängig von der Wahl, wird dem Bearbeiter Kontrolle bei "Halbautomatisch" oder "Automatisch" noch zusätzlich ein Link zu "Verwendete IT-System" eingeblendet. Dieser Link ist verpflichtend auszufüllen, wenn es sich um die Auswahl "Automatisch" handelt.

4. **Wirkung der Kontrolle**: Eine *Kontrolle* kann vorbeugend - also präventiv - oder detektiv sein. Eine entsprechende Wahl über den Zweck muss hier angegeben werden.
5. **Kontrollauslagerung**: Wird die *Kontrolle* nicht innerhalb des Prozesses/ der Organisationseinheit durchgeführt, kann hier alternativ angegeben werden, wohin die *Kontrolle* ausgelagert ist. Die *Kontrolle* kann dabei innerhalb des Unternehmens oder außerhalb des Unternehmens durchgeführt werden.

   Sollte die *Kontrolle* innerhalb des Unternehmens ausgelagert sein, erscheint bei der entsprechenden Auswahl "Auslagerung" ein Link zur Asset Hierachie in BIC GRC. Der Bearbeiter Kontrolle kann dann mittels des Icons die verantwortliche Einheit auswählen.

   > Im Hintergrund filtert ein Filter auf Assets der Typen "Organisationseinheit".

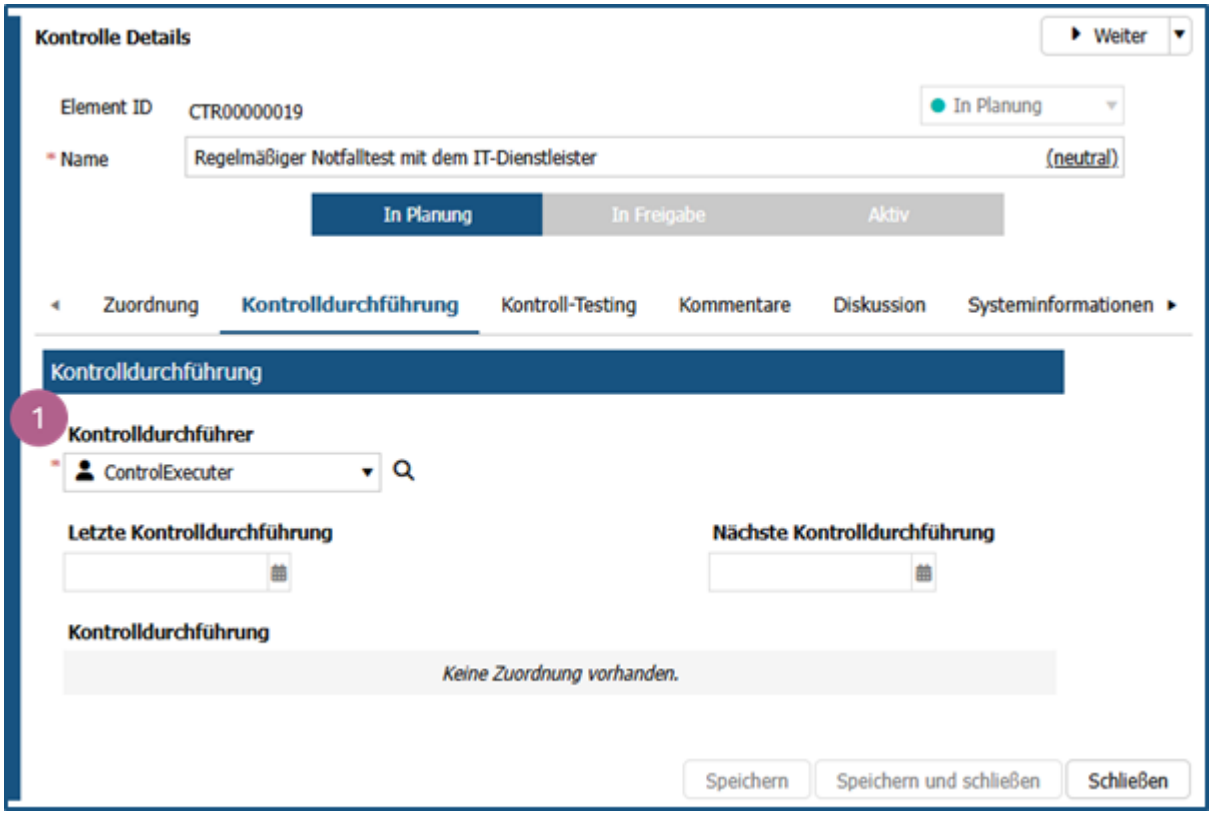
   Ist die Auslagerung nicht innerhalb des Unternehmens wird ein weiterer Link zu einem Lieferantenverzeichnis angezeigt. Auch hier ist mittels des Icons eine entsprechende Verlinkung vorzunehmen.
6. **Referenzen**: Neben den oben genannten können auch folgende Zuordnungen gemacht werden:

- **Dokumentierte Informationen**: Der Bearbeiter Kontrolle kann ein oder mehrere *Dokumentierte Informationen* hinterlegen.

> *Dokumentierte Informationen* unterstützen insbesondere im Informationssicherheitsbereich um Effizienz und Nachvollziehbarkeit zu verbessern, können aber auch in anderen Modulen dazu beitragen Transparenz zu schaffen.

Schritt 4: Kontrolldurchführer & -tester hinterlegen

In den beiden Tabs " Kontrolldurchführung" (Optional) und "Kontroll-Testing" muss der Bearbeiter Kontrolle noch passende Benutzer hinterlegen bevor ein Statuswechsel durchgeführt wird.



1 **Kontrolldurchführer**:

Für die *Kontrolldurchführung* kann im zweiten Tab "*Kontrolldurchführung*" mittels des Icons 🔍 ein verantwortlicher Kontrolldurchführer hinterlegt werden.

> Der Bearbeiter kann nur einen Benutzer als Kontrolldurchführer hinterlegen. Weiters kann der Bearbeiter kein weiteres Attributsfeld in diesem Tab bearbeiten.

Das Verhalten der Attribute in diesem Tab erfolgt wie folgt:

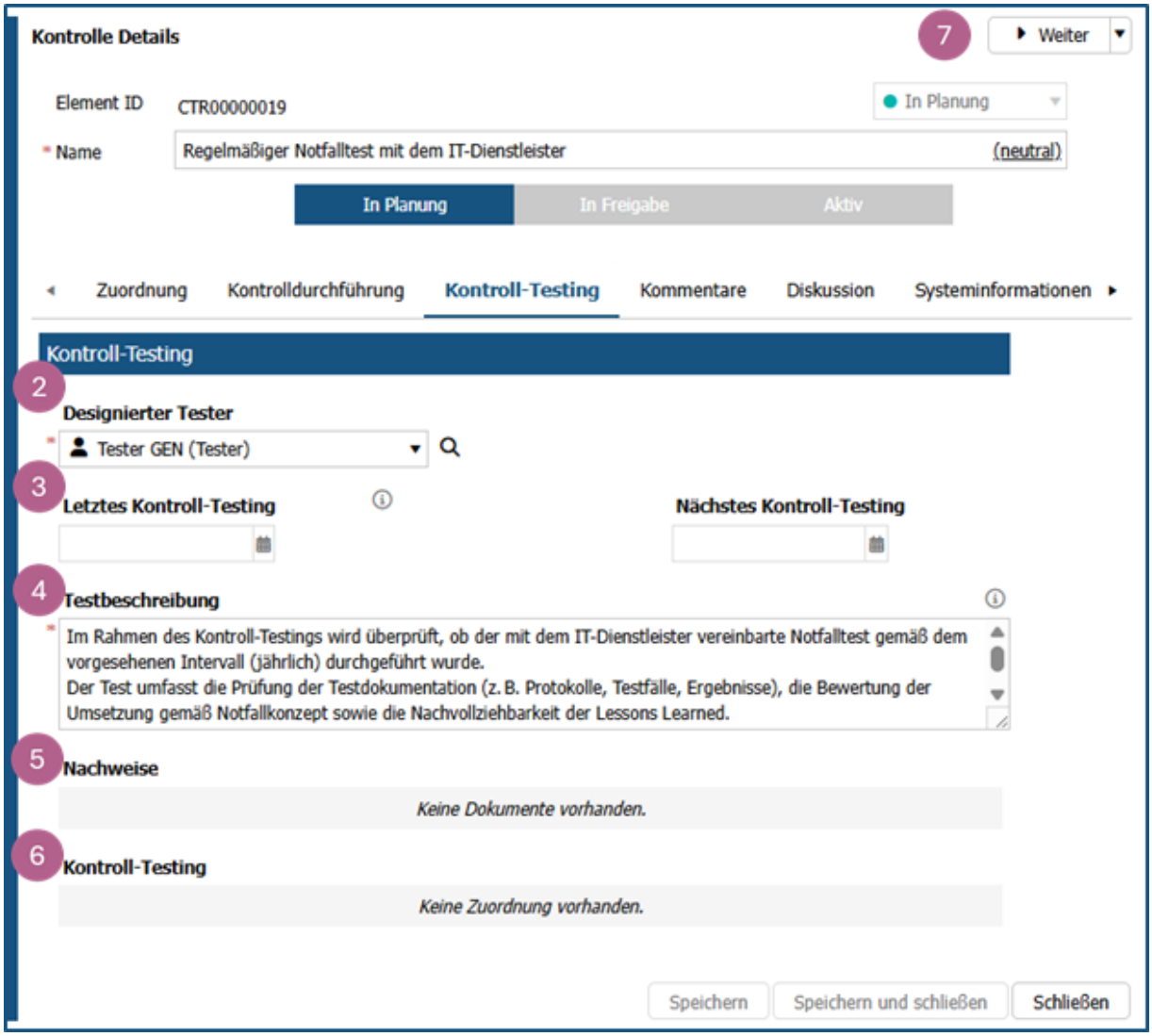
- **Letzte Kontrolldurchführung**: Setzt sich automatisch nach dem Statusübergang der *Kontrolldurchführung* von "Durchführung" zu "Abgeschlossen".

  > Das Attribut ist Read Only und kann nicht manuell verändert werden.

- **Nächste Kontrolldurchführung**: Setzt sich automatisch nachdem es erstmalig ein Datum in "Letzte Kontrolldurchführung"gibt. Das "Nächste Kontrolldurchführungs"- Datum ist anschließend eine Addition aus dem "Letzte Kontrolldurchführungs"- Datum und der Kontroll- Frequenz aus dem Tab "*Zuordnung*".

  > Das Attribut ist Read Only und kann nicht manuell verändert werden.

- **Kontrolldurchführung**: Die Erstellung einer Kontrolldurchführung kann nur von einem Benutzer mit dem passenden Benutzerprofil erstellt werden. Mehr Informationen unter Kontrolldurchführer - Kontrolldurchführung erstellen & durchführen.



2. **Designierter Tester**: Für die Hinterlegung eines Testers muss der Bearbeiter in den dritten Tab "*Kontroll-Testing*" wechseln. Wie schon im Tab "*Kontrolldurchführung*" muss der Bearbeiter hier mittels des Icons  einen verantwortlichen Tester für die *Kontrolle* hinterlegen.
3. **Daten des Kontroll-Testings**: Wie schon in der Kontrolldurchführung werden in dem Tab "*Kontroll-Testing*" zwei Daten-Attribute angezeigt.
    - **Letztes Kontrolltesting**: Setzt sich automatisch nach dem Statusübergang des *Kontroll-Testings* von "Durchführung" zu "Überprüfung".

      > Das Attribut ist Read Only und kann nicht manuell verändert werden.

    - **Nächstes Kontroll-Testing**: Setzt sich automatisch nachdem es erstmalig ein Datum in "Letztes Kontroll-Testing" gibt. Das "Nächste Kontroll-Testings"-Datum ist anschließend eine Addition aus dem "Letztes Kontroll-Testing"-Datum und der Kontroll-Testing-Frequenz aus dem Tab "*Zuordnung*".

      > Das Attribut ist Read Only und kann nicht manuell verändert werden.

4. **Testbeschreibung**: In der Testbeschreibung muss der Bearbeiter angeben, wie die *Kontrolle* validiert werden kann.

   > So kann an dieser Stelle angegeben werden, mit welcher Aktivität der Tester das *Kontroll-Testing* durchführen kann oder ein Vorschlag wie groß die Stichprobe zu wählen ist.

5. **Nachweis**: Neben der Beschreibung kann auch ein Dokument oder Memo an die *Kontrolle* angehängt werden.

   > Handelt es sich um eine Datei kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend im Attributsfeld verlinkt.

   > Beispielsweise ein Template einer Checkliste für die Prüfung der *Kontrolle*.

6. **Kontroll-Testing**: Die Erstellung eines *Kontroll-Testings* kann nur von einem Bearbeiter Kontrolle erstellt werden. Mehr Informationen unter Bearbeiter Kontrolle - Kontroll-Testing einleiten & erstellen.
7. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Freigabe" durchgeführt.

   > Nach dem Speichervorgang wird der eingetragene Freigeber Kontrolle mittels Notifikation benachrichtigt.

2.9.3 Kontroll-Testings einleiten & erstellen

In der Dokumentationsphase einer *Kontrolle*, kann der Bearbeiter Kontrolle einen passenden Tester im dritten Tab "*Kontroll-Testing*" nominieren. Sobald die *Kontrolle* freigegeben und im Status "Aktiv" ist, kann ein *Kontroll-Testing* gestartet werden.

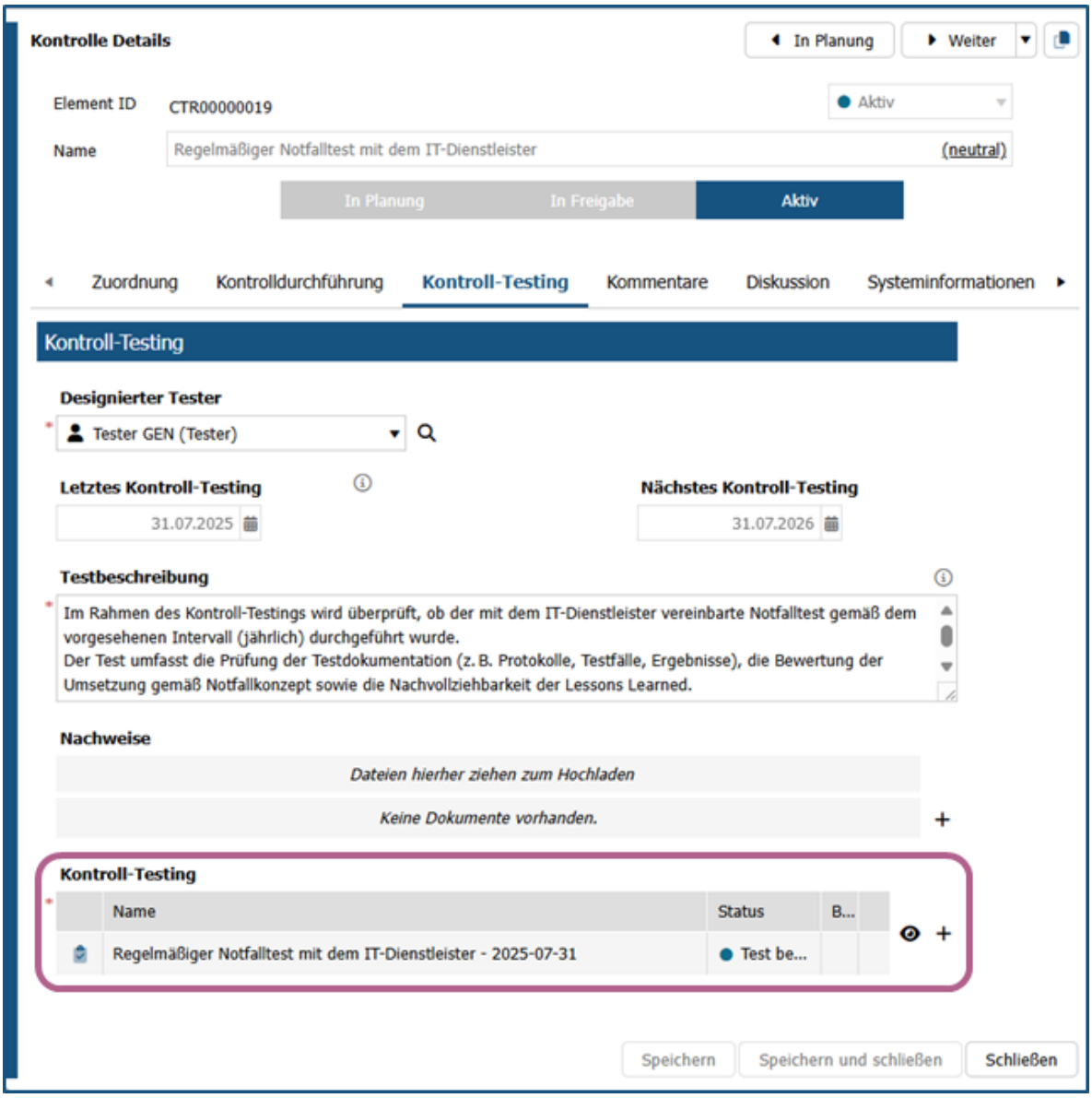
> Der Bearbeiter der Kontrolle kann dabei die Erstellung des Kontroll-Testings nur manuell durchführen. Um dies in regelmäßigen Abständen zu machen unterstützt ein Scheduler der den Bearbeiter Kontrolle einen Tag bevor das "Nächstes Kontroll-Testing" erreicht ist, erinnert.

Schritt 1: Navigation zu Kontrolle

Der Bearbeiter Kontrolle bekommt automatisch eine E-Mail zugesendet, sobald das Datum zu "Nächstes Kontroll-Testing" erreicht wurde. Der Link zu der spezifischen *Kontrolle* befindet sich in der Notifikation.

Schritt 2: Kontroll-Testing erstellen

Das *Kontroll-Testing* entsteht aus der *Kontrolle* heraus, indem der Bearbeiter Kontrolle mittels des Icons + ein neues *Kontroll-Testing* erstellt.



> Es ist nicht vorgesehen, dass ein *Kontroll-Testing* verlinkt wird, da *Kontroll-Testings* unique zu einer *Kontrolle* durchgeführt werden.

Schritt 3: Details hinterlegen

1. **Name**: Als erster Schritt erfolgt die Hinterlegung des "Namens" automatisch von der *Kontrolle* auf das *Kontroll-Testing*. Somit muss der Bearbeiter keine Auswahl eines "Namens" treffen.

   > Bei Statusübergang wird der "Name" um das Datum von "Zeitpunkt der Testdurchführung" ergänzt.

2. **GRC- Perspektive**: Die Perspektive wird automatisch aus der *Kontrolle* übernommen und gesetzt. Sie kann nach dem ersten Speichervorgang nicht mehr verändert werden.

3. **Verantwortlichkeiten**: Des Weiteren werden bei der Erstellung des *Kontroll- Testings* automatisch die Verantwortlichen, die in der *Kontrolle* definiert wurden, übertragen.
4. **Testing für:**: Des Weiteren wird automatisch das Asset der *Kontrolle* übernommen.

Nach dem Speichervorgang wird der eingetragene Tester mittels Notifikation benachrichtigt.

Im Anschluss kann das Fenster geschlossen werden.

2.9.4 Finding verwalten & behandeln

Ein Bearbeiter bekommt eine Notifikation zugesendet, wenn er als Bearbeiter in einem *Finding* eingetragen wurde. Seine Aufgabe ist es im *Finding* passende Maßnahmen zu definieren, um das *Finding* angemessen zu behandeln.

Schritt 1: Navigation zu spezifischem Finding nach Fremderstellung

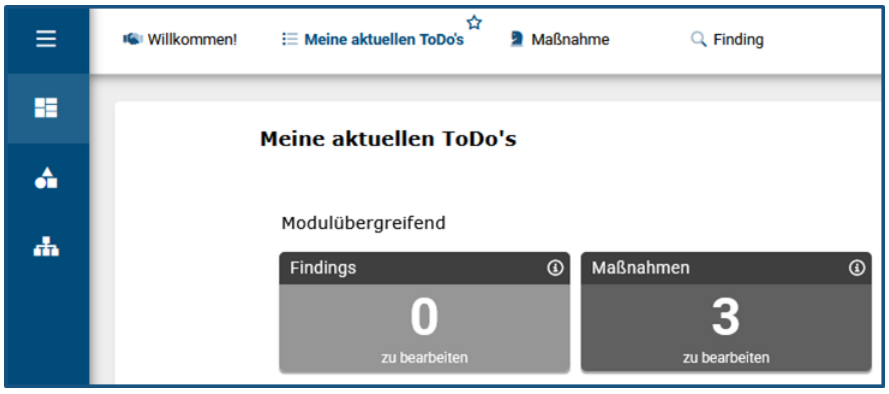
Der Bearbeiter hat zwei Möglichkeiten ein zu bearbeitendes *Finding* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "Erfassung" abgeschlossen hat. Der Link zu dem spezifischen *Finding* befindet sich in der Notifikation.

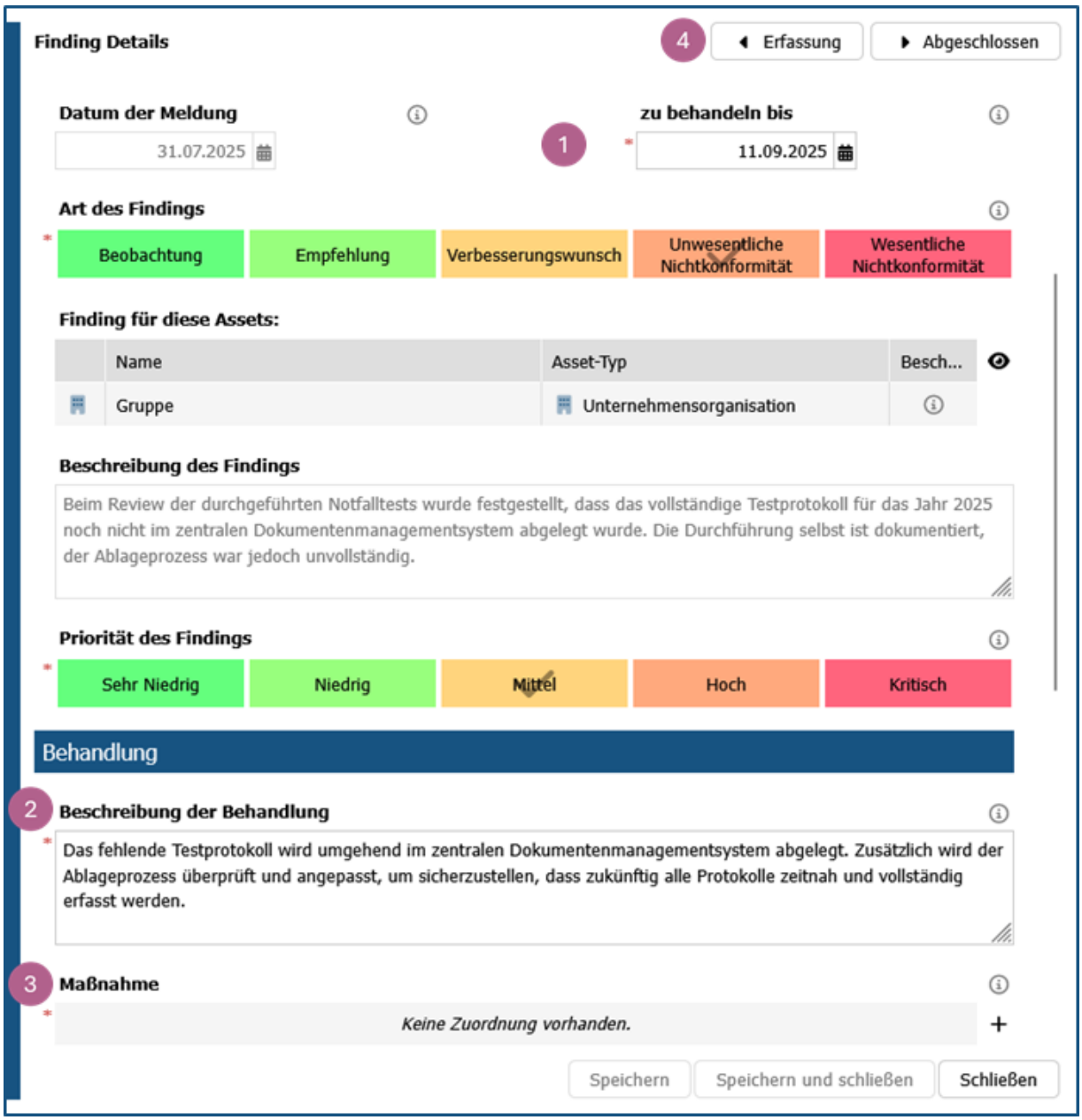
2. Öffnen über Dashboard "Meine aktuellen To's"

Der Bearbeiter kann in dem Dashboard seine aktuellen *Findings* sehen.



Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Finding* automatisch.

Schritt 2: Finding behandeln



1. **Angaben überprüfen**: Als erstes kann der Bearbeiter bei Bedarf die Einschätzungen des Erstellers überarbeiten. So kann er das "zu behandeln bis"-Datum so setzen, dass es für ihn realistisch ist. Zudem kann er die "Art des Findings" und die "Priorität des Findings" neu einschätzen.
2. **Beschreibung der Behandlung**: Danach sollte der Bearbeiter beschreiben wie er das *Finding* behandeln möchte. Dies passiert im ersten Schritt schriftlich, bevor konkrete *Maßnahmen* dazu erstellt werden.
3. **Maßnahme**: Das *Finding* wird durch eine *Maßnahme* behandelt. Mehr Informationen über die Erstellung einer Maßnahme unter Bearbeiter Maßnahme - Maßnahme definieren & erstellen Schritt 2.

> Es ist im *Finding* nur möglich neue *Maßnahmen* zu erstellen und keine bestehenden *Maßnahmen* zu verlinken.

4 **Statuswechsel**: Der Bearbeiter kann abschließend in den Status "Abgeschlossen" weiterschalten.

> Der Ersteller wird über den Statusübergang mittels Notifikation benachrichtigt.

2.9.5 Kontroll-Testing überprüfen & freigeben

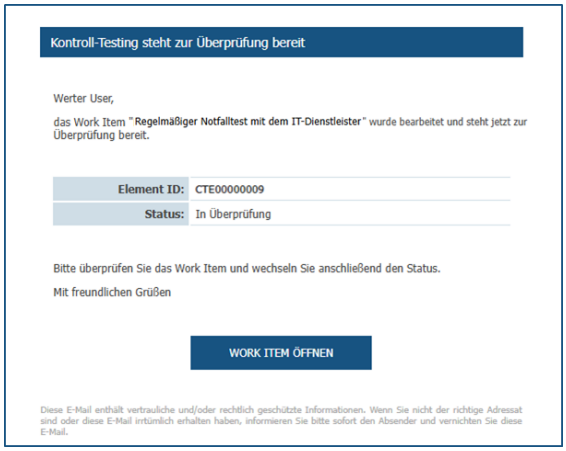
Ein *Kontroll-Testing* wird vom Bearbeiter Kontrolle erstellt und vom Tester dokumentiert. Sobald die Eingaben der Prüfungsergebnisse abgeschlossen sind, kann das *Kontroll-Testing* dem Bearbeiter Kontrolle weitergegeben werden mittels Statusübergang in "Überprüfung".

Schritt 1: Navigation zu Kontroll-Testing

Der Bearbeiter Kontrolle hat zwei Möglichkeiten eine freizugebende *Kontrolle* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter Kontrolle bekommt eine E-Mail zugesendet, sobald der Tester alle Eingaben im Status "Durchführung" abgeschlossen hat. Der Link zu dem spezifischen *Kontroll-Testing* befindet sich in der Notifikation.



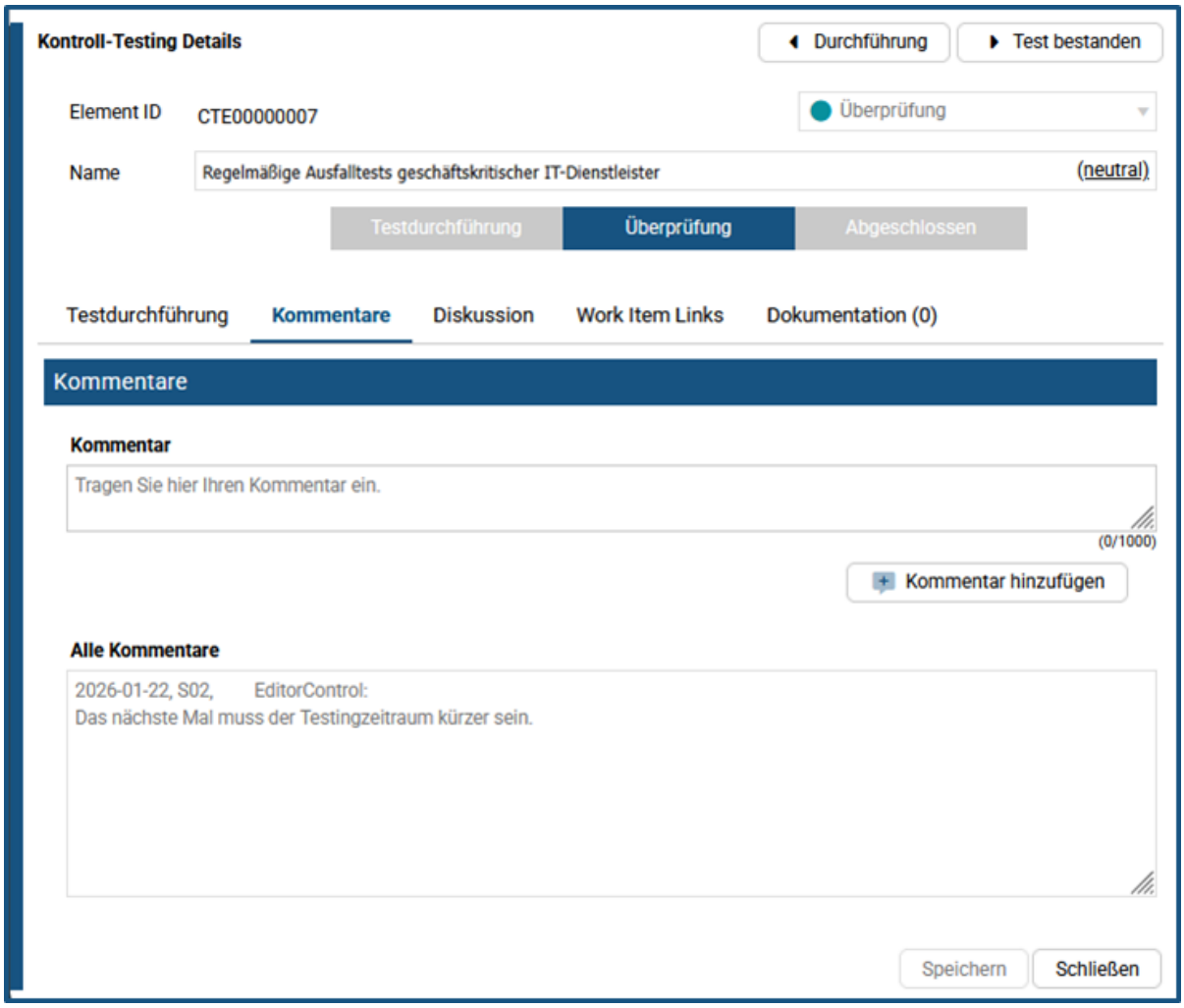
2. Öffnen über Dashboard "Meine aktuelle ToDo`s"

Im oberen Teil des Dashboards "Meine aktuelle ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter Kontrolle noch eine Überprüfung durchzuführen hat.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontroll-Testing* automatisch.

Schritt 2: Überprüfung durchführen

Der Bearbeiter Kontrolle hat in dem *Kontroll- Testing* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob das *Kontroll- Testing* erfolgreich durchgeführt werden konnte oder nicht. Dabei stehen zwei Statusübergänge zur Verfügung: "Test bestanden" und "Test nicht bestanden".



Wurde entweder die "Angemessenheitsprüfung" oder die "Wirksamkeitsprüfung" nicht bestanden kann der Bearbeiter Kontrolle nur in den Status "Test nicht bestanden" wechseln. Alternativ kann der Bearbeiter Kontrolle ein Kommentar im Tab "*Kommentar*" hinterlassen und einen Statusübergang zu "Durchführung" durchführen. Der Tester wird mittels Notifikation benachrichtigt.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzers passen und ist das Testergebnis positiv kann der Bearbeiter Kontrolle weiter in den Status "Test bestanden" schalten.

> Nach dem Speichervorgang wird der Tester mittels Notifikation benachrichtigt.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.10 Freigeber Kontrolle

Der Freigeber Kontrolle ist in BIC GRC für mindestens eine *Kontrolle*, die seinem Asset zugeordnet ist, für die Freigabe verantwortlich.

- Kontrolle überprüfen & freigeben

Der Freiegeber Kontrolle kann darüber hinaus noch *Kontrollen* erstellen in BIC GRC. Da dies aber nicht seine Hauptaufgabe ist, wird an dieser Stelle nur auf das Benutzerprofile "Bearbeiter Kontrolle" verwiesen:

- Kontrolle ableiten & erstellen

2.10.1 Kontrolle überprüfen & freigeben

Ein *Kontrolle* wird vom Bearbeiter Kontrolle erstellt und dokumentiert. Sobald die Eingaben aller Informationen abgeschlossen und überprüft wurde, kann eine *Kontrolle* dem Freigeber Kontrolle weitergegeben werden mittels Statusübergang in "Freigabe".

Schritt 1: Navigation zu Kontrolle

Der Freigeber Kontrolle hat zwei Möglichkeiten eine freizugebende *Kontrolle* zu öffnen.

1. Öffnen über Notifikation

Der Freigeber Kontrolle bekommt eine E- Mail zugesendet, sobald der Bearbeiter Kontrolle alle Eingaben im Status "Planung" abgeschlossen hat. Der Link zu der spezifischen *Kontrolle* befindet sich in der Notifikation.

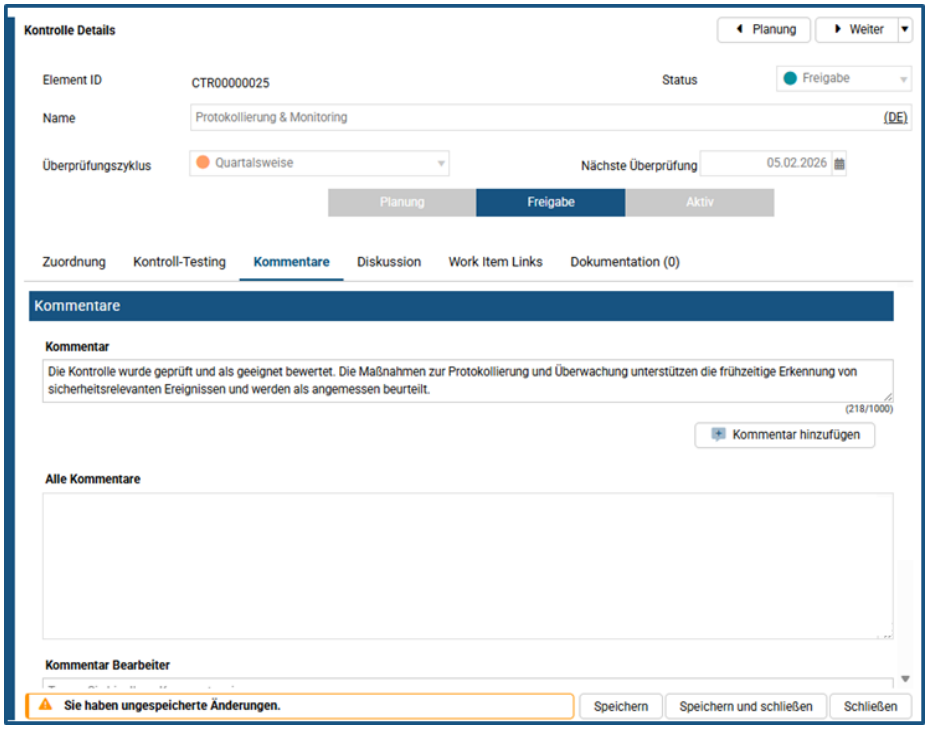
2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber Kontrolle noch eine Freigabe durchzuführen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontrolle* automatisch.

Schritt 2: Überprüfung durchführen

Der Freigeber Kontrolle hat in der *Kontrolle* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Kontrolle* in ihrer Beschaffenheit dazu geeignet ist den Prozess zu verbessern. Sollte dies nicht der Fall sein und muss die *Kontrolle* aus Sicht des Freigebers Kontrolle überarbeitet werden, kann der Freigeber Kontrolle einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "Planung" durchführen.



Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzers passen, kann der Freigeber Kontrolle weiter in den Status "Aktiv" schalten

> Nach dem Speichervorgang wird der Bearbeiter Kontrolle mittels Notifikation benachrichtigt.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.11 Kontrolldurchführer

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.

2.11.1 Kontrolldurchführung erstellen & durchführen

In der Dokumentationsphase einer *Kontrolle*, kann der Bearbeiter Kontrolle einen passenden Kontrolldurchführer im zweiten Tab "*Kontrolldurchführung*" nominieren. Sobald die *Kontrolle* freigegeben und im Status "Aktiv" ist, kann eine *Kontrolldurchführung* gestartet werden.

Schritt 1: Navigation zu Kontrolle

Der Kontrolldurchführer hat zwei Möglichkeiten, eine *Kontrolle* zu öffnen.

1. Öffnen über Notifikation

Der Kontrolldurchführer bekommt eine E-Mail zugesendet, sobald der Freigeber Kontrolle einen Statusübergang zu "Aktiv" durchgeführt hat bzw. wird eine automatische Notifikation durch einen Scheduler versendet. Der Link zu der spezifischen *Kontrolle* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

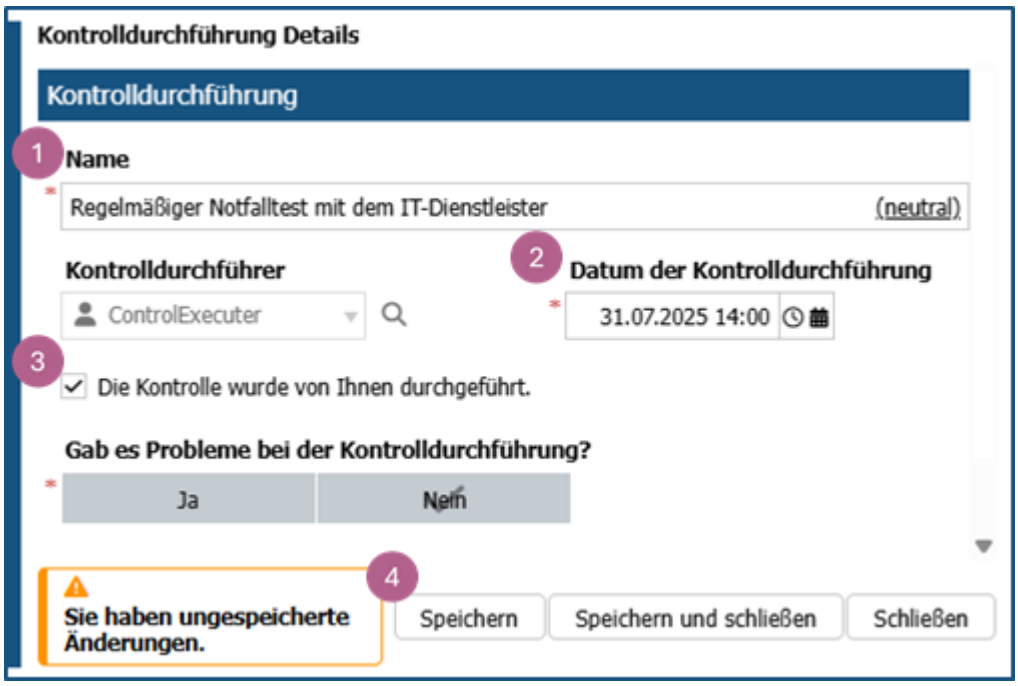
Im Dashboard "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Kontrolldurchführer noch eine Durchführung durchzuführen hat (öffnen über *Kontrolle*) oder weitermachen kann.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontrolle* automatisch. Der Kontrolldurchführer steigt direkt in den Tab *"Kontrolldurchführung"* der *Kontrolle* ein.

Schritt 2: Durchsicht der Eingaben des Bearbeiters Kontrolle

Es empfiehlt sich, als ersten Schritt im Work Item *Kontrolle* zu dem Tab *"Zuordnung"* zu wechseln, um die Detaileingaben des Bearbeiters Kontrolle einzusehen und festzustellen, was die Vorgaben für die Durchführung der Kontrolle sind.

Schritt 3: Kontrolldurchführung erstellen



1 **Name und Verantwortlicher**: Als erster Schritt wird der "Name" und das Benutzerfeld "Kontrolldurchführer" von BIC GRC automatisch befüllt, sodass der Kontrolldurchführer nicht bei jeder neu erstellten *Kontrolldurchführung* einen neuen Namen und sich selber eingeben muss.

2 **Datum der Kontrolldurchführung**: Das Datum muss der Kontrolldurchführer individuell eingeben. Dabei kann er nicht nur das Datum hinterlegen, sondern bei Bedarf auch eine genaue Uhrzeit.

> Dieses Datum wird für das Attributsfeld "Letzte Kontrolldurchführung" in der *Kontrolle* herangezogen.

> Das Datum der *Kontrolldurchführung* muss dem aktuellen Tag oder in der Vergangenheit liegen, dass die *Kontrolldurchführung* später in den Status "Abgeschlossen" gewechselt werden kann. Siehe auch Punkt 6 unten.

3 **Angabe der Durchführung**: Der Kontrolldurchführer hat mit dieser Checkbox explizit zu bestätigen, dass er die Kontrolle durchgeführt hat.

4 Nach dem ersten Speichervorgang werden weitere Attributsfelder eingeblendet

Details der Kontrolldurchführung: Falls es Besonderheiten bei *Kontrolldurchführung* gegeben haben sollte, oder andere Details relevant sind, können diese an dieser Stelle beschrieben werden.

5 **Geprüfte Dokumente**: Weiters kann der Kontrolldurchführer Dokumente anhängen die entweder geprüft worden sind oder bei der Durchführung der Kontrolle unterstützt haben.

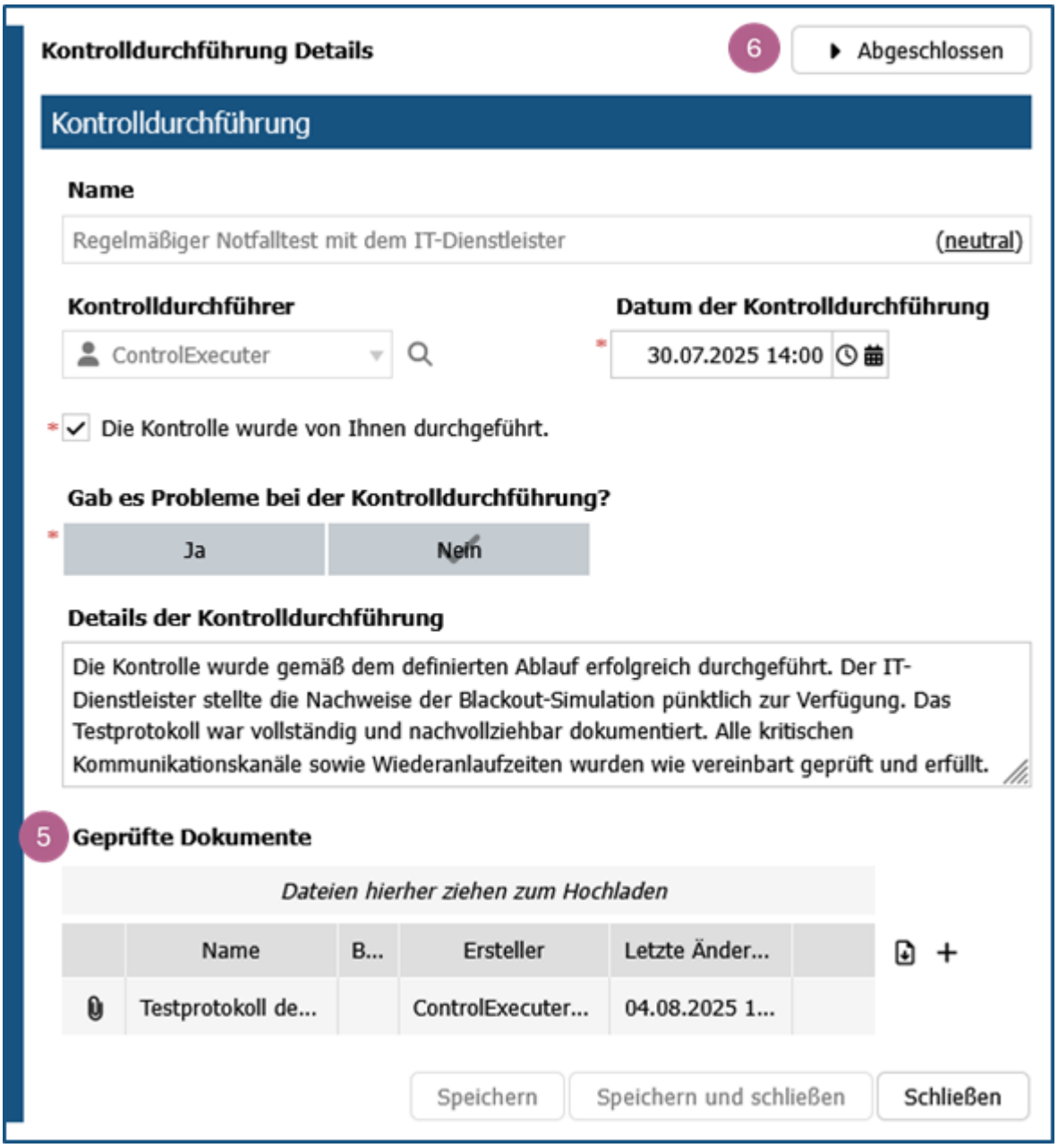
> Handelt es sich um eine Datei kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend automatisch im Attributsfeld verlinkt.

> So kann zum Beispiel auch eine unterschriebene Checkliste über alle durchführten Schritte hinterlegt werden.

6 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Abgeschlossen" durchgeführt.

> Sollte es bei der *Kontrolldurchführung* zu Herausforderungen gekommen sein, wird der Bearbeiter Kontrolle darüber mittels Notifikation benachrichtigt.

> Es ist nicht vorgsehen, dass es eine Überprüfung der *Kontrolldurchführung* in BIC GRC gibt. Jedoch wird der Bearbeiter Kontrolle mittels Notifikation darüber informiert, wenn eine *Kontrolldurchführung* abgeschlossen wurde.



2.12 Bearbeiter "Domänenspezifisch"

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

> Das Benutzerprofil setzt dadurch voraus, dass alle zugeteilten Bearbeiter Domänenspezifisch ein spezifisches Set an Wissen für eine Domäne mitbringen, um die Aufgaben gerecht erfüllen zu können.

> Der Bearbeiter "Domänenspezifisch" wird in den nächsten Kapiteln mit Bearbeiter DS abgekürzt werden.

Folgende Aufgaben hat ein Bearbeiter DS in BIC GRC:

- Finanzielle Wesentlichkeit definieren & bewerten
- Auswirkungs-Wesentllichkeit definieren & bewerten
- Management Review definieren & erstellen
- Management Review durchführen & überprüfen
  - Finding identifizieren & erstellen

Der Bearbeiter DS kann darüber hinaus noch weitere Work Items erstellen in BIC GRC. Da dies aber nicht seine Hauptaufgabe ist, wird an dieser Stelle nur auf andere Benutzerprofile verwiesen:

- Ziel definieren & erstellen
  - Zwischenziel definieren & erstellen
- Kontrolle ableiten & erstellen
- Maßnahme definieren & erstellen

2.12.1 Finanzielle Wesentlichkeit definieren & bewerten

Eine *Finanzielle Wesentlichkeit* wird von einem Assessor identifiziert und erstellt bevor sie optional einem Bearbeiter DS übergeben wird.

> Der Assessor muss keinen Bearbeiter eintragen, wenn er die Bewertung selber durchführen kann. Wenn dies der Fall ist kann der Assessor die folgende Beschreibung für den Bearbeiter DS ab dem Schritt 3 übernehmen.

Schritt 1: Navigation zu Finanzielle Wesentlichkeit

Der Bearbeiter DS hat zwei Möglichkeiten eine zu bewertende *Finanzielle Wesentlichkeit* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter DS bekommt eine E-Mail zugesendet, sobald der Assessor alle Eingaben im Status "Entwurf" abgeschlossen und einen Statusübergang zu "In Bewertung" durchgeführt hat. Der Link zu der spezifischen *Finanzielle Wesentlichkeit* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Doppelte Wesentlichkeit"

Der Bearbeiter DS navigiert zu dem Dashboard "Doppelte Wesentlichkeit" und sieht alle Auswirkungen, die in seinen Tätigkeitsbereich fallen.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Finanzielle Wesentlichkeit*automatisch.

Schritt 2: Überprüfung der Eingaben des Erstellers

Es wurde sich empfehlen, als ersten Schritt im Work Item *Finanzielle Wesentlichkeit* zu dem Tab *"Details"* zu wechseln, um die Detaileingaben des Erstellers einzusehen.

Sollten die Eingaben des Ersteller nicht richtig oder unvollständig sein, kann der Bearbeiter Risiko einen Kommentar im Tab *"Diskussion"* hinterlassen.

Sind die Eingaben des Erstellers richtig und vollständig, kann der Bearbeiter DS in den Tab *"Bewertung"* zurückkehren und mit der Bewertung der *Finanziellen Wesentlichkeit* beginnen.

Schritt 3: Finanziellen Wesentlichkeit bewerten

1. **Risiko oder Chance?**: Der Bearbeiter muss angeben, ob dies Auswirkung auf das Unternehmen ein Risiko birgt oder eine Chance sein könnte.

   Anders als in anderen Bereichen des Risikomanagements ist es im Nachhaltigkeitsbereich dezitiert gewünscht, dass auch positive Effekte aufgenommen werden.

2. **Was wird beeinflusst**: Aus diesem Blickwinkel wird betrachtet, auf was die Umwelt im finanziellen Bereich des eigenen Unternehmens wirken wird.

   So kann eine CO2-Besteuerung möglicherweise auf die Performance Einfluss haben.

3. **Stärke der Beeinflussung**: Weiters muss mittels einer 5-stufigen Skala eingeschätzt werden, wie stark die Auswirkung auf das Unternehmen wäre.
4. **Abhängigkeiten**: Des weiteren macht es Sinn anzugeben, auf welche Ressourcen bzw. Beziehungen sich die Auswirkung beziehen wird.
5. **Wahrscheinlichkeit**: Der Bearbeiter kann mittels einer 5-stufigen Einschätzung angeben, wie wahrscheinlich der Eintritt ist, mit dem das Unternehmen beeinflusst wird.
6. **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen kann die *Finanziellen Wesentlichkeit* gespeichert werden.

Schritt 4: Ergebnis auswerten

1. **Ergebnis**: Mittels einer einfache Berechnung wird im Hintergrund ein Mittelwert der Stärke der Beeinflussung und der Wahrscheinlichkeit berechnet und als Ergebnis ausgegeben. Das Ergebnis ist dabei nicht bearbeitbar.

2. **Expertenschätzung**: Falls dieses automatisch berechnete Ergebnis nicht der Realität entspricht kann es mittels der Checkbox "Übersteuerung durch Expertenschätzung" übersteuert werden. Wenn die Checkbox angeklickt wurde kann der Bearbeiter DS eine Übersteuerung vornehmen. Wenn er dies macht muss er aber auch verpflichtend eine Begründung für diesen Vorgang angeben.
3. **Nachhaltigkeitsrisiko oder -chance**: Sollte das Ergebnis - durch die Berechnung oder die Übersteuerung - als "Wesentlich" eingestuft werden muss verpflichtend ein bzw. - chance erstellt werden.
4. **Optional - Schritt 5: Nachhaltigkeitsstrategie**
5. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Überprüfung" durchgeführt.

Schritt 5: Nachhaltigkeitsstrategie hinterlegen

Der Bearbeiter kann im Tab "*Nachhaltigkeitsstrategie*" zusätzliche Links hinterlegen.

1. **Strategie**: Der Link "Strategie" führt zu dem Work Item *Dokumentierte Informationen*. Es können dabei keine neuen *Dokumentierte Informationen* erstellt, sondern nur verlinkt werden.

> Da nur Benutzer mit dem spezifischen Profil Dokumenteneigner *Dokumentierte Informationen* erstellen dürfen, kann der Bearbeiter bei der Notwendigkeit einer noch nicht vorhandenen "Strategie" eine Diskussion im "*Diskussions*"-Tab beginnen.

2. **Maßnahme**: Neben der "Strategie" sollten auch *Maßnahmen* gesetzt und hinterlegt werden. Sie sollen dazu beitragen die aktuelle *Finanziellen Wesentlichkeit* zu reduzieren oder zu optimieren.
3. **Ziele**: Zuletzt kann es Sinn machen nicht nur Maßnahmen zu definieren, sondern sich auch Ziele zu setzen, wie mit der *Finanziellen Wesentlichkeit* in Zukunft umgegangen werden soll.

2.12.2 Auswirkungs-Wesentlichkeit definieren & bewerten

Eine *Auswirkungs- Wesentlichkeit* wird von einem Assessor identifiziert und erstellt bevor sie optional einem Bearbeiter DS übergeben wird.

> **Der Assessor muss keinen Bearbeiter eintragen, wenn er die Bewertung selber durchführen kann. Wenn dies der Fall ist kann der Assessor die folgende Beschreibung für den Bearbeiter DS ab dem Schritt 3 übernehmen.**

Schritt 1: Navigation zu Auswirkungs-Wesentlichkeit

Der Bearbeiter DS hat zwei Möglichkeiten eine zu bewertende *Auswirkungs- Wesentlichkeit* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter DS bekommt eine E-Mail zugesendet, sobald der Assessor alle Eingaben im Status "Entwurf" abgeschlossen und einen Statusübergang zu "In Bewertung" durchgeführt hat. Der Link zu der spezifischen *Auswirkungs-Wesentlichkeit* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Doppelte Wesentlichkeit"

Der Bearbeiter DS navigiert zu dem Dashboard "Doppelte Wesentlichkeit" und sieht alle Auswirkungen, die in seinen Tätigkeitsbereich fallen.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Auswirkungs-Wesentlichkeit* automatisch.

Schritt 2: Überprüfung der Eingaben des Erstellers

Es wurde sich empfehlen, als ersten Schritt im Work Item *Auswirkungs-Wesentlichkeit* zu dem Tab *"Details"* zu wechseln, um die Detaileingaben des Erstellers einzusehen.

Sollten die Eingaben des Ersteller nicht richtig oder unvollständig sein, kann der Bearbeiter Risiko einen Kommentar im Tab *"Diskussion"* hinterlassen.

Sind die Eingaben des Erstellers richtig und vollständig, kann der Bearbeiter DS in den Tab *"Bewertung"* zurückkehren und mit der Bewertung der *Auswirkungs-Wesentlichkeit* beginnen.

Schritt 3: Finanziellen Wesentlichkeit bewerten

1. **Auswirkungsart**: Der Bearbeiter muss angeben, ob dies Auswirkung auf die Umwelt negativ oder positiv ist.

   > Anders als in anderen Bereichen des Risikomanagements ist es im Nachhaltigkeitsbereich dezitiert gewünscht, dass auch positive Effekte aufgenommen werden.

2. **Potenziell oder Tatsächlich**: Dabei kann die Auswirkung potenziell sein (also sie kann eintreten) oder tatsächlich (es steht schon fest).
3. **Wahrscheinlichkeit**: Der Bearbeiter kann mittels einer 5-stufigen Einschätzung angeben, wie wahrscheinlich der Eintritt ist, mit dem die Umwelt positiv oder negativ beeinflusst wird.
4. **Schwere der Auswirkung**: Weiters muss mittels einer 5-stufigen Skala eingeschätzt werden, wie gravierend die Auswirkung wäre für die Umwelt.
5. **Verbreitung der Auswirkung**: Schlussendlich ist mittels einer 5- stufigen Einschätzung anzugeben, wie verbreitet die Auswirkung sein wird.

> So kann der Effekt von verschmutzten Abwasser abgeleitet vom eigenen Unternehmen in einen nahegelegenen See die Einschätzung "lokal" ergeben, bei einer Ableitung von verschmutzten Abwasser in die Meere kann die Einschätzung schon zwischen "national" und "kontinental" liegen.

6. **Beseitung möglich?**: Sollte es möglich sein die Auswirkungen wieder zu beseitigen, muss zusätzlich angegeben werden mit welcher Umfang/Aufwand dies erreicht werden kann.

Schritt 4: Ergebnis auswerten

1. **Ergebnis**: Mittels einer einfache Berechnung wird im Hintergrund ein Mittelwert der Stärke der Beeinflussung und der Wahrscheinlichkeit berechnet und als Ergebnis ausgegeben. Das Ergebnis ist dabei nicht bearbeitbar.
2. **Expertenschätzung**: Falls dieses automatisch berechnete Ergebnis nicht der Realität entspricht kann es mittels der Checkbox "Übersteuerung durch Expertenschätzung" übersteuert werden. Wenn die Checkbox angeklickt wurde kann der Bearbeiter DS eine Übersteuerung vornehmen. Wenn er dies macht muss er aber auch verpflichtend eine Begründung für diesen Vorgang angeben.
3. **Nachhaltigkeitsrisiko oder -chance**: Sollte das Ergebnis - durch die Berechnung oder die Übersteuerung - als "Wesentlich" eingestuft werden muss verpflichtend ein bzw. - chance erstellt werden.
4. **Optional - Schritt 5: Nachhaltigkeitsstrategie**
5. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "In Überprüfung" durchgeführt.

Schritt 5: Nachhaltigkeitsstrategie hinterlegen

Der Bearbeiter kann im Tab "*Nachhaltigkeitsstrategie*" zusätzliche Links hinterlegen.

1. **Strategie**: Der Link "Strategie" führt zu dem Work Item *Dokumentierte Informationen*. Es können dabei keine neuen *Dokumentierte Informationen* erstellt, sondern nur verlinkt werden.

> Da nur Benutzer mit dem spezifischen Profil Dokumenteneigner *Dokumentierte Informationen* erstellen dürfen, kann der Bearbeiter bei der Notwendigkeit einer noch nicht vorhandenen "Strategie" eine Diskussion im "*Diskussions*"-Tab beginnen.

2. **Maßnahme**: Neben der "Strategie" sollten auch *Maßnahmen* gesetzt und hinterlegt werden. Sie sollen dazu beitragen die aktuelle *Auswirkungs-Wesentlichkeit* zu reduzieren oder zu optimieren.
3. **Ziele**: Zuletzt kann es Sinn machen nicht nur Maßnahmen zu definieren, sondern sich auch Ziele zu setzen, wie mit der *Auswirkungs-Wesentlichkeit* in Zukunft umgegangen werden soll.

2.12.3 Management Review definieren & erstellen

In BIC GRC ist es möglich *Management Review* zu definieren und in unterschiedlichen Kontexten zu betrachten. Hierzu kann der Bearbeiter Risiko das Work Item *Management Review* erstellen.

> Ein *Management Review* sollte für die Erfüllung der meisten Normen mindestens einmal pro Jahr durchgeführt werden. Die zusätzliche Erstellung aufgrund von besonderen Anlässen wird empfohlen.

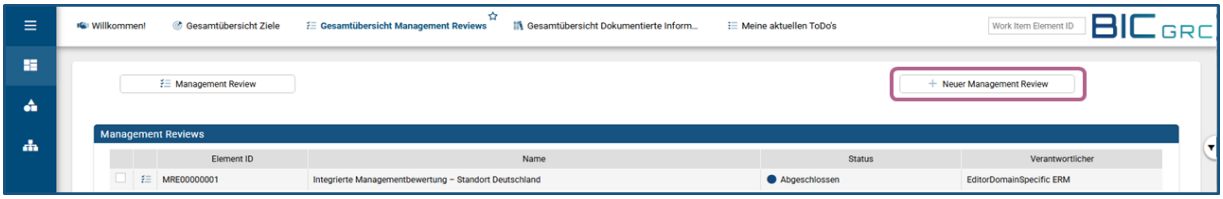
Schritt 1: Management Review erstellen

Der Bearbeiter DS kann in BIC GRC an mehreren Stellen *Management Reviews* erstellen.

1. Erstellen über Dashboard "Gesamtübersicht Management Review"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Gesamtübersicht Management Review >> "Neues Management Review"**

Die Erstellung eines neuen *Management Reviews* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

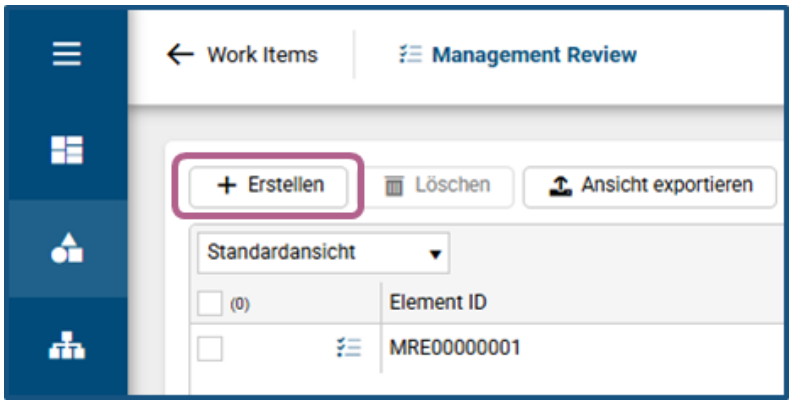


Ein neues Fenster öffnet sich anschließend automatisch.

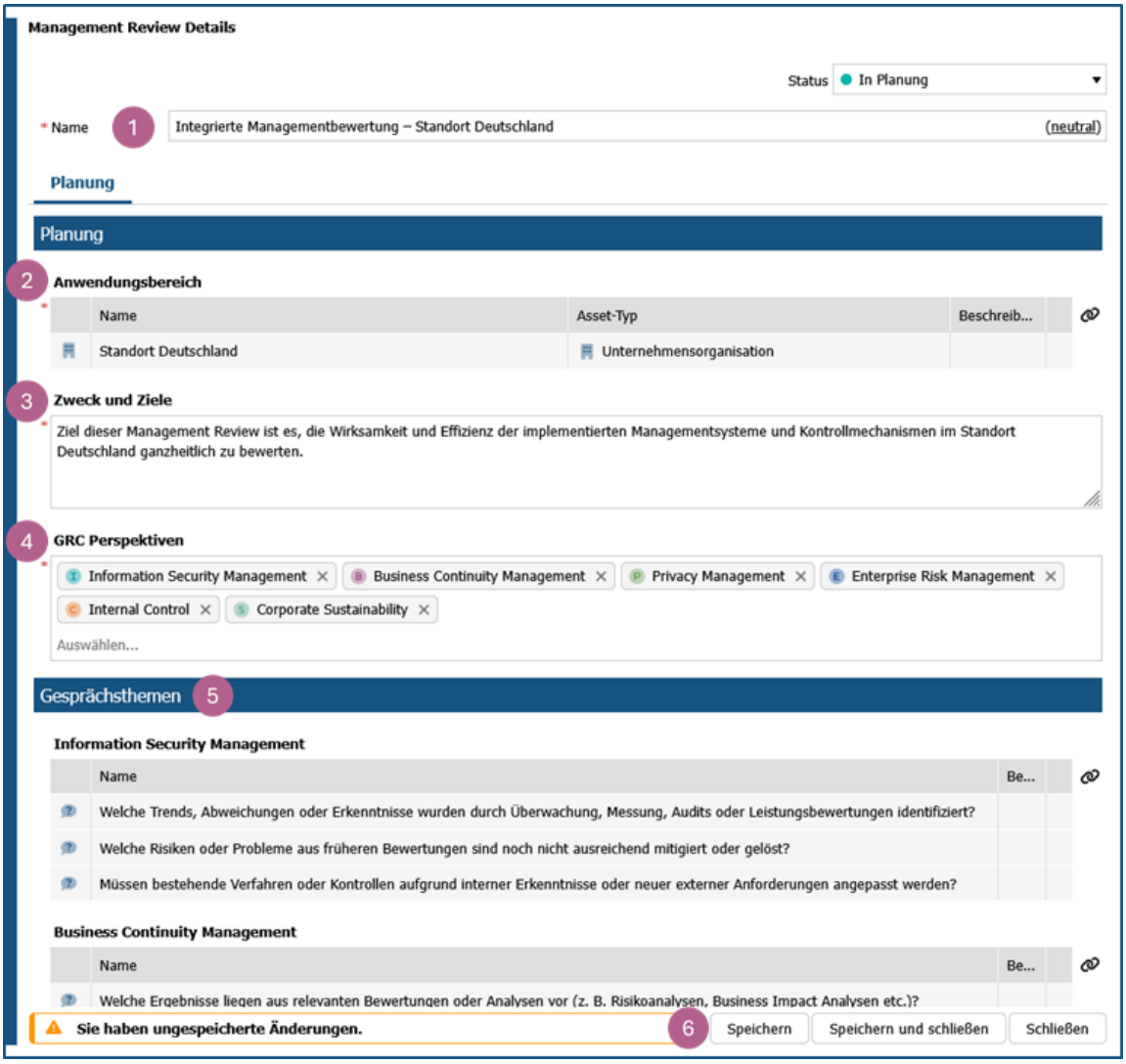
2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Management Review >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details definieren



1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Management Review* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht der *Management Review* einzigartig.
2. **Anwendungsbereich**: Der *Management Review* muss einem Anwendungsbereich zugewiesen werden.

> Dabei darf dem Anwendungsbereich nur eine Organisationseinheit mit dem Tag "Unternehmen" zugewiesen werden.

3. **Zweck und Ziel**: Der *Management Review* sollte so ausführlich wie möglich dokumentiert und beschrieben werden, sodass auch andere Perspektiven einen Kontext bzw. Zusammenhang erkennen können.
4. **GRC Perspektive**: Der Bearbeiter kann ein oder mehrere GRC Perspektiven auswählen.

> Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.

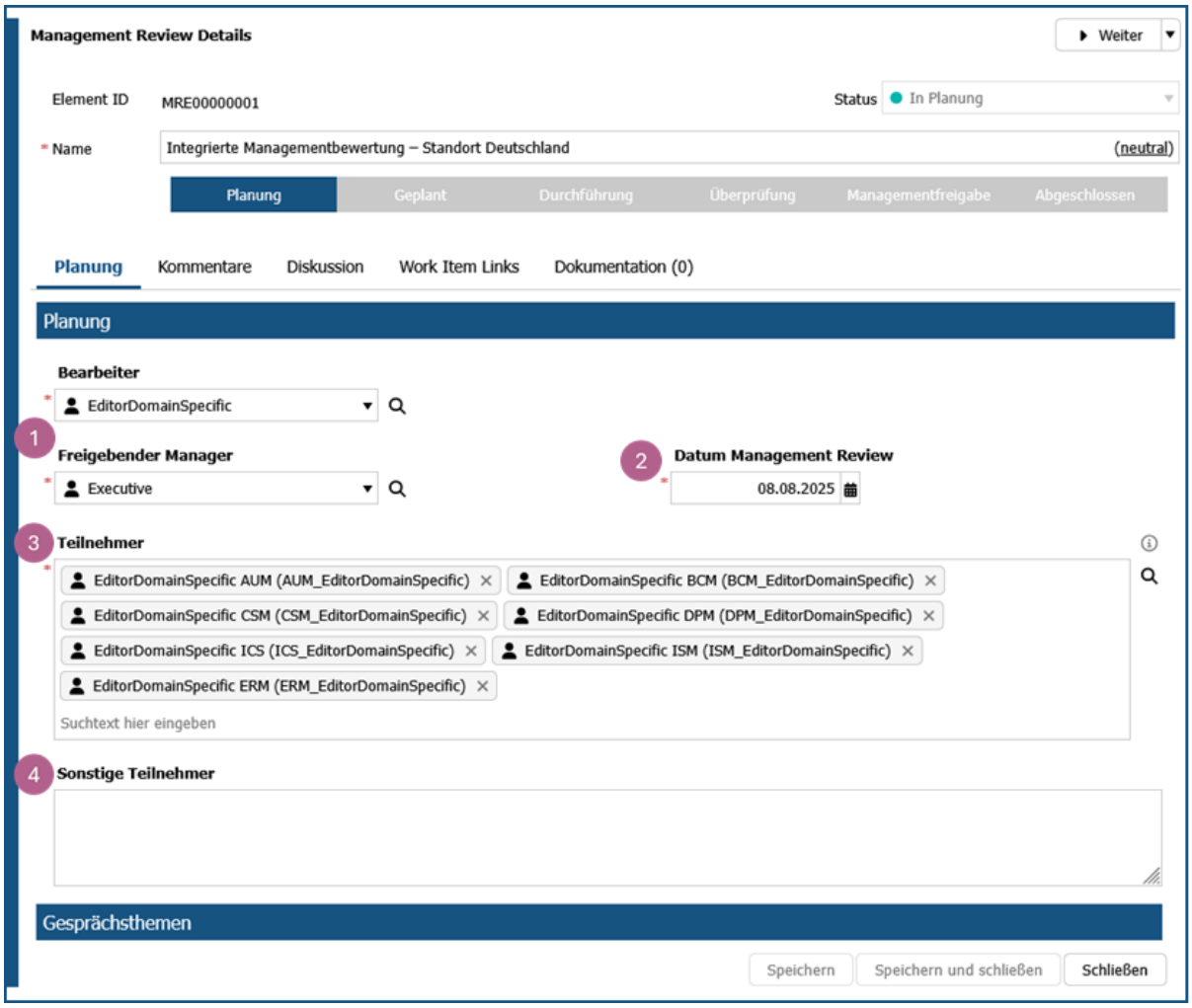
5 **Management Review Fragen** : Nachdem der Beabeiter DS GRC Perspektiven ausgewählt hat werden im darunter je nach gewählter Perspektive Links angezeigt. Diese Links führen jeweils zu einem GRC Framework "Fragen Management Review".

> Dabei werden dem Bearbeiter DS nur jene "Fragen Management Review" angezeigt, die den passenden Tag im GRC Framework zu der Link-Überschrift haben.

6 **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen, kann der *Management Review* erstmalig gespeichert werden

> Beim Speichervorgang wird der Ersteller automatisch als "Verantwortlicher" eingetragen.

Schritt 3: Weitere Informationen hinterlegen



1 **Verantwortliche Personen**: Der Bearbeiter wird automatisch in dem Feld "Bearbeiter" hinterlegt und kann noch geändert werden. Ein "Freigeber Manager", der für die Freigabe des *Management Reviews* verantwortlich ist muss vom Bearbeiter hinterlegt werden.

Dieser Benutzer wird durch das Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

> Anders als bei andere Work Item Typen ist der Freigeber hier ein Manager, also die Person mit dem höchsten Benutzerprofil. Der einzutragende Benutzer muss daher das Benutzerprofil "Executive" haben.

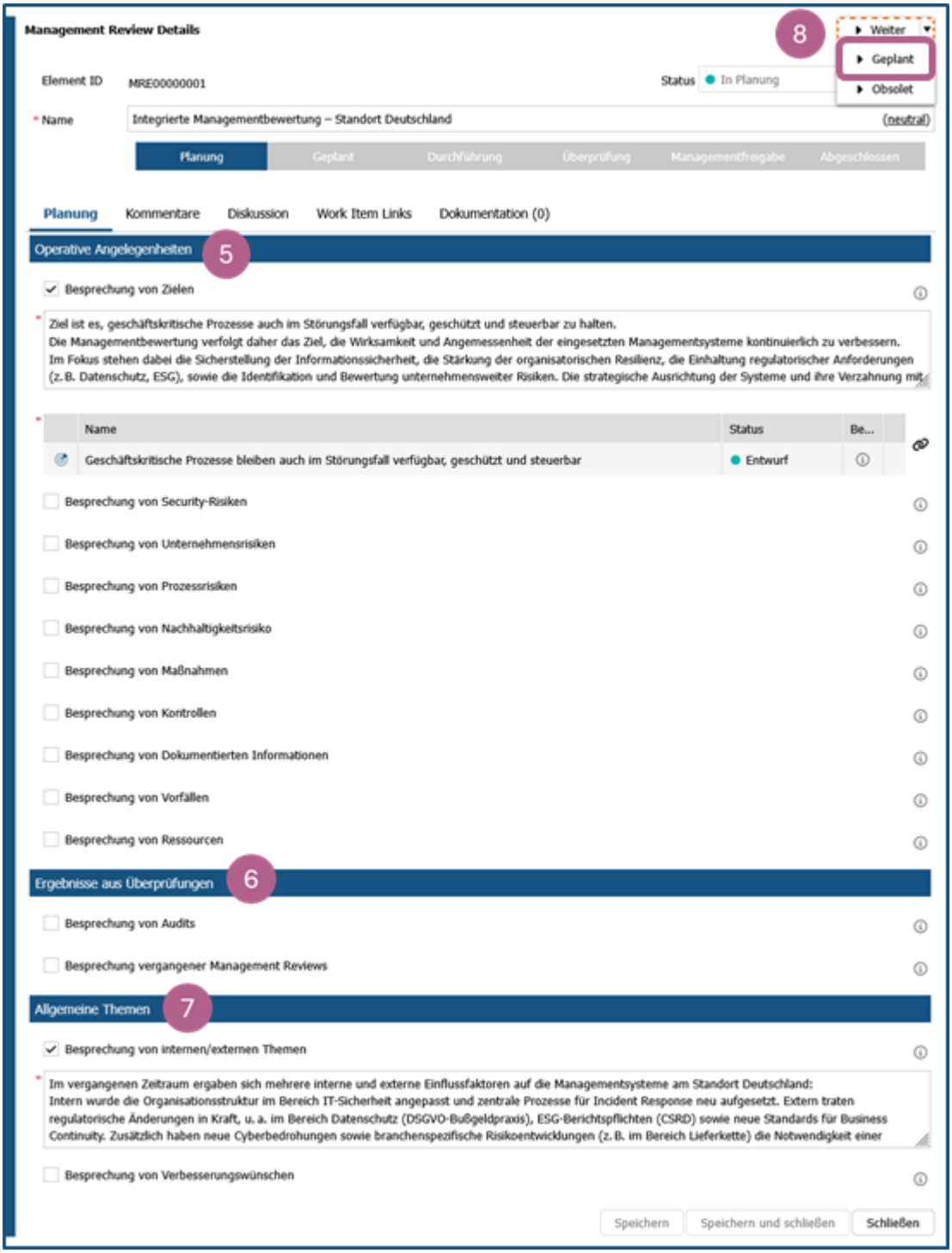
2. **Datum Management Review**: Dieses Datum gibt an wann der *Management Review* durchgeführt werden soll.

> Eine Woche vor der Erreichung des Datums bekommt der Bearbeiter eine Notifikation automatisch zugesendet, die ihn an die Durchführung erinnert.

3. **Teilnehmer**: Mittels des Icons  können alle Benutzer die in BIC GRC aktiv sind ausgewählt werden, um an dem *Management Reviews* mit zu wirken.
4. **Sonstige Teilnehmer**: Der Bearbeiter kann des weiteren noch schriftlich Teilnehmende dokumentieren, wenn diese kein Benutzer in BIC GRC sind.

> Diese Personen können auch nicht benachrichtigt werden oder bekommen Zugang zu dem Work Item.

Schritt 4: Management Review dokumentieren



5 **Operative Angelegenheiten**: Wenn der Bearbeiter vorhat im *Management Review* "Operative Angelegenheiten" anzusprechen, kann er dies mittels unterschiedlicher Checkboxen konkretisieren.

Sollte der Bearbeiter eine Checkbox anklicken werden im unter der Checkbox jeweils immer zwei zusätzliche Attribute angezeigt. Während eines davon zur Beschreibung dient, ist im anderen eine Verlinkung zu machen.

6. **Ergebnisse aus Überprüfungen**: In diesem Abschnitt ist der Fokus auf Ergebnisse von *Audits* und vorherigen *Management Reviews*.
7. **Allgemeine Themen**: Der Bearbeiter kann des weiteren noch schriftlich Teilnehmende dokumentieren, wenn diese kein Benutzer in BIC GRC sind.

> Diese Personen können auch nicht benachrichtigt werden oder bekommen Zugang zu dem Work Item.

8. **Statuswechsel**: Für den Statuswechsel muss zumindest eine Checkbox angeklickt und eine Beschreibung sowie Verlinkung hergestellt worden sein. Danach kann der Bearbeiter in den Status "Geplant" weiterschalten.

> Der eingetragene "Freigeber Manager" wird mittels Notifikation über den Statusübergang informiert.

> Nach der Eingabe aller notwendigen Informationen kann das Work Item gespeichert und ein Statusübergang durchgeführt werden, bevor das Fenster manuell geschlossen wird.

2.12.4 Management Review durchführen & überprüfen

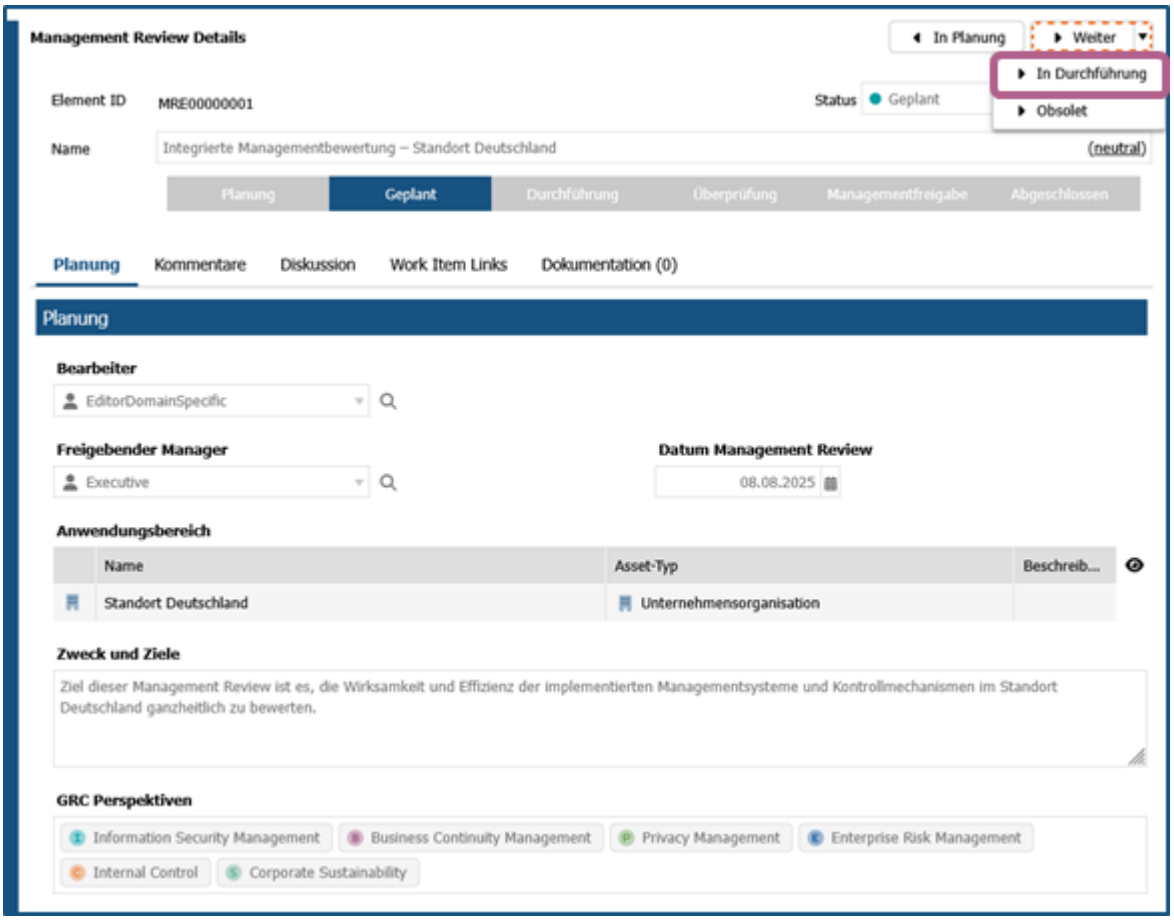
Der Bearbeiter DS wird sieben Tage vor der Erreichung des "Datum Management Review" automatisch von BIC GRC erinnert.

Schritt 1: Navigation zu Management Review

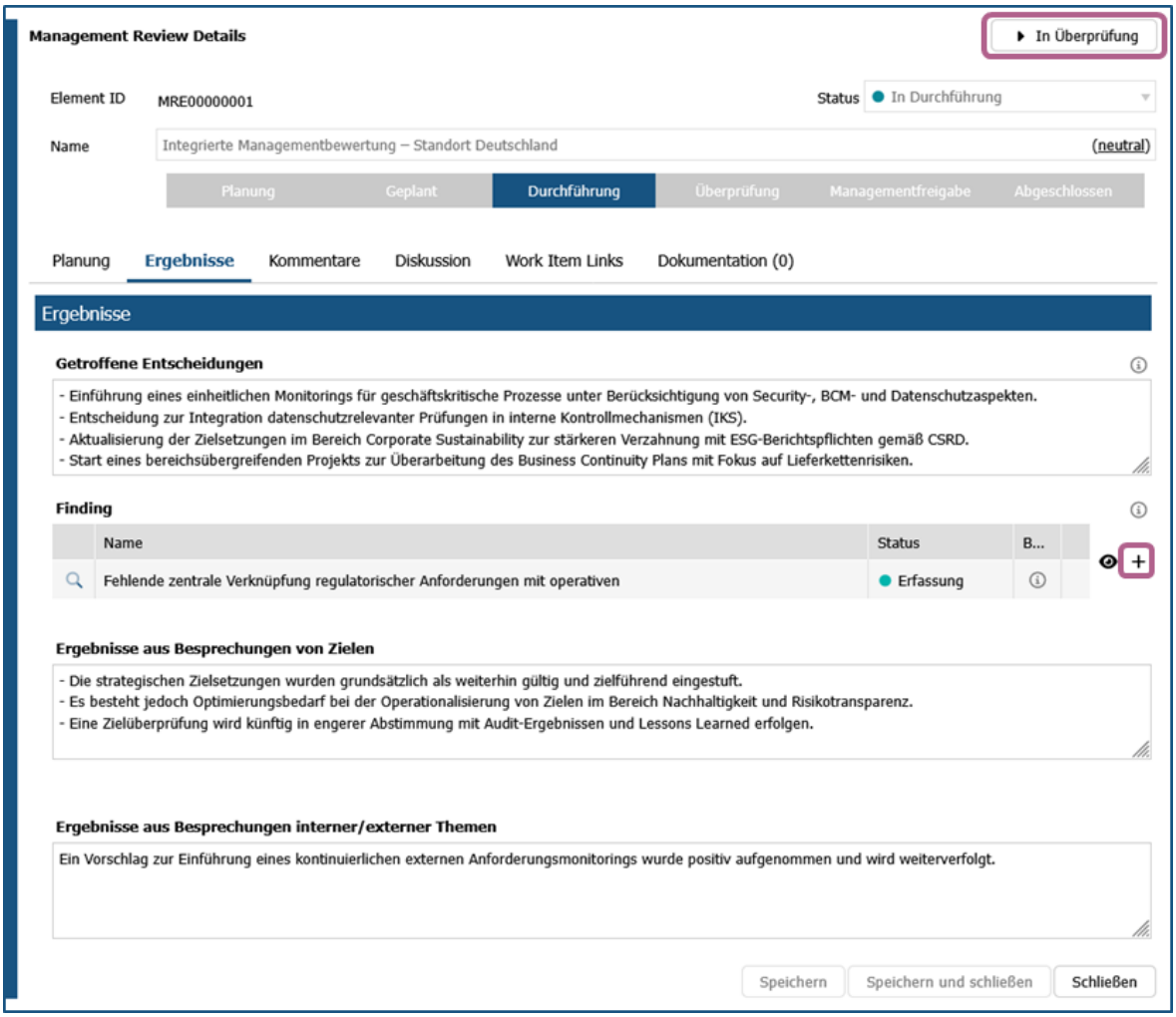
Der Bearbeiter DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald ein *Management Review* für die Durchführung bereit ist. Der Link zu dem spezifischen *Management Review* befindet sich in der Notifikation.

Schritt 2: Management Review durchführen

Der Bearbeiter DS hat in dem von ihm erstellten *Management Review* weiterhin alle Bearbeitungsrechte, um bei Bedarf bei bisher eingegebenen Informationen Erweiterungen vornehmen zu können.



Für die Durchführung wird empfohlen alle Eingaben aus dem Tab "*Planung*" erneut zu sichten. Anhand der Eingaben können dann zusammen mit dem "Freigeber Manager" Ergebnisse und Entscheidungen dokumentiert werden. Sollten *Findings* besprochen werden können diese über das Icon + erstellt werden. Mehr Informationen über die Erstellung des **Findings** unter Finding identifizieren & erstellen.

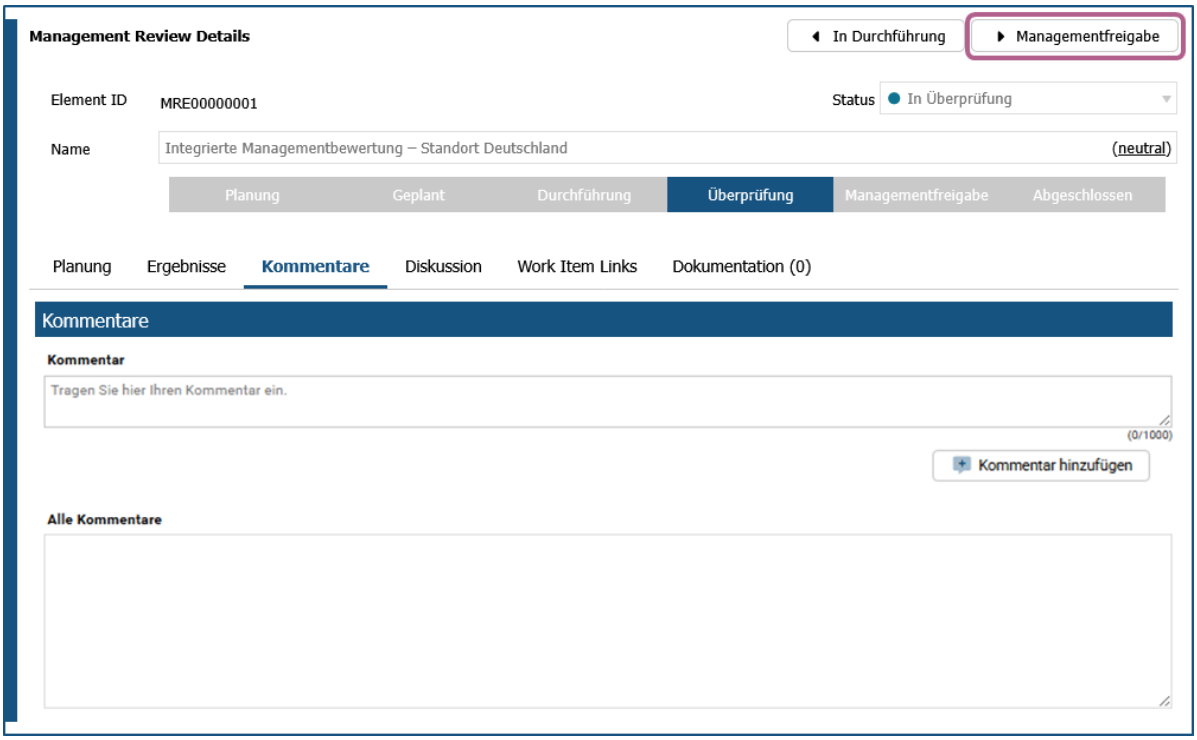


Schritt 3: Statusübergang durchführen

Der Bearbeiter DS kann nach der Eingabe aller Ergebnisse und Entscheidungen in den nächsten Status "Überprüfung" wechseln. In diesem Status ist weiterhin der Bearbeiter DS verantwortlich und kann bei Bedarf die besprochenen Themen ein letztes Mal selbständig überprüfen und finalisieren.

Der Bearbeiter DS kann im Status "Überprüfung" alle Attribute im Tab "*Ergebnisse*" bearbeiten. Es sind allerdings keine Attribute im Tab "*Planung*" sowie der Link zu den *Findings* mehr bearbeitbar.

Sind alle Ergebnisse und Entscheidungen finalisiert kann der Bearbeiter DS einen letzten Statusübergang in "Managementfreigabe" vornehmen. Der Benutzer im Attribut "Freigeber Manager" wird mittels Notifikation über den Statusübergang informiert.



2.12.5 Finding identifizieren & erstellen

Sollte der Bearbeiter DS während der Durchführung eines *Management Reviews* zu der Erkenntnis kommen, dass es Verbesserungspotenzial gibt, das im Rahmen des *Management Reviews* aufgekommen ist, muss der Bearbeiter DS ein *Finding* erstellen.

Schritt 1: Finding aus Management Review erstellen

Ein *Finding* kann aus einem *Management Review* entstehen.

Die Erstellung erfolgt durch das Icon + nach einer schriftlichen Stellungnahme unter "Getroffene Entscheidungen".

> Das *Finding* geht automatisch in dem *Management Review* auf.

Schritt 2: Finding dokumentieren

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Finding* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Finding* einzigartig.
2. **GRC-Perspektive**: Die Perspektive wird nicht automatisch aus dem *Management Review* übernommen, sondern der Bearbeiter kann jene Perspektiven auswählen, die im Rahmen des *Management Reviews* betrachtet worden sind.

3. **Bearbeiter**: In das Attribut soll jener Bearbeiter eingetragen werden der für das *Finding* des *Management Reviews* eine Behandlung durchzuführen hat.

   > Damit auf einen Blick erkennbar ist, von wem das *Finding* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

4. **Datum der Meldung**: Der Ersteller muss angeben, wann er das *Finding* offiziell gemeldet/entdeckt hat. Daher muss das Datum nicht mit dem tagesaktuellen Datum übereinstimmen.
5. **zu behandeln bis**: Unter dem Datum wird jenes Datum verstanden, bis zu dem das *Finding* behoben werden sollte. Es soll einen Hilfestellung sein, um eine Orientierung für im Workflow nachgelagerte Benutzer zu geben, bis wann die Behebung des *Findings* wünschenswert wäre.
6. **Art des Findings**: Der Ersteller kann im Rahmen von fünf Stufen einordnen, wie bedenklich das *Finding* im Kontext des *Management Reviews* ist.
7. **Finding für dieses Asset**: Das Asset wird automatisch aus dem Work Item übernommen und muss nicht manuell eingetragen werden.
8. **Beschreibung des Findings**: Die "Beschreibung des Findings" soll so viele Informationen und Inputs wie möglich enthalten, beispielsweise wie das *Finding* entdeckt wurde. Weiters kann möglicherweise Rückschlüsse auf Ursache und Wirkung entstehen.
9. **Priorität des Findings**: Dem *Finding* kann eine Priorität hinterlegt werden, die später für Auswertungen auf beispielsweise Dashboads verwendet werden kann.
10. **Statuswechsel**: Der Ersteller kann abschließend in den Status "Behandlung" schalten. Mehr Informationen zu dem Statuswechsel in Finding sichten & behandeln.

> Anschließend kann der Bearbeiter Management Review in den *Management Review* zurückkehren und mit der Dokumentation der Überprüfung des *Management Review* fortfahren. Bearbeiter DS - Management Review durchführen & überprüfen.

2.13 Freigeber "Domänenspezifisch"

Der Freigeber "Domänenspezifisch" hat die meisten Berechtigungen und Ansichten für seine Domäne. Er ist für die angemessene Führung von BIC GRC verantwortlich und somit nicht nur für die Assets, GRC Framework und Work Item Verwaltung, sondern auch für die Vorgaben des Managements und die Archivierung der Daten in BIC GRC.

> Der Freigeber "Domänenspezifisch" wird in den nächsten Kapiteln mit Freigeber DS abgekürzt.

Folgende vorbereitende Aufgaben hat der Freigeber DS:

- Ziel definieren & erstellen (Weiterleitung zu Bearbeiter Risiko - Ziel definieren & erstellen)
  - Zwischenziel definieren & erstellen (Weiterleitung zu Bearbeiter Risiko - Zwischenziel definieren & erstellen)
- IRO Template herleiten & erstellen

Folgende laufende Aufgaben hat ein Freigeber DS in BIC GRC:

- Nachhaltigkeitsmeldung sichten & bewerten

Der Freigeber DS kann darüber hinaus noch weitere Work Items erstellen in BIC GRC. Da dies aber nicht seine Hauptaufgabe ist, wird an dieser Stelle nur auf andere Benutzerprofile verwiesen:

- Nachhaltigkeitsrisiko identifizieren & erstellen
- Management Review definieren & erstellen
- Maßnahmen identifizieren & erstellen
- Kontrolle ableiten & erstellen

2.13.1 IRO Template herleiten & erstellen

In BIC GRC ist es möglich *IRO Templates* zu definieren und in Assessments des Typen "Doppelte Wesentlichkeit" den Assessoren zur Verfügung zu stellen. Hierzu kann der Freigeber DS das Work Item *IRO Template* erstellen.

Schritt 1: IRO Template erstellen

Der Freigeber navigiert über die Menüleiste zu **Work Items >> IRO Template >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: IRO Template definieren

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *IRO Template* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht das *IRO Template* einzigartig.
2. **Auswirkungstyp**: Der Freigeber muss angeben ob das Unternehmen auf die Umwelt wirkt - es handelt sich dann um eine "Nicht-finanzielle Auswirkung" - oder sein Unternehmen von der Umwelt beeinflusst wird, was einer "Finanziellen Auswirkung" auf das Unternehmen entspricht.

   > So wirkt eine CO2-Besteuerung auf das Unternehmen, während beispielsweise ein Fischereibetrieb Auswirkungen auf die Meere und somit Umwelt hat.

3. **Zeithorizont**: Das *IRO Template* braucht einen Zeithorizont für das es gültig ist.
4. **Beschreibung**: Das *IRO Template* sollte so ausführlich wie möglich dokumentiert und beschrieben werden, sodass auch andere Perspektiven einen Kontext bzw. Zusammenhang erkennen können.
5. **Zugehörige Topics**: Der Freigeber muss angeben welche Topics des ESRS 1 AR16 von diesem Topic angesprochen werden.

   > Diese Auswahl ist ausschlaggebend für die spätere Anzeige in den Assessments. Es

> werden im Assessment "Doppelte Wesentlichkeitsanalyse" dem Assessor für einen Unterpunkt des ESRS 1 AR16 nur *IRO Templates* angezeigt, wo die beiden GRC Framework Elemente einander matchen.

6. **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen kann das *IRO Template* erstmalig gespeichert werden.

> Beim Speichervorgang wird der Ersteller automatisch als "Bearbeiter" eingetragen.

Schritt 3: Bewertung hinterlegen

Abhängig von der Wahl "Nicht-finanzielle Auswirkung" oder "Finanziellen Auswirkung" werden dem Freigeber zwei Bewertungsmöglichkeiten angezeigt.

1. Bewertung "Nicht-finanzielle Auswirkung"

1. **Auswirkungsart**: Der Bearbeiter muss angeben, ob dies Auswirkung auf die Umwelt negativ oder positiv ist.

> Anders als in anderen Bereichen des Risikomanagements ist es im Nachhaltigkeitsbereich dezitiert gewünscht, dass auch positive Effekte aufgenommen werden.

2. **Potenziell oder Tatsächlich**: Dabei kann die Auswirkung potenziell sein (also sie kann eintreten) oder tatsächlich (es steht schon fest).
3. **Wahrscheinlichkeit**: Der Bearbeiter kann mittels einer 5-stufigen Einschätzung angeben, wie wahrscheinlich der Eintritt ist, mit dem die Umwelt positiv oder negativ beeinflusst wird.
4. **Schwere der Auswirkung**: Weiters muss mittels einer 5-stufigen Skala eingeschätzt werden, wie gravierend die Auswirkung wäre für die Umwelt.
5. **Verbreitung der Auswirkung**: Schlussendlich ist mittels einer 5- stufigen Einschätzung anzugeben, wie verbreitet die Auswirkung sein wird.

> So kann der Effekt von verschmutzten Abwasser abgeleitet vom eigenen Unternehmen in einen nahegelegenen See die Einschätzung "lokal" ergeben, bei einer Ableitung von verschmutzten Abwasser in die Meere kann die Einschätzung schon zwischen "national" und "kontinental" liegen.

6. **Beseitung möglich?**: Sollte es möglich sein die Auswirkungen wieder zu beseitigen, muss zusätzlich angegeben werden mit welcher Umfang/Aufwand dies erreicht werden kann.
7. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

> Die Freigabe eines *IRO Templates* ist nicht vorgesehen.

2. Bewertung "Finanziellen Auswirkung"

1. **Risiko oder Chance?**: Der Bearbeiter muss angeben, ob dies Auswirkung auf das Unternehmen ein Risiko birgt oder eine Chance sein könnte.

> Anders als in anderen Bereichen des Risikomanagements ist es im Nachhaltigkeitsbereich dezitiert gewünscht, dass auch positive Effekte aufgenommen werden.

2. **Was wird beeinflusst**: Aus diesem Blickwinkel wird betrachtet, auf was die Umwelt im finanziellen Bereich des eigenen Unternehmens wirken wird.

> So kann eine CO2-Besteuerung möglicherweise auf die Performance Einfluss haben.

3. **Stärke der Beeinflussung**: Weiters muss mittels einer 5-stufigen Skala eingeschätzt werden, wie stark die Auswirkung auf das Unternehmen wäre.
4. **Abhängigkeiten**: Des weiteren macht es Sinn anzugeben, auf welche Ressourcen bzw. Beziehungen sich die Auswirkung beziehen wird.
5. **Wahrscheinlichkeit**: Der Bearbeiter kann mittels einer 5-stufigen Einschätzung angeben, wie wahrscheinlich der Eintritt ist, mit dem das Unternehmen beeinflusst wird.
6. **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

> Die Freigabe eines *IRO Templates* ist nicht vorgesehen.

2.13.2 Nachhaltigkeitsmeldung sichten & bewerten

Wenn im Unternehmen eine *Nachhaltigkeitsmeldung* gemeldet wurde, kann der Freigeber DS die Dokumentation und Einschätzung bzw. Bewertung vornehmen.

Schritt 1: Navigation zu spezifischer Nachhaltigkeitsmeldung

Der Freigeber DS hat zwei Möglichkeiten eine zu bewertende *Nachhaltigkeitsmeldung* zu öffnen.

1. Öffnen über Notifikation

Der Freigeber DS bekommt eine E-Mail zugesendet, sobald der Ersteller die Meldung abgeschlossen und einen Statusübergang zu "Gemeldet" durchgeführt hat. Der Link zu der spezifischen *Nachhaltigkeitsmeldung* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine ToDo`s"

Im oberen Teil des Dashboards "Meine ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Staus anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber DS noch eine Bewertung durchzuführen hat.

Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Nachhaltigkeitsmeldung* automatisch.

Schritt 2: Nachhaltigkeitsmeldung sichten

Als erstes sollte der Freigeber DS eine Sichtung der Eingaben zu der Meldung vornehmen bevor er einen Statusübergang von "Gemeldet" in "In Bewertung" durchführt. Beim Statuswechsel wird er automatisch in den Tab "Bewertung" weitergeleitet.

Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.

Schritt 3: Bewertung durchführen

1. **Zuordnung**: Der Freigeber sollte mittels des Icons eine Zuordnung zu einem oder mehreren betroffenen "Themenbezogenen ESRS" vornehmen. Sollte es an dem angegebenen "Geltungsbereich" bereits ein Assessment des Typen "Doppelte Wesentlichkeitsanalyse" geben, wird es dem Freigeber angezeigt und er kann eine passende Verlinkung vornehmen.

   Die *Nachhaltigkeitsmeldung* wird anschließend an den passenden GRC Framework Elementen im Assessment angegeben, um eine bessere Referenz für die nächste Bewertung des Assessments zu haben.

2. **Mitwirkende**: Der Freigeber kann angeben, ob er dazu in der Lage war die Bewertung der Meldung alleine vorzunehmen, oder ob er sich Unterstützung durch Experten im Unternehmen dazu geholt hat.
3. **Schadenseinordnung**: Der Bearbeiter kann in vier Kategorien entscheiden, ob der *Nachhaltigkeitsmeldung* zu nachgelagerten Auswirkungen führen kann. Anhand einer Heatmap kann er zwischen vier Schweregraden oder einer nicht-Relevanz entscheiden. Die vorgegebenen Kategorien sind hierbei immer:
   - Strafrechtliche Sanktionen
   - Beeinträchtigung der Vertragserfüllung
   - Beeinträchtigung der Aufgabenerfüllung
   - Vertrauens- oder Reputationsverlust
4. **Zeitliche Relevanz**: Neben der Einordnung ob für eine bestimmte Kategorie eine Relevanz besteht muss zusätzlich ein passender Zeihorizont angegeben werden. Nur wenn der Freigeber "Nicht Relevant" auswählt muss kein Zeithorizont angegeben werden.
5. **Risikozuordnung**: Der Bearbeiter kann bei Bedarf ein passendes *Nachhaltigkeitsrisiko* verlinken oder erstellen. Mehr Informationen dazu unter Bearbeiter - Risiko - Nachhaltigkeitsrisiko identifizieren & erstellen.
6. **Beschreibung**: Anschließend kann der Freigeber noch seine Bewertung und Einschätzung begründen. Dafür stehen im unter der Bewertung die Attributsfelder "Beschreibung der

Bewertung", "Einschätzung der potenziellen Auswirkung" und "Zusätzliche Informationen" zur Verfügung, wobei nicht alle Angaben verpflichtend auszufüllen sind.

7 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Abgeschlossen" durchgeführt.

> Nach dem Speichervorgang wird der Erfasser mittels Notifikation benachrichtigt.

2.14 Dokumenteneigner

Der Dokumenteneigner ist ein besonderes Benutzerprofil. Benutzer dieses Profils setzen sich mit der Hinterlegung und Pflege eines oder mehrere Dokumentierter Informationen in BIC GRC auseinander. Ihre Hauptaufgabe ist daher in erster Linie die Erstellung und regelmäßige Überprüfung des Dokuments auf deren Aktualität.

- Dokumentierte Information definieren & erstellen
- Dokumentierte Information evaluieren & überprüfen

2.14.1 Dokumentierte Information definieren & erstellen

Dokumentierte Informationen können in BIC GRC an mehreren Stellen verwendet und eingesetzt werden. Für die Erstellung und Pflege ist aber ausschließlich der Dokumenteneigner verantwortlich.

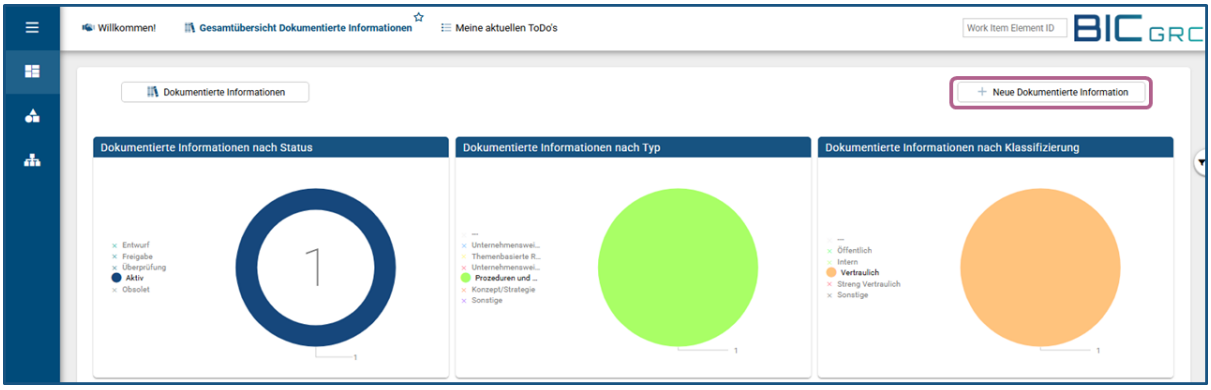
Schritt 1: Dokumentierte Information erstellen

Der Dokumenteneigner kann in BIC GRC an mehreren Stellen *Dokumentierte Informationen* erstellen.

1. Erstellen über Dashboard "Gesamtübersicht Dokumentierte Information"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Gesamtübersicht Dokumentierte Information >> "Neuer Dokumentierte Information"**

Die Erstellung eines neuen *Dokumentierte Information* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

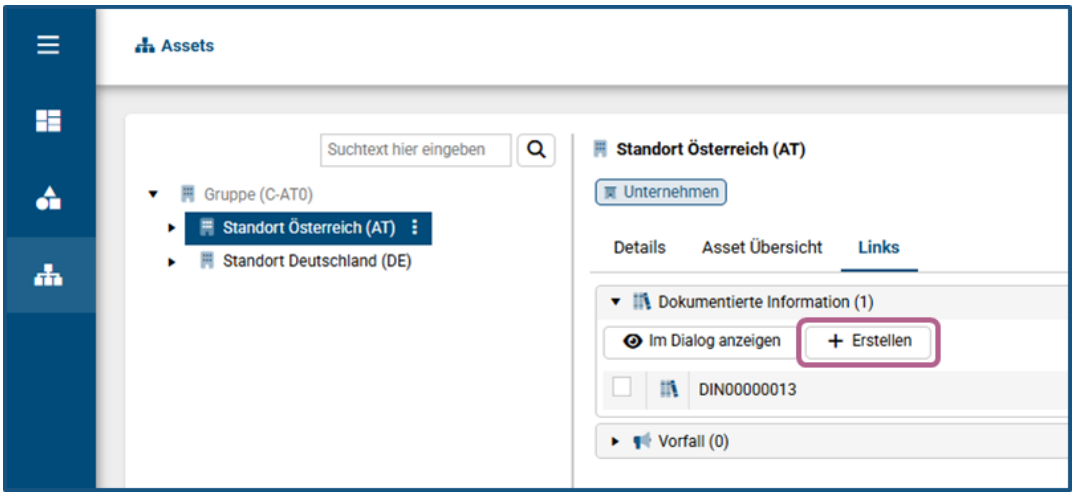


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellen über Asset Übersicht "Links"

Der Bearbeiter navigiert über die Menüleiste zu **Assets >> Auswahl des Assets >> Links >> Öffnen des Reiters "Dokumentierte Information" >> "Erstellen"**

Die Erstellung eines neuen *Dokumentierte Information* wird durch einen Button "Erstellen" in der Mitte des Fensters durchgeführt.

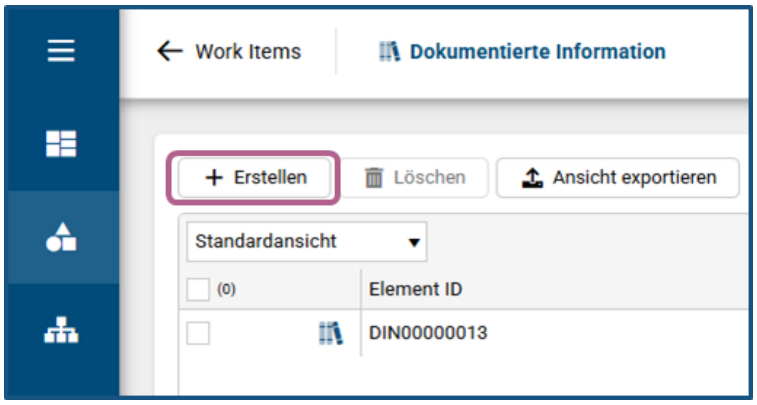


Ein neues Fenster öffnet sich anschließend automatisch.

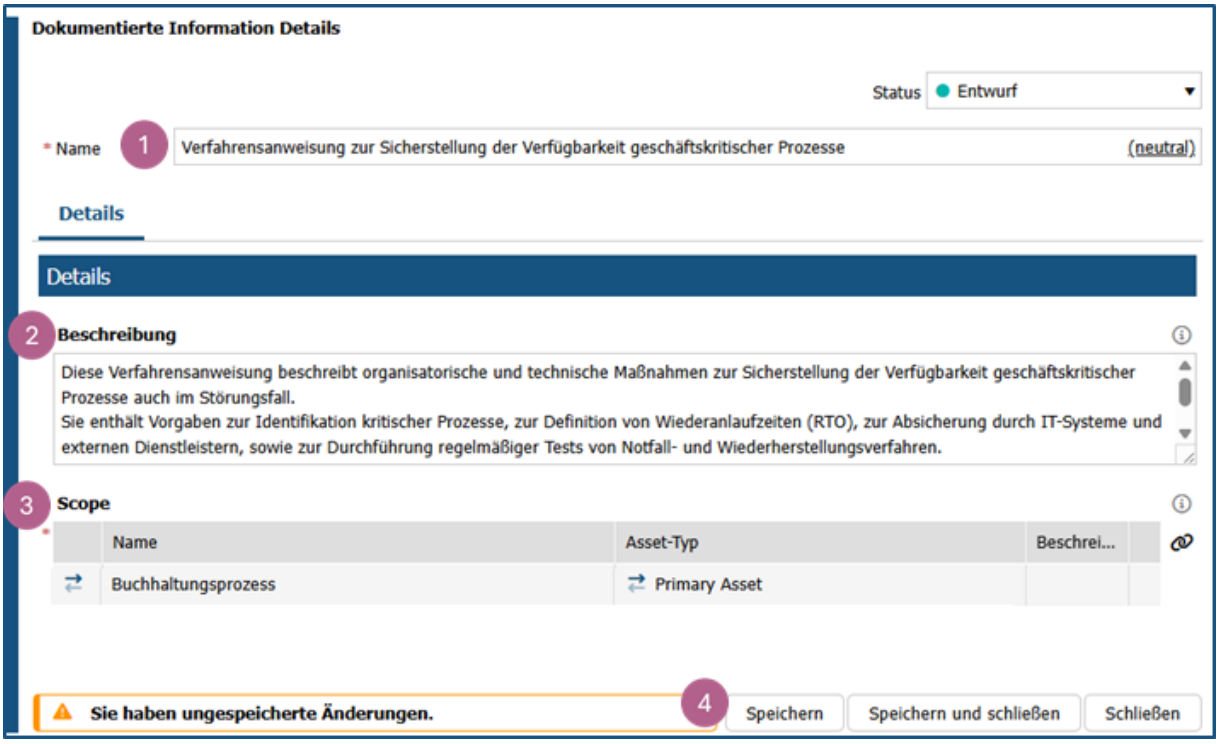
3. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Dokumentierte Information >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen



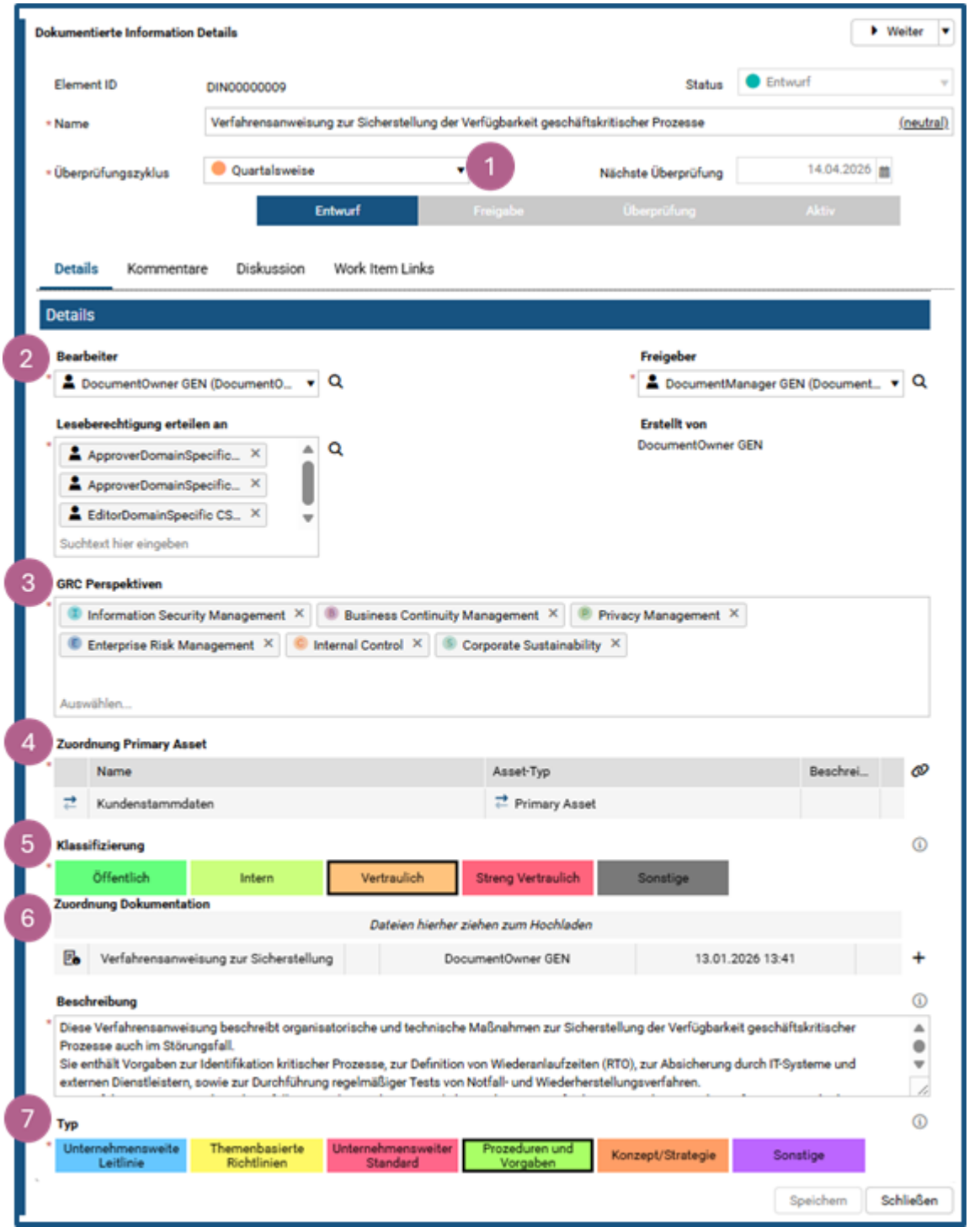
1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Dokumentierte Information* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Dokumentierte Information* einzigartig.
2. **Beschreibung**: Anschließend ist eine Beschreibung des *Dokumentierte Information* zu hinterlegen. Alle Benutzer, die im Workflow der *Dokumentierte Information* nachgelagert sind, orientieren sich an dieser Beschreibung, daher sollte sie so viele notwendige Informationen und Daten wie möglich enthalten.
3. **Scope**: Der Dokumenteneigner kann mittels des Icons ein Asset verlinken.

   > Es werden nur Assets der Typen "Primary Asset" und "Organisationseinheit" unterstützt.

   > Der "Scope"-Link wird automatisch befüllt, wenn die Erstellung über die Asset-Ansicht (2) erstellt worden ist.

4. **Speichern**: Sobald die Informationen angegeben sind kann der Dokumenteneigner speichern.

Schritt 3: Eingaben vervollständigen



1 **Überprüfungszyklus**: Der Dokumenteneigner muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft eine *Dokumentierten Information* zurück in den Status "Überprüfung" geschalten wird, um die *Dokumentierten Information* in regelmäßigen Zeitabständen zu evaluieren.

> Das Attributsfeld "Nächste Überprüfung" wird automatisch von BIC GRC gesetzt.

2 **Verantwortliche Personen**: Der Dokuementeneigner wird automatisch in dem Feld "Bearbeiter" hinterlegt und kann nicht mehr geändert werden. Ein Dokumentenmanager der für die Freigabe der *Dokumentierten Information*verantwortlich ist, muss vom Bearbeiter im Benutzerattribut "Freigeber" hinterlegt werden.

> Zusätzlich können noch "Leseberechtigte Personen" ausgewählt werden, die aufgrund ihres Benutzerprofils aus dem Standard heraus nicht Leseberechtigt wären, aber Zugriff auf diese Information bräuchten.

Dieser Benutzer wird durch das  Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

> Damit auf einen Blick erkennbar ist, von wem die *Dokumentierten Information* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

3 **GRC Perspektive**: Um die *Dokumentierten Information* eindeutig einer oder mehreren Perspektiven zuordnen zu können muss der Dokumenteneigner Perspektiven hinterlegen.

> Die Anzahl der angezeigten GRC Perspektiven ist abhängig von den freigeschaltenen Modulen.

4 **Zuordnung Primary Asset**: Dieser Link kann freiwillig befüllt werden, da ein "Primary Asset" auch in erster Linie Informationen sein können und somit ein Konex geschaffen wird.

5 **Klassifizierung**: Mittels eines Klassifizierungsschema kann den *Dokumentierten Informationen* eine oder keine Vertraulichkeit der Information zugeordnet werden.

6 **Zuordnung Dokumentation**: Die Zuordnung ist das Kernstück des Work Items, da hier mittels Link, Memo oder Anhang die Information angehängt wird.

> Handelt es sich um eine Datei, kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend im Attributsfeld verlinkt.

7 **Typ**: Der Typ unterstützt bei der Einordnung, inwiefern die *Dokumentierte Information* einem oder mehreren Benutzerkreisen zugänglich sein sollte.

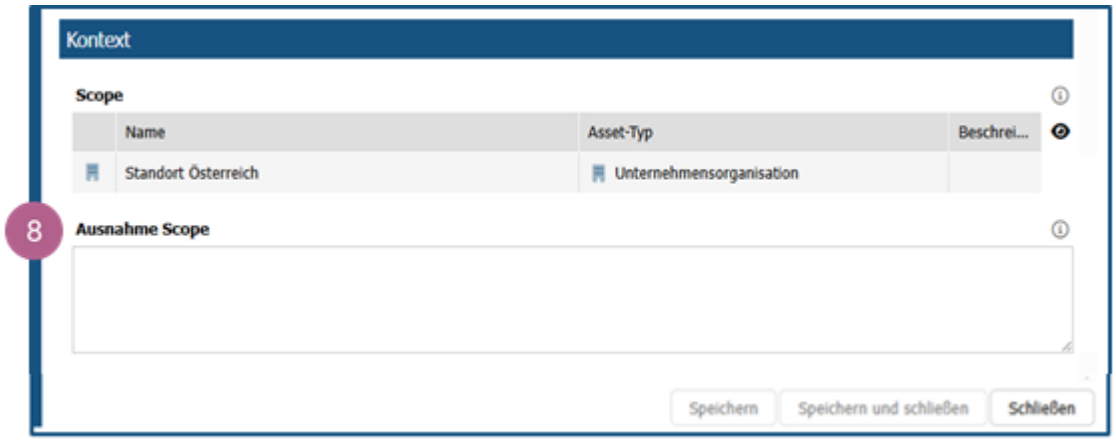
> Sollte kein Typ passend sein kann der Dokumenteneigner einen "Sonstigen Typ" auswählen. Ist "Sonstiges" ausgewählt wird dem Dokumenteineigner ein zusätzliches Attribut angezeigt, in dem er manuell einen Text hinterlegen kann.

8 **Ausnahme Scope**: Neben dem anfänglich hinterlegten Scope kann der Dokumenteneigner zusätzlich schriftlich hinterlegen, ob es Ausnahmen bei diesem Scope gibt.

9 **Statuswechsel**: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Freigabe" durchgeführt.

> Der Dokumentenmanager wird mittels Notfikation automatisch über den

Statusübergang informiert.



Nach der Eingabe aller notwendigen Informationen kann das Work Item gespeichert und ein Statusübergang durchgeführt werden, bevor das Fenster manuell geschlossen wird.

Sollten die Eingaben nicht richtig oder unvollständig sein, kann der Dokumentenmanager ein Kommentar in dem Tab "Kommentar" hinterlassen und die *Dokumentierte Informationen* erneut in den Status "Entwurf" setzen. Der Dokumenteneigner wird über diesen Vorgang mittels Notifikation benachrichtigt.

2.14.2 Dokumentierte Information evaluieren & überprüfen

Der Dokumenteneigner sollte die *Dokumentierte Information* regelmäßig dahingehend überprüfen, ob die *Dokumentierte Information*in seiner Art und Weise noch aktuell und korrekt ist.

Um dies in regelmäßigen Abschnitten zu überprüfen, unterstützt das Feld "Nächste Überprüfung". Zwei Wochen vor dem erreichen des Datums bekommt der Bearbeiter eine Notifikation automatisch zugesendet, die ihn an eine bevorstehende Neubewertung erinnert.

An dem Tag der "Nächsten Überprüfung" wird die *Dokumentierte Information* im Status "Aktiv" in den Status "Überprüfung" geschalten und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.

Das Datum wird nach dem Statuswechsel automatisch neu gesetzt abhängig von der Zeitangabe in "Überprüfungszyklus".

Wenn die *Dokumentierte Information* einer der Überprüfungszyklen "Alle ... Tage", "Anlassbezogen", "Täglich" oder "Wöchentlich" hat, wird der Status nicht automatisch zurückgesetzt und der Bearbeiter wird nicht über einen Statusübergang mittels Notifikation benachrichtigt.

Schritt 1: Navigation zu Dokumentierte Information

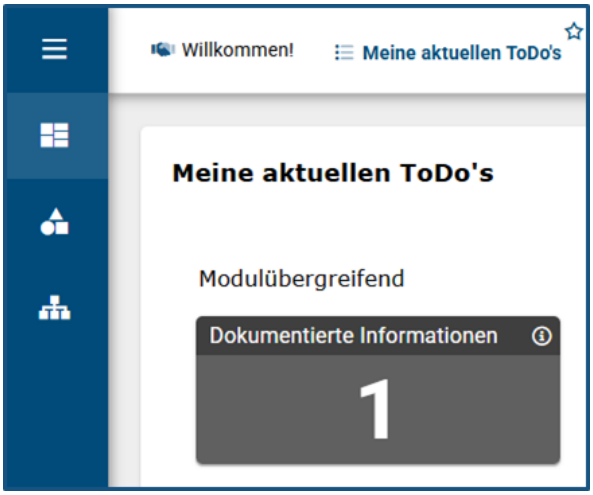
Der Dokumenteneigner hat zwei Möglichkeiten, eine zu bearbeitende *Dokumentierte Information* zu öffnen.

1. Öffnen über Notifikation

Der Dokumenteneigner bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald das Datum des Überprüfungszyklus erreicht ist. Der Link zu der spezifischen *Dokumentierte Information* befindet sich in der Notifikation.

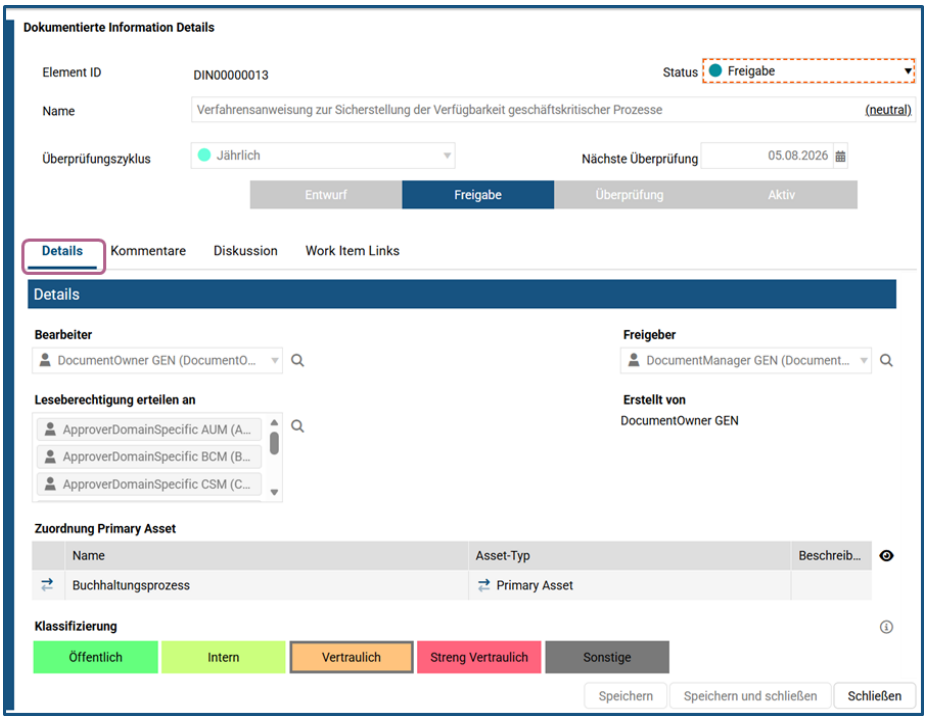
2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Dokumenteneigner noch eine Aufgabe zu erledigen hat.



Schritt 2: Dokumentierte Information sichten

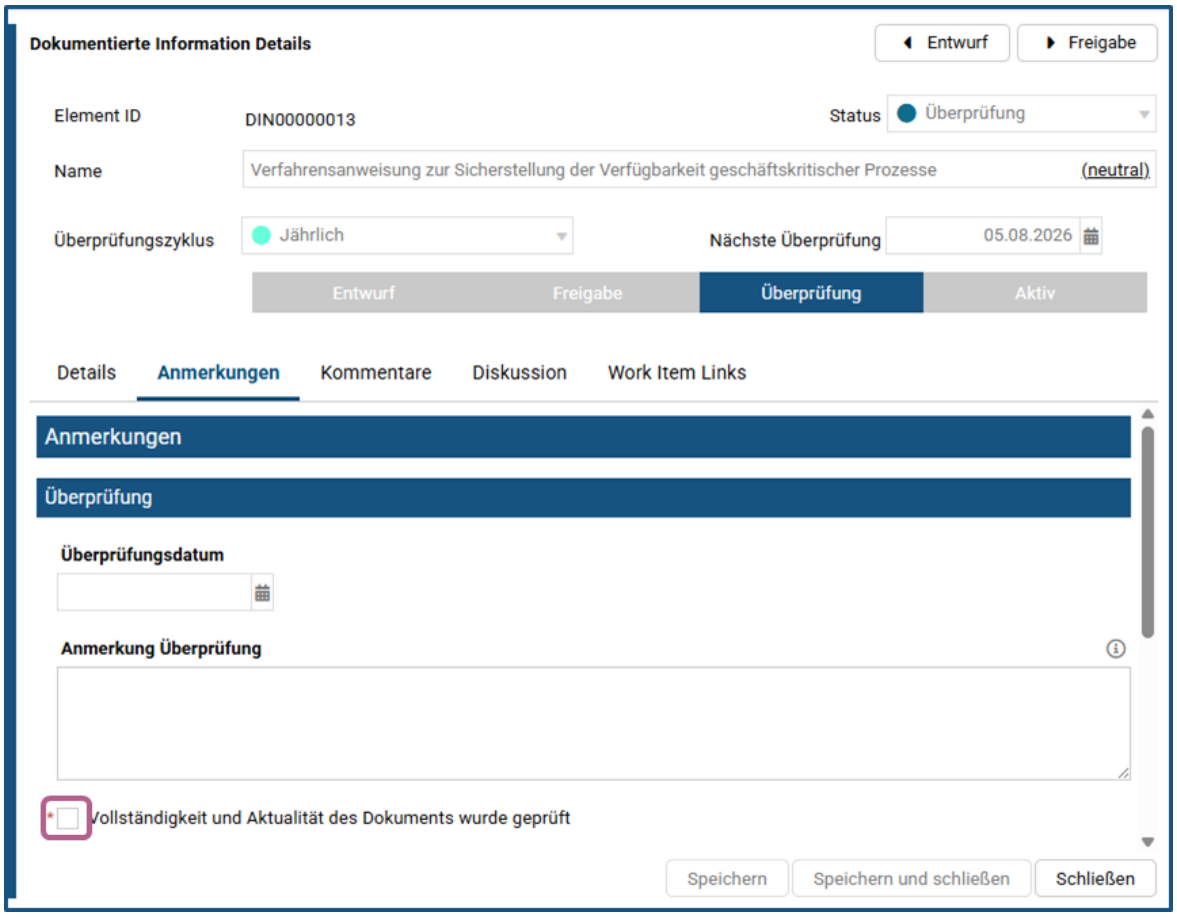
Der Dokumenteneigner sollte bei der Überprüfung mit der Überprüfung des Tabs "Details" beginnen.



> Der Dokumenteneigner kann die Eingaben im Status "Überprüfung" nur sichten, aber keine Änderungen vornehmen. Möchte der Dokumenteneigner Änderungen vornehmen, muss er in den Status "Entwurf" zurückschalten.

Schritt 3: Anmerkung hinterlassen

Der Dokumenteneigner hat in dem Tab "*Anmerkung*" noch die notwendige Überprüfung auf Vollständigkeit und Aktualität zu machen, indem er die Checkbox "Vollständigkeit und Aktualität des Dokuments wurde geprüft" anklickt.



Zusätzlich kann er eine schriftliche Anmerkung hinterlassen.

Das Datum "Überprüfungsdatum" wird von BIC GRC automatisch gesetzt, sobald der Dokumenteneigner den Statuswechsel durchgeführt hat.

Nach dem Statusübergang in den Status "Freigabe" kann das Fenster geschlossen werden.

2.15 Dokumentenmanager

Das Benutzerprofil Dokumentenmanager ist für die Freigabe und ordnungsgemäße Ablage einer spezifischen Information in BIC GRC verantwortlich.

2.15.1 Dokumentierte Information überprüfen & freigeben

Nach der Erstellung und Hinterlegung einer *Dokumentierte Information* durch einen Dokumenteneigner, muss diese vor der Aktivierung einer Freigabe durch den Dokumentenmanager vollzogen werden.

Schritt 1: Navigation zur Dokumentierten Information

Der Dokumentenmanager hat zwei Möglichkeiten, eine zu bearbeitende *Dokumentierte Information* zu öffnen.

1. Öffnen über Notifikation

Der Dokumentenmanager bekommt eine E- Mail zugesendet, sobald der Dokumenteneigner den Status der *Dokumentierte Informationzu* "Freigabe" wechselt. Der Link zu der spezifischen *Dokumentierte Information* befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Dokumentenmanager noch eine Aufgabe zu erledigen hat.

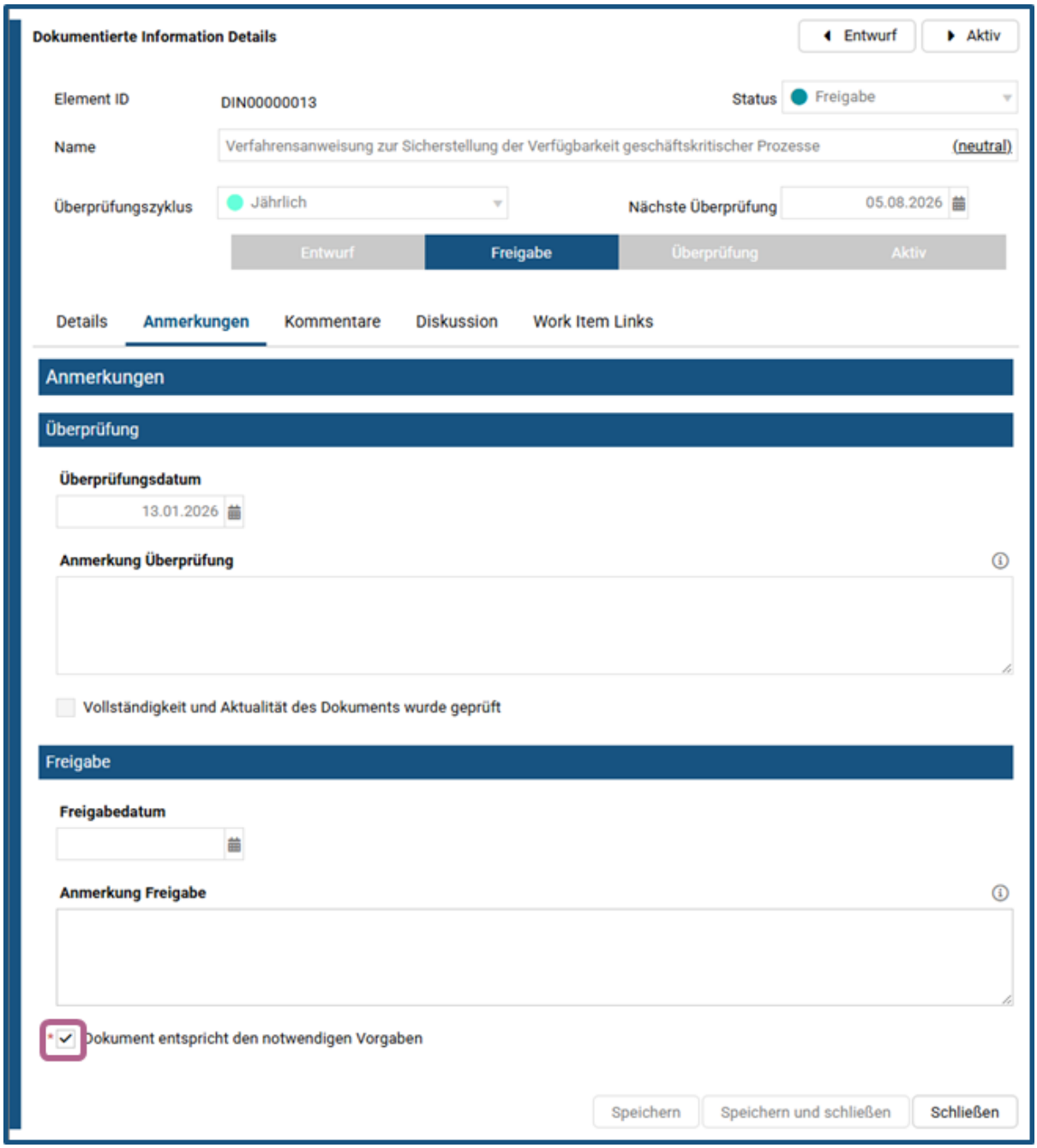
Schritt 2: Dokumentierte Information sichten

Der Dokumentenmanager hat in der erstellten und hinterlegten *Dokumentierte Information* alle Leserechte, um auf Basis aller eingegebenen Informationen zu entscheiden, ob die *Dokumentierte Information* in einem ausreichenden Ausmaß beschrieben und eingeordnet wurde. Wenn dies der Fall ist, kann der Dokumentenmanager in Status "Aktiv" weiterschalten.

Sollte dies nicht der Fall sein und muss die *Dokumentierte Information* aus Sicht des Dokumentenmanagers erneut bewertet werden, kann der Dokumentenmanager einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "Entwurf" durchführen.

Schritt 3: Anmerkung hinterlassen

Der Dokumentenmanager hat in dem Tab "*Anmerkung*" noch die notwendige Freigabe zu machen, indem er die Checkbox "Dokument entspricht den notwendigen Vorgaben" anklickt.



Zusätzlich kann er eine schriftliche Anmerkung hinterlassen.

Das Datum "Freigabedatum" wird von BIC GRC automatisch gesetzt, sobald der Dokumentenmanager den Statuswechsel durchgeführt hat.

Nach dem Statusübergang kann das Fenster geschlossen werden.

2.16 Bearbeiter Audit

Der Bearbeiter Audit ist in BIC GRC für die Planung, Erstellung und Durchführung von Audits verantwortlich. Er kann diese Audits im Rahmen der vorhandenen Informationen der Module in BIC GRC durchführen.

Folgende Aufgaben hat ein Bearbeiter Audit in BIC GRC:

- Audit definieren & erstellen
  - Auditaktivität definieren & planen
- Audit starten & durchführen
  - Auditaktivität starten & durchführen
  - Finding identifizieren & erstellen
  - Finding verwalten & behandeln
  - Maßnahme definieren & erstellen
- Audit bewerten & abschließen

2.16.1 Audit definieren & erstellen

In BIC GRC können in regelmäßigen Abständen Audits durchgeführt werden.

> Audits können freiwillig auf Basis der Informationen und Daten in BIC GRC durchgeführt werden.

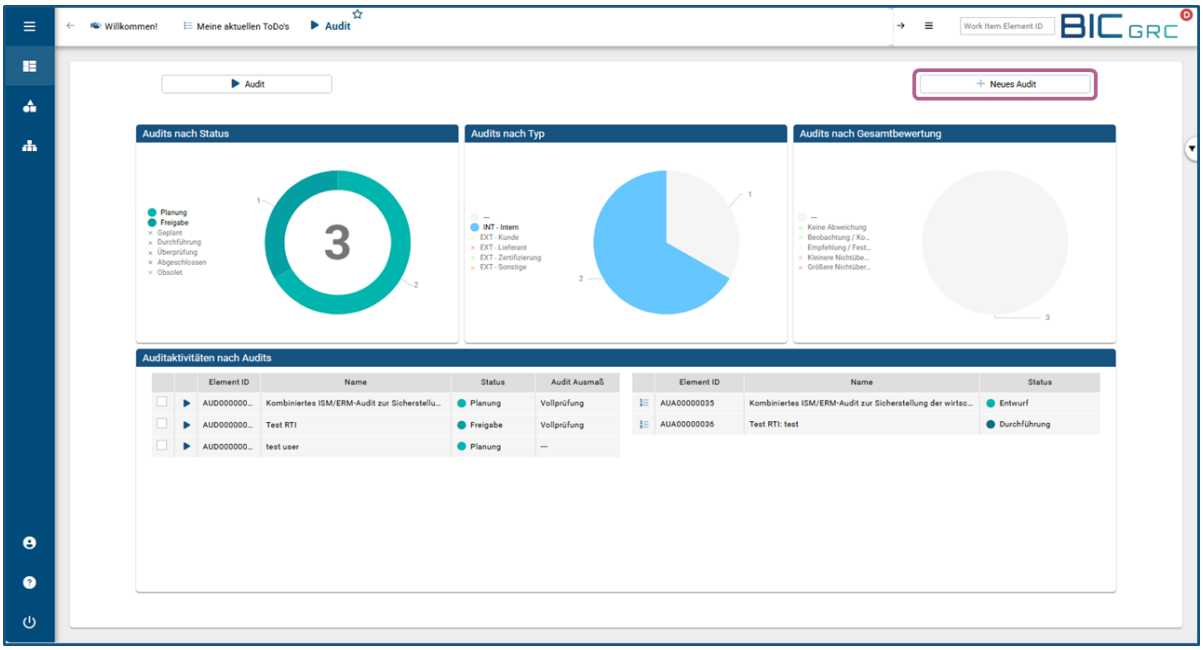
Schritt 1: Audit erstellen

Der Bearbeiter Audit kann in BIC GRC an mehreren Stellen *Audits* erstellen.

1. Erstellen über Dashboard "Audit"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Audit >> "Neues Audit "**.

Die Erstellung eines neuen *Audits* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

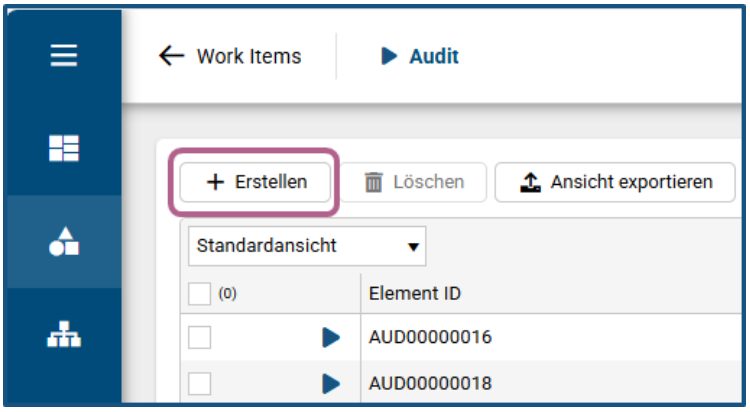


Ein neues Fenster öffnet sich anschließend automatisch.

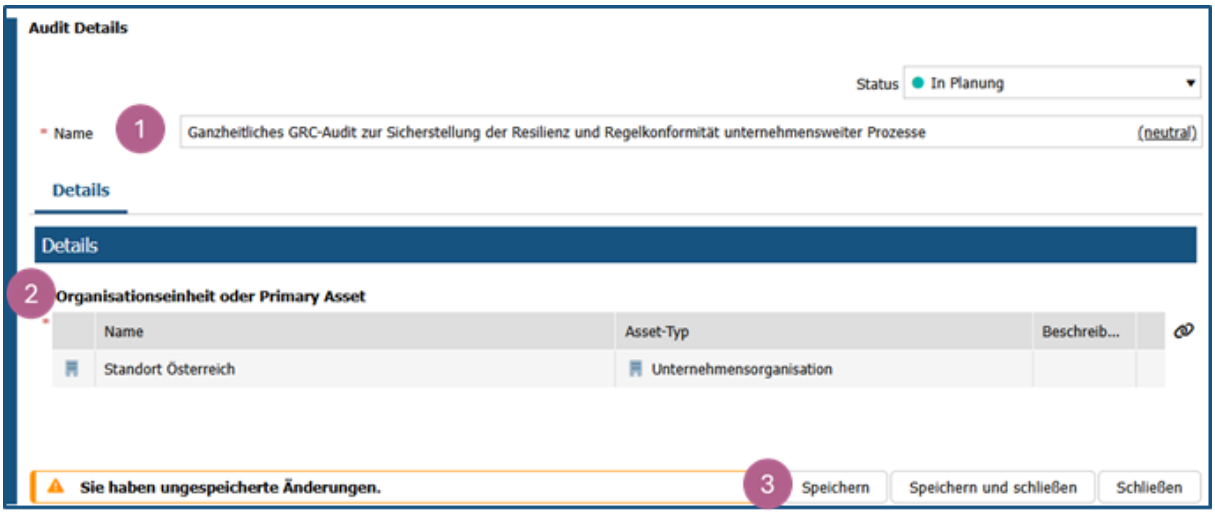
2. Erstellunf über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Audit >> "Erstellen"**.

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen

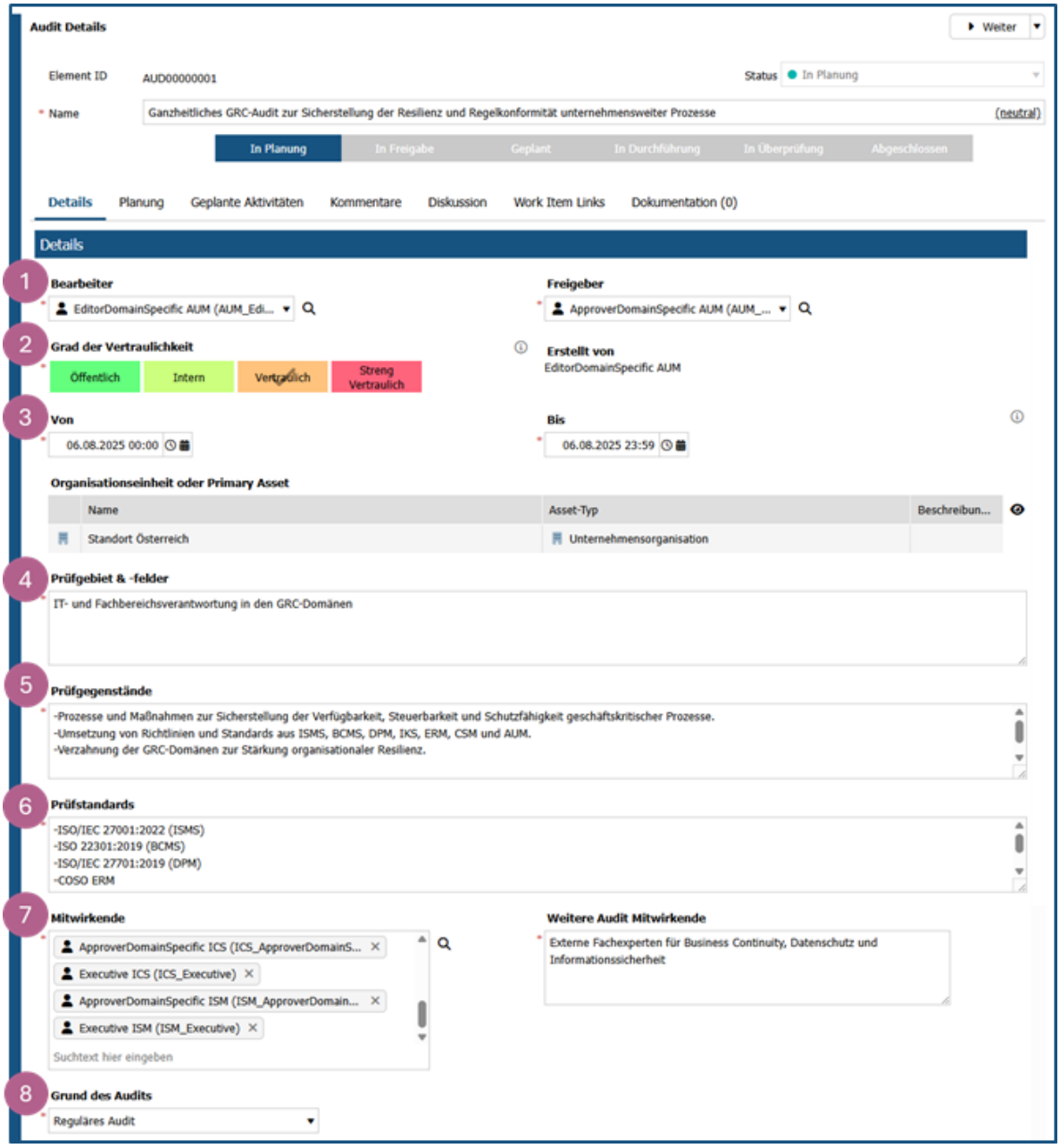


1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Audit* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Audit* einzigartig.
2. **Asset**: Es ist eine Verlinkung mittels des Icons  zu einer "Organisationseinheit" oder einem "Primary Assets" notwendig, wobei vorselektiert Assets angezeigt werden, bei denen der Bearbeiter Berechtigungen hat.

   > Wird das *Audit* über "2. Erstellen über Asset Übersicht Links" erstellt, wird der Link zur Organisationseinheit automatisch gesetzt von BIC GRC.

   > Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer keine Rolle auf dem Asset zugewiesen, das er verlinken möchte. Mittels des Work Items *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.
3. **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen, kann das *Audit* erstmalig gespeichert werden

Schritt 3: Details ergänzen



1 **Verantwortlichkeiten**: Der Bearbeiter wird automatisch in dem Attribut "Bearbeiter" eingetragen. Weiters ist ein "Freigeber " zu nominieren der das *Audit* freigibt.

Dieser Benutzer wird durch das Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.

> Damit auf einen Blick erkennbar ist von wem das *Audit* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

2 **Grad der Vertraulichkeit**: Der Bearbeiter kann hinterlegen mit welcher Vertraulichkeit dieses Audit zu behandeln ist.

> Diese Information wird auch später bei der Erstellung des Berichts auf dem Deckblatt angezeigt.

3. **Zeitraum**: Es sollte ein Zeitraum angegeben werden in dem das *Audit* durchgeführt wird. Dabei wird ein Vorschlagsdatum für den nächsten Tag automatisch hinterlegt, wenn der Bearbeiter das Audit erstmalig speichert.

> Dabei kann nicht nur ein Zeitraum mittels Daten hinterlegt werden, sondern auch die genaue Uhrzeit, falls das *Audit* beispielsweise nur für 2 Stunden an einem Tag geplant wäre.

4. **Prüfgebiet & -felder**: Zusätzlich muss das Textfeld "Prüfgebiet & -felder" ausgefüllt werden.

5. **Prüfgegenstände**: Der Bearbeiter hat schriftlich zu hinterlegen, welche Prüfgegenstände als Basis für das Audit herangezogen werden.

6. **Prüfstandards**: Der Bearbeiter hat schriftlich anzugeben welche Standards als Grundlage dienen.

7. **Mitwirkende & Weitere Audit Mitwirkende**: Mittels des Icons kann der Bearbeiter mittwirkende Benutzer aus BIC GRC auswählen.

   Weitere Audit Mitwirkende: Sollten die mitwirkenden keinen Benutzer in BIC GRC haben können die beteiligten Personen auch in Textform hinterlegt werden.

8. **Grund des Audits**: In BIC GRC gibt es zwei Gründe um ein *Audit* durchzuführen: eine reguläre Prüfung oder eine Sonderprüfungen.

> Sollte der Grund eine "Sonderprüfung" sein muss der Bearbeiter zusätzlich angeben, um welche Kategorie von Anlass es sich handelt bzw. muss er den Anlassfall mit einigen Worten beschreiben.

9. **Audit Typ**: Der "Audit Typ" gibt an, ob es sich um eine interne oder externe Prüfung bzw. einem Kunden- oder Lieferantenaudit handelt.

> Wir bei "Grund des Audits" "Sonderprüfung" angegeben kann der Benutzer nicht den Typen "Zertifizierung" auswählen.

> Wird entweder Lieferanten- oder Kundenaudit ausgewählt wird dem Bearbeiter zusätzlich ein Link zu dem passenden GRC Framework angezeigt, sodass der betroffene Lieferant/Kunde direkt verlinkt werden kann.

10. **Audit Kategorie**: Es werden dem Bearbeiter mehrere Kategorien angezeigt aus denen er auswählen kann um welche Art von *Audit* es sich handeln wird.

11. **Audit Ausmaß**: Der Bearbeiter hat zu entscheiden, ob es sich um ein Voll- oder nur ein Teilaudit handeln wird. Abhängig von der Eingabe wird der Scope der Prüfung größer oder kleiner.

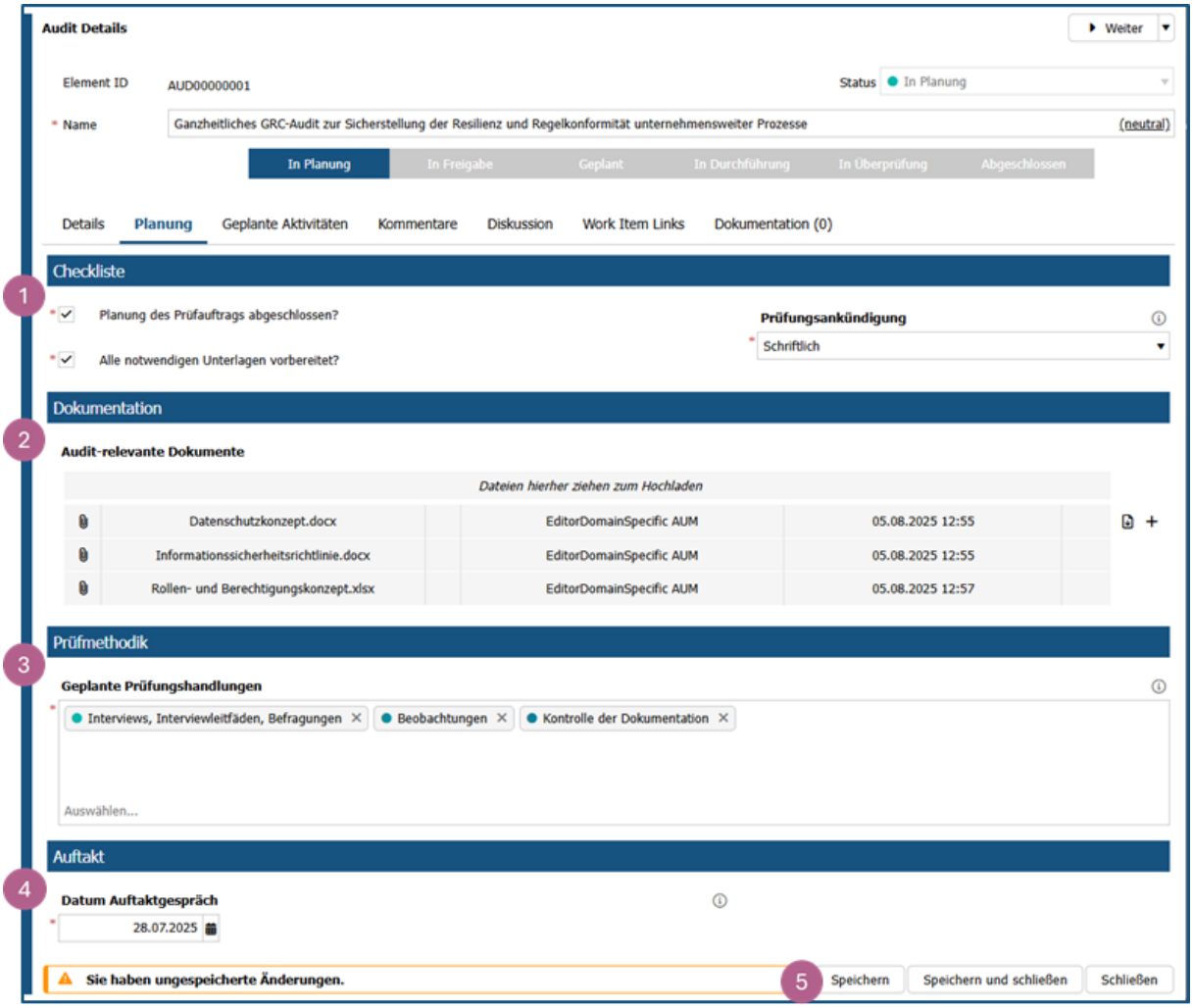
12 **Audit Beschreibung**: Schlussendlich muss der Bearbeiter das Audit in Worten beschreiben. Dabei können noch wichtige Informationen hinterlegt werden die zu keiner Angabe zuvor passend gewesen wäre.

13 **Audit Nicht-Ziele**: Neben dem Scope kann der Bearbeiter auch dezidiert festlegen was nicht im Rahmen des Audits behandelt werden soll.

14 **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Maßnahme* gespeichert werden.

> Nachdem alle Details hinterlegt wurden kann in den Tab "*Planung*" gewechselt und mit Schritt 4 fortgefahren werden.

Schritt 4: Planung hinterlegen



1 **Checkliste**: Mittels der Checkliste gibt der Bearbeiter offiziell an, ob die Planung abgeschlossen ist und alle notwendigen Unterlagen vorbereitet und hinterlegt worden sind.

Zusätzlich hat der Bearbeiter die Angabe zu machen, ob und in welcher Form die "Prüfungsankündigung" vorgenommen worden ist.

2 **Audit-relevante Dokumente**: Um die Frage der Checkliste, ob alle Unterlagen vorbereitet wurden, zu untermauern kann der Bearbeiter relante Dokumente hinterlegen, die im Rahmen des *Audits* herangezogen werden sollen.

> Dabei kann es sich um intere Checklisten, Memos zu dem Auftaktgespräch, Links zum internen Sharepoint oder andere relevante Dokumente, Memos oder Links handeln.

> Handelt es sich um eine Datei, kann diese z.B. vom Desktop in den Bereich "Datei hierher ziehen zum Hochladen" gezogen werden. Die Datei wird anschließend im Attributsfeld verlinkt.

3 **Geplante Prüfungshandlungen**: Im Rahmen der "Geplanten Prüfungshandlungen" gibt der Bearbeiter an, welche Handlungen er im Audit setzen möchte.

> Bei den meisten *Audits* wird mindestens ein Interview geführt bzw. werden bei *Audits* im Finanzbereich des öfteren "Kontrolle von Dokumenten" vorgenommen.

4 **Auftaktgespräch**: Neben der Angabe in welcher Form die Prüfungsankündigung vorgenommen wurde muss auch ein Datum angegeben werden, zu dem das offizielle "Auftaktgespräch" geführt worden ist.

5 **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen, kann das *Audit* erstmalig gespeichert werden

> Nachdem alle Details hinterlegt wurden kann in den Tab "*Geplante Aktivitäten*" gewechselt und mit Schritt 5 fortgefahren werden.

Schritt 5: Auditaktivitäten planen

Der Bearbeiter kann *Auditakivitäten* planen die später im Zeitraum des *Audits* durchgeführt werden. Dabei erstellt der Bearbeiter *Auditaktivitäten* mittels des Icons +. Mehr Informationen zu der Erstellung unter Bearbeiter Audit - Auditaktivität definieren & planen.

> Es können keine Auditaktivitäten verlinkt, sondern nur neue erstellt werden.

Schritt 6: Statuswechsel vornehmen

Sollten alle Angaben gemacht worden sein und passen kann der Bearbeiter einen Statusübergang zu "Freigabe" durchführen.

> Der Freigeber Audit wird über den Statusübergang mittels Notifikation informiert.

> Damit der Bearbeiter in den Status "Freigabe" schalten kann muss er davor alle geplanten Auditaktivitäten in den Status "Geplant" schalten.

2.16.2 Auditaktivität definieren & planen

Nach der Erstellung eines *Audits* können passende *Auditaktivitäten* geplant und im Rahmen des *Audits* durchgeführt werden.

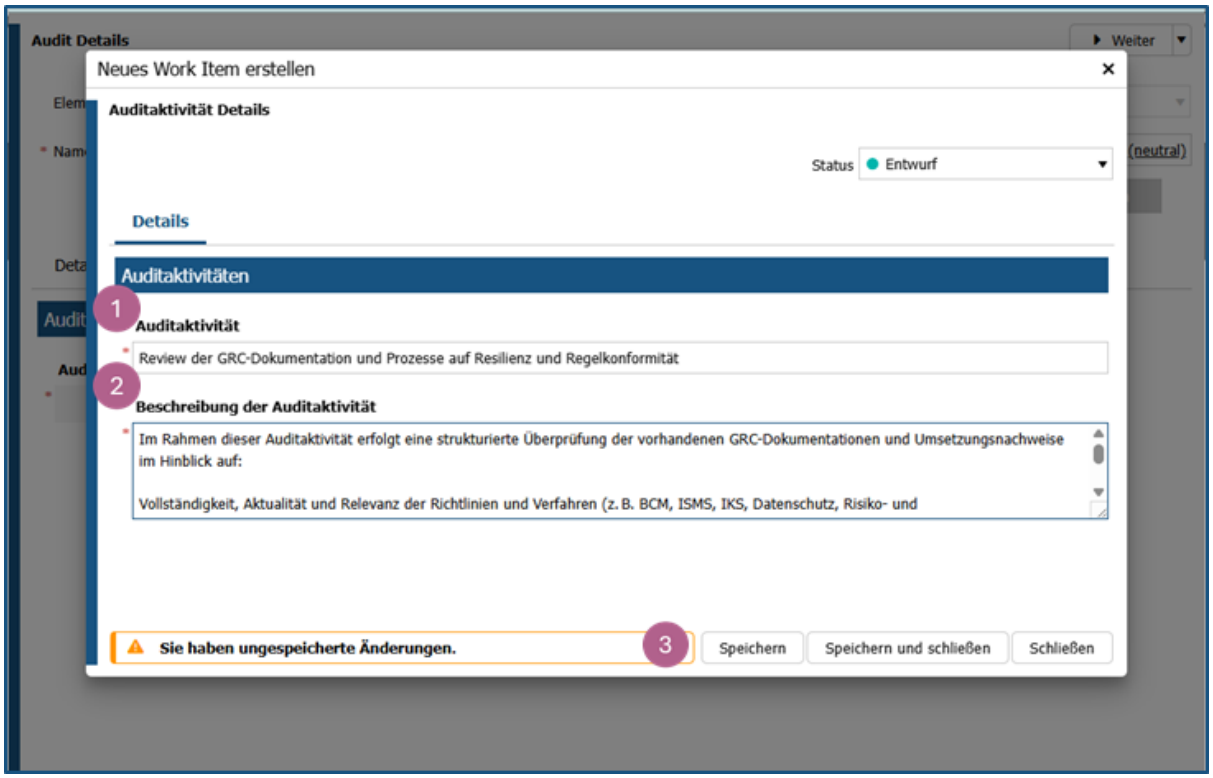
Schritt 1: Auditaktivität erstellen

Die *Auditaktivität* kann nur mittels Erstellung aus dem Work Item *Audit* durch den verantwortlichen Bearbeiter erfolgen.

Für die Erstellung wird im Work Item *Audit* im Tab "*Auditaktivitäten*" durch das Icon + eine neue *Auditaktivität* erstellt.

> Die *Auditaktivität* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des *Audits*.

Schritt 2: Auditaktivität definieren



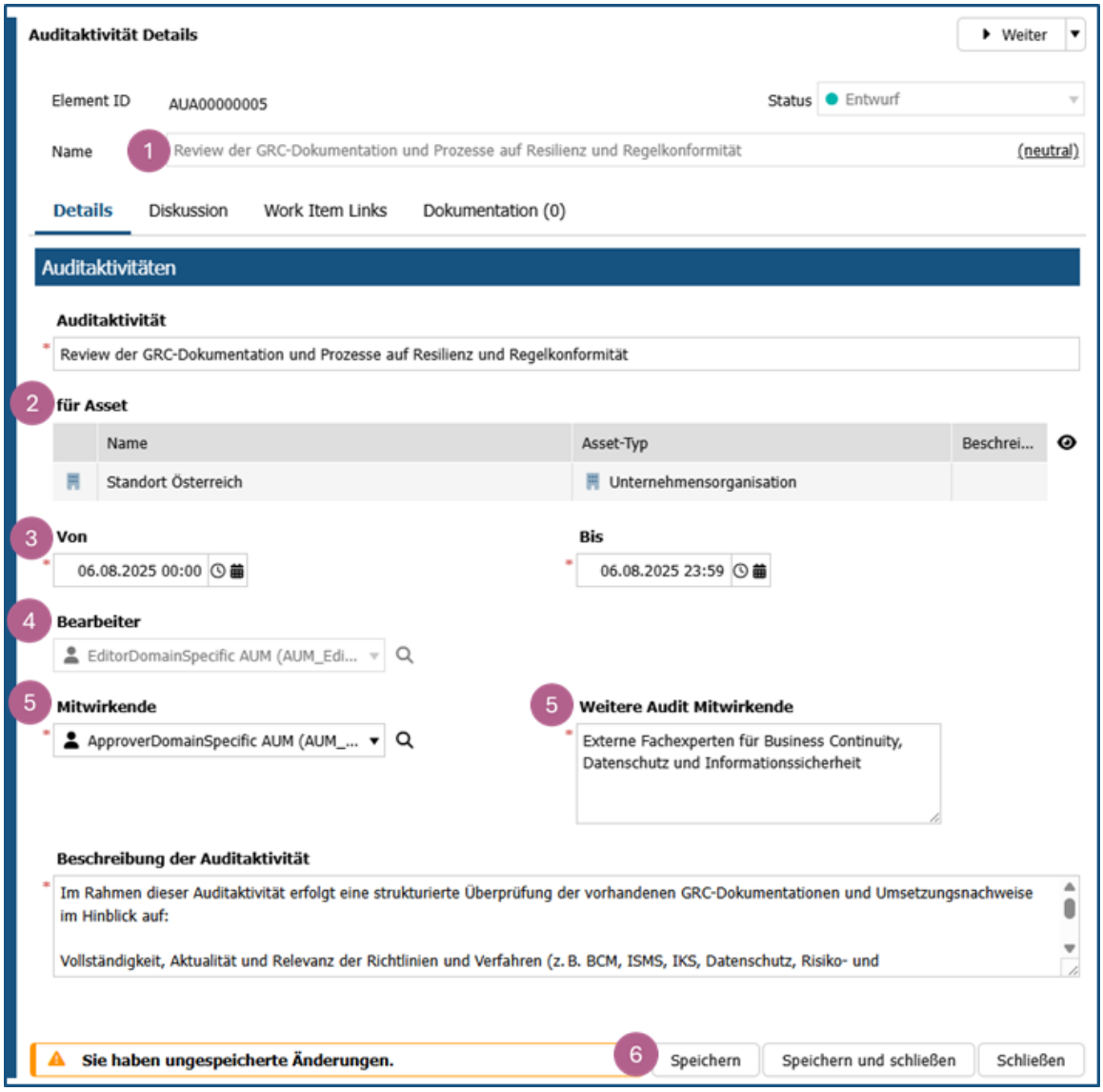
1. **Auditaktivität**: Der Bearbeiter muss manuell einen Namen für die *Auditaktivität* eingeben.
2. **Beschreibung der Auditaktivität**: Es kann vom Bearbeiter eine genaue Beschreibung angegeben werden, was während der *Auditaktivität* zu tun ist.

> Sollte der Bearbeiter die Auswahl "Wiederkehrende Auditaktivität" und einen GRC Framework Link hinterlegt haben wird die Beschreibung beim Statusübergang

> vom GRC Framework übernommen, wenn dort eine vom Management gepflegt wird.

3 **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Auditaktivität* erstmalig gespeichert werden.

Schritt 3: Weiteres Vorgehen



1 **Name**: Nachdem die *Auditaktivität* zum ersten Mal gespeichert wurde wird der Name automatisch gesetzt.

> Der Name ergibt sich aus der Eingabe des hinterlegten Textes bei "Auditaktivität".

2 **Asset**: Das Asset wird vom *Audit* automatisch beim Speichern übernommen.

> Das Asset kann nicht verändert werden und ist Read Only.

3. **Zeitraum**: Auch der Zeitraum wird beim Speichervorgang vom *Audit* übernommen. Der Bearbeiter kann den Zeitraum allerdings manuell anpassen, um die *Auditaktivität* und deren Umfang besser zeitlich zu konkretisieren.

   > Falls der Bearbeiter einen Zeitraum angibt der Zeitlich nicht in das *Audit* passt wird er darauf hingewiesen.

4. **Verantwortlich**: Der Bearbeiter wird automatisch in das Attribut "Bearbeiter" übertragen und kann nicht mehr geändert werden.
5. **Mitwirkende**: Der Bearbeiter kann in der *Auditaktivität* - wie auch schon im *Audit* - "Mitwirkende" zuteilen.
6. **Speichervorgang**: Nach der Hinterlegung der notwendigen Informationen kann die *Auditaktivität* gespeichert werden

   > Nach Eingabe aller notwendigen Informationen kann das Work Item gespeichert und ein Statusübergang durchgeführt werden, bevor das Fenster geschlossen wird.

> Sollte die *Auditaktivität* entlinkt werden, wird direkt sie aus dem gesamten System gelöscht und verbleibt nicht als Waise im System.

> Wenn das *Audit* in den Status "Obsolet" geschalten wird, wird auch die *Auditaktivität* in "Obsolet" gesetzt.

> Zurück zu dem Schritt Bearbeiter Audit - Audit definieren & erstellen Schritt 5.

2.16.3 Audit starten & durchführen

Der Bearbeiter wird im Rahmen eines Schedulers mittels einer Notifikation erinnert, dass das *Audit* durchzuführen ist. Dabei bezieht sich die Erinnerung auf das hinterlegte Datum, wann das *Audit* beginnen wird.

Schritt 1: Navigation zu Audit

Der Bearbeiter Audit hat zwei Möglichkeiten ein durchzuführendes *Audit* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter Audit bekommt eine E-Mail zugesendet, sobald das Datum wann das *Audit* durchgeführt werden soll erreicht ist. Der Link zu dem spezifischen *Audit*befindet sich in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo´s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Bearbeiter noch eine Bearbeitung durchzuführen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Audit* automatisch.

Schritt 2: Auditaktivitäten durchführen

Der Bearbeiter Audit sollte in den Tab "*Auditaktivitäten*" wechseln. Dort findet er alle von ihm geplanten *Auditaktivitäten*.

> Sollten die bisher geplanten *Auditaktivitäten* nicht ausreichen kann der Bearbeiter bei Bedarf noch weitere ergänzen.

Weitere Schritte zu der Durchführung der *Auditaktivtäten* findet der Bearbeiter unter Auditaktivität starten & durchführen.

> Anschließend sollte der Bearbeiter in diesem Abschnitt mit Schritt 3 fortfahren.

Schritt 3: Auditaktivitäten abschließen

Nachdem alle *Auditaktivitäten* durchgeführt worden sind soll der Bearbeiter das gesamte *Audit* final bewerten. Mehr Informationen zu dem Schritt unter Audit bewerten & abschließen.

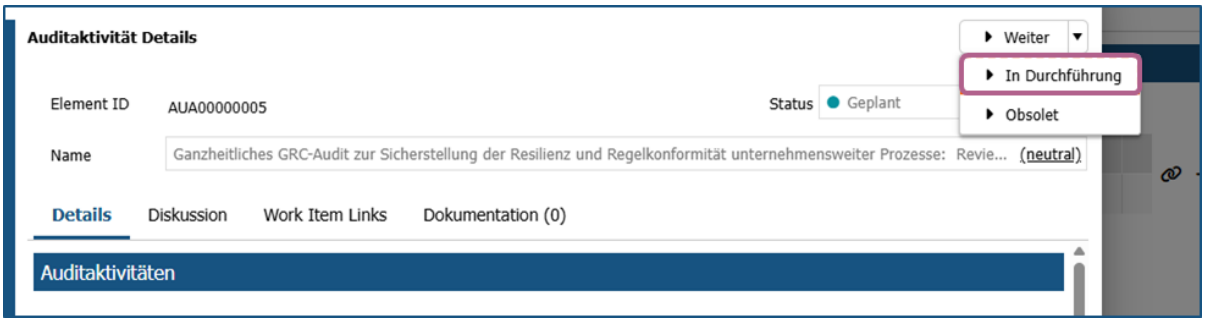
> Damit der Bearbeiter in den Status "Überprüfung" schalten kann müssen alle *Auditaktivitäten* im Status "Abgeschlossen" sein.

2.16.4 Auditaktivität starten & durchführen

Nachdem ein *Audit* gestartet wurde kann vom Bearbeiter Audit auch mit der Durchführung der *Auditaktivitäten* gestartet werden.

Schritt 1: Auditaktivität öffnen

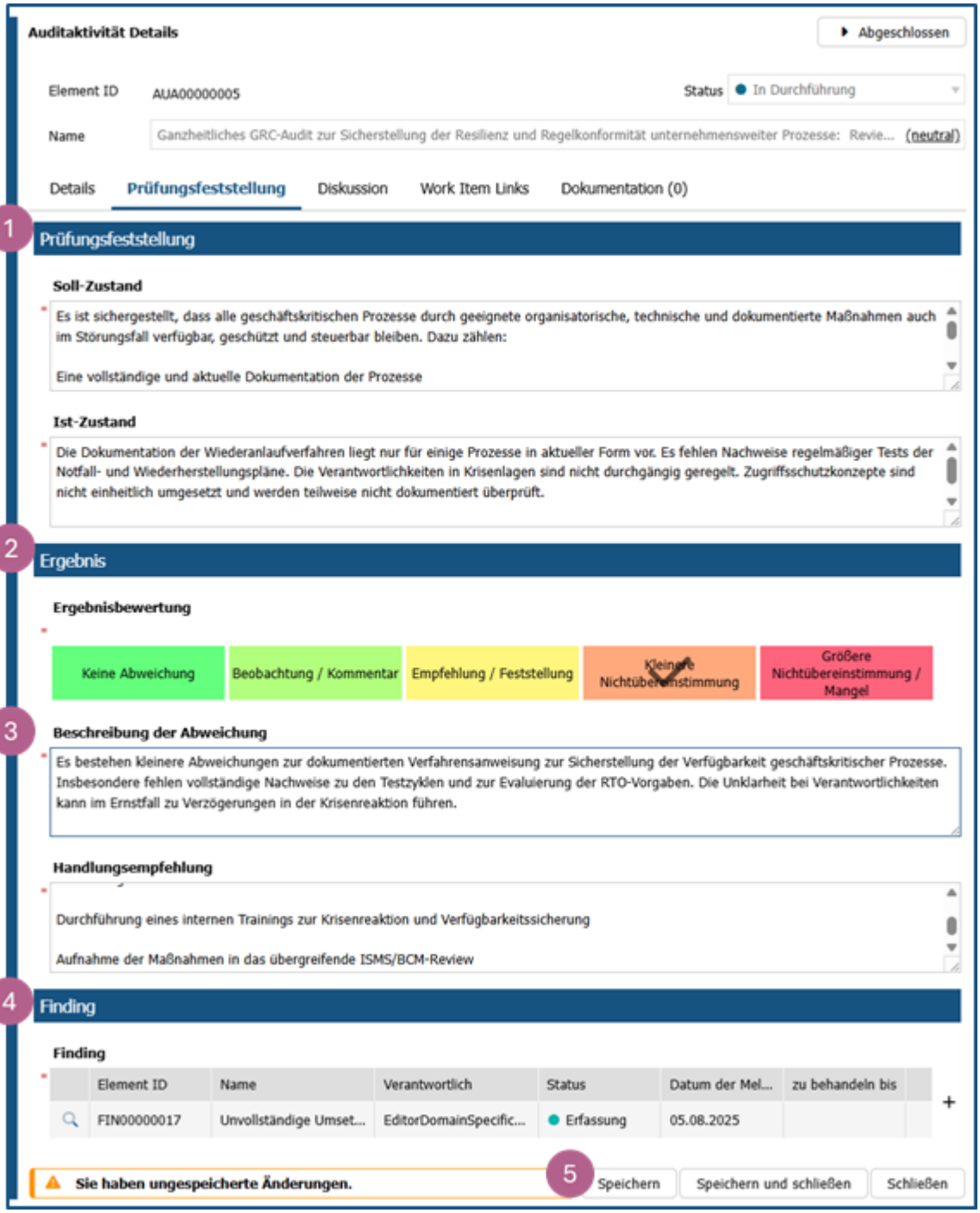
Die *Auditaktivität* sollte über das Work Item *Audit* geöffnet werden. Dabei kann der Bearbeiter die jeweilige *Auditaktivität* mittels Doppelklick auf eine *Auditaktivität* in der Liste öffnen.



Die *Auditaktivität* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des *Audits*.

Der Bearbeiter sollte in den Status "Durchführung" in der rechten oberen Fensterecke und in den Tab "*Prüfungsfeststellung*" wechseln.

Schritt 2: Auditaktivität durchführen



1. **Prüffeststellung**: Der Bearbeiter hat als ersten Schritt zu dokumentieren was der gewollte "Soll-Zustand" ist, bevor er den tatsächlichen "Ist-Zustand" beschreibt.
2. **Ergebnisbewertung**: Nachdem es einen Überblick über den möglichen Gap zwischen Soll- und Ist-Zustand" gibt muss vom Bearbeiter eingeschätzt werden, wie sein Ergebnis ausfallen wird.

> Dabei gibt es im besten Fall "Keine Abweichung" zwischen den Soll- und Ist-Zustand und im schlechtesten Fall einen "Größeren Mangel".

> Sollte das Ergebnis eine kleinere oder größere Nichtübereinstimmung sein muss der Bearbeiter verpflichtend ein *Finding* angeben.

3. **Beschreibung der Abweichung & Handlungsempfehlung**: Neben einer Ergebnisbewertung hat der Bearbeiter auch eine schriftliche Stellungnahme abzugeben. So kann er im Textfeld "Beschreibung der Abweichung" angeben zu welchen Abweichungen es seiner Meinung nach gekommen ist und kann zugleich "Handlungsempfehlungen" abgeben, um diesen Umstand zu verbessern.

> Sollte es eine Abweichung geben - unabhängig von der Klassifizierung - muss eine Angabe in den beiden Textfeldern hinterlegt werden.

4. **Finding**: Durch die Erstellung eines *Findings* kann genauer bestimmt werden, was dem Bearbeiter im Rahmen der *Auditaktivität* aufgefallen ist. Mehr Informationen unter Bearbeiter Audit - Finding identifizieren & erstellen.
5. **Speichern**: Sobald alle Informationen eingetragen wurden kann die *Auditaktivität* gespeichert werden.

Schritt 3: Auditaktivität abschließen

Sobald alle Eingaben gemacht bzw. *Findings* erstellt wurden kann die *Auditaktivtät* in den Status "Abgeschlossen" geschalten werden.

> Zurück zu dem Schritt Bearbeiter Audit - Audit starten & durchführen Schritt 5.

2.16.5 Finding identifizieren & erstellen

Sollte der Bearbeiter Audit während der Durchführung einer *Auditaktivität* zu der Erkenntnis kommen, dass es Verbesserungspotenzial bzw. Abweichungen gibt muss der Bearbeiter Audit ein *Finding* erstellen.

Schritt 1: Finding aus Auditaktivität erstellen

Ein *Finding* kann aus einer *Auditaktivität* entstehen.

Die Erstellung erfolgt durch das Icon ✚nach einer schriftlichen Stellungnahme unter "Getroffene Entscheidungen".

Schritt 2: Finding dokumentieren

1. **Name**: Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Finding* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Finding* einzigartig.

2. **GRC- Perspektive**: Die Perspektive wird nicht automatisch aus der *Auditaktivität* übernommen, sondern der Bearbeiter kann jene Perspektiven auswählen, die im Rahmen der *Auditaktivität* betrachtet worden ist.
3. **Bearbeiter**: In das Attribut soll jener Bearbeiter eingetragen werden der für das *Finding* der *Auditaktivität* eine Behandlung durchzuführen hat.

> Damit auf einen Blick erkennbar ist, von wem das *Finding* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

> Mehr Informationen über die Behandlungen von *Findings* unter Bearbeiter Audit - Finding verwalten & behandeln.

4. **Datum der Meldung**: Der Ersteller muss angeben, wann er das *Finding* offiziell gemeldet/entdeckt hat. Daher muss das Datum nicht mit dem tagesaktuellen Datum übereinstimmen.
5. **zu behandeln bis**: Unter dem Datum wird jenes Datum verstanden, bis zu dem das *Finding* behoben werden sollte. Es soll einen Hilfestellung sein, um eine Orientierung für im Workflow nachgelagerte Benutzer zu geben, bis wann die Behebung des *Findings* wünschenswert wäre.
6. **Art des Findings**: Der Ersteller kann im Rahmen von fünf Stufen einordnen, wie bedenklich das *Finding* im Kontext der *Auditaktivität* ist.
7. **Finding für dieses Asset**: Das Asset wird nicht automatisch aus dem Work Item übernommen sondern muss manuell eingetragen werden.

> Sollten dem Benutzer keine "Assets" angezeigt werden, dann ist dem Benutzer keine Rolle auf dem Asset zugewiesen, das er verlinken möchte. Mittels des Work Items *Berechtigungsanfrage* kann der Benutzer um die passende Berechtigung am Asset bitten. Mehr Informationen unter Standard User - Berechtigungsanfrage definieren & erstellen.

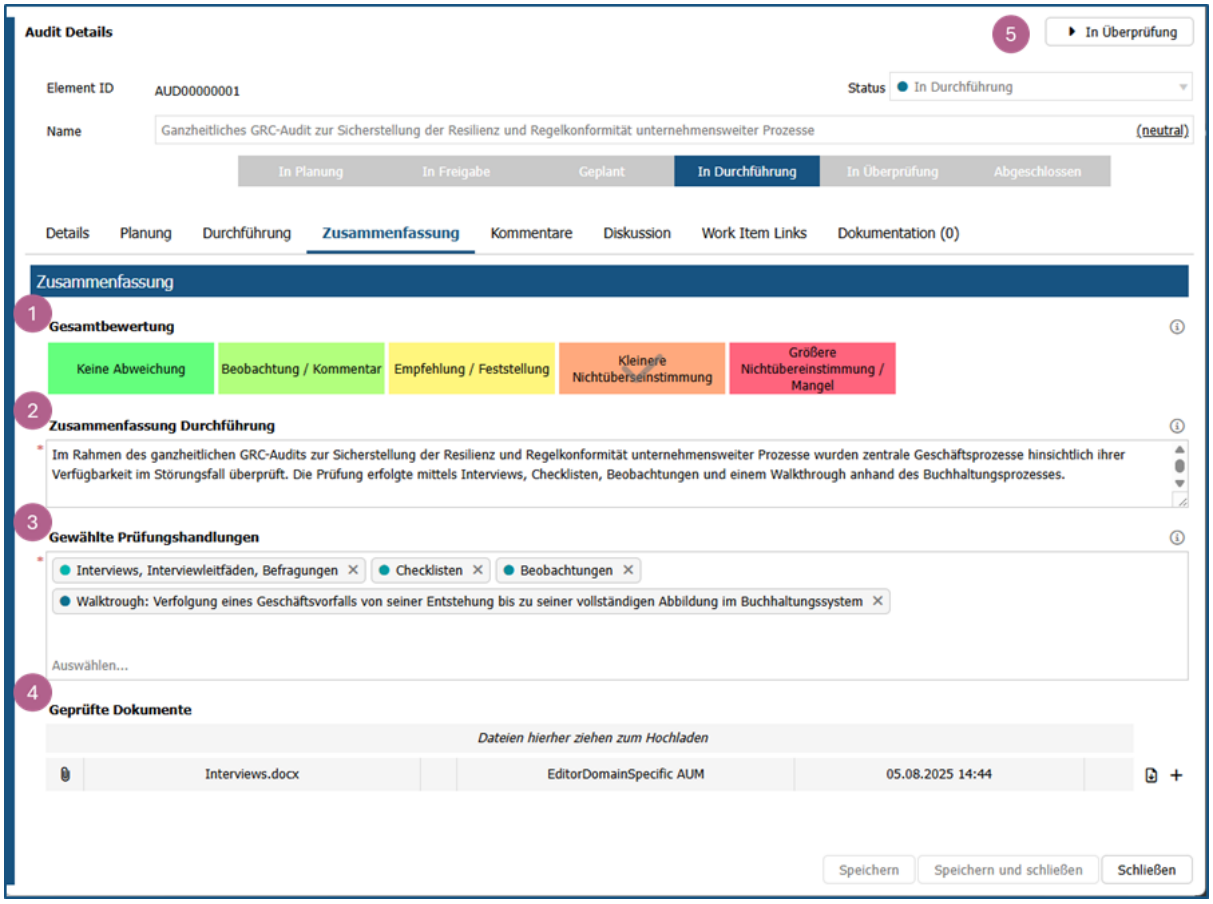
8. **Beschreibung des Findings**: Die "Beschreibung des Findings" soll so viele Informationen und Inputs wie möglich enthalten, beispielsweise wie das *Finding* entdeckt wurde. Weiters kann möglicherweise Rückschlüsse auf Ursache und Wirkung entstehen.
9. **Priorität des Findings**: Dem *Finding* kann eine Priorität hinterlegt werden, die später für Auswertungen auf beispielsweise Dashboads verwendet werden kann.
10. **Statuswechsel**: Der Ersteller kann abschließend in den Status "Behandlung" schalten. Mehr Informationen zu dem Statuswechsel in Finding sichten & behandeln.

> Anschließend kann der Bearbeiter Management Review in die *Auditaktivität* zurückkehren und dort mit der Arbeit fortfahren. Bearbeiter Audit - Auditaktivität starten & durchführen.

2.16.6 Audit bewerten & abschließen

Die Bewertung des gesamten *Audits* erfolgt im Tab "*Zusammenfassung*".

Schritt 1: Audit bewerten



1 **Gesamtbewertung**: Nachdem der Bearbeiter Audit noch einmal alle *Auditaktivitäten* und deren Ergebnisse gesichtet hat kann er eine "Gesamtbewertung" des *Audits* angeben.

> Das Ergebnis der "Gesamtbewertung" gilt für das *gesamte* Audit und nicht nur für Teile des *Audits*.

> Sollte die "Gesamtbewertung" mit dem Ergebnis kleinere oder größere Nichtübereinstimmung abschließen wird der Manager des Moduls Audit mittels Notifikation über das kritische Ergebnis informiert.

2 **Zusammenfassung Durchführung**: Der Bearbeiter hat in diesem Textfeld anzugeben wie der gesamte Eindruck des Audits, die Durchführung und möglichen Herausforderungen gemanagt worden sind.

3 **Gewählte Prüfungshandlungen**: Die schlussendlich herangezogenen Prüfungshandlungen können oft von der Planung abweichen. Daher hat der Bearbeiter anzugeben, welche Prüfungshandlungen für das Audit vorgenommen worden sind.

Die "Geplanten Prüfungshandlungen" werden als Vorschlag automatisch übernommen, können allerdings überarbeitet werden.

4 **Geprüfte Dokumente**: Der Bearbeiter hat zu hinterlegen, welche Dokumente final für das Audit herangezogen worden sind

5 **Statuswechsel**: Der Bearbeiter kann abschließend in den Status "Abgeschlossen" schalten.

Nachdem ein *Audit* geschlossen wurde kann es nicht mehr geöffnet werden.

2.17 Freigeber Audit

Ein Freigeber Audit in BIC GRC ist für die abschließende Prüfung und formale Freigabe eines *Audits* verantwortlich. Er stellt sicher, dass alle *Auditaktivitäten* ordnungsgemäß durchgeführt und dokumentiert wurden und dass die *Findings* nachvollziehbar und regelkonform sind.

Folgende Aufgabe hat der Freigeber Audit in BIC GRC:

- Audit überprüfen & freigeben

2.17.1 Audit überprüfen & freigeben

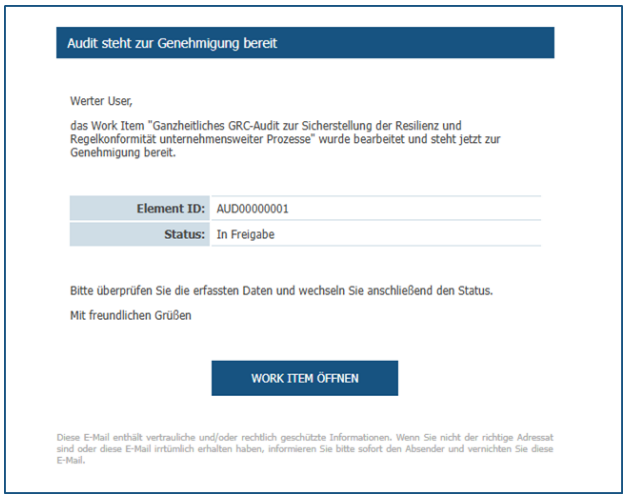
Der Freigeber Audit wird nach der Erstellung eines *Audits* des Bearbeiter Audit mittels Notifikation informiert.

Schritt 1: Navigation zu Audit

Der Freigeber Audit hat zwei Möglichkeiten ein *Audit* zu öffnen.

1. Öffnen über Notifikation

Der Freigeber Audit bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald ein *Audit* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu dem spezifischen *Audit* befindet sich in der Notifikation.



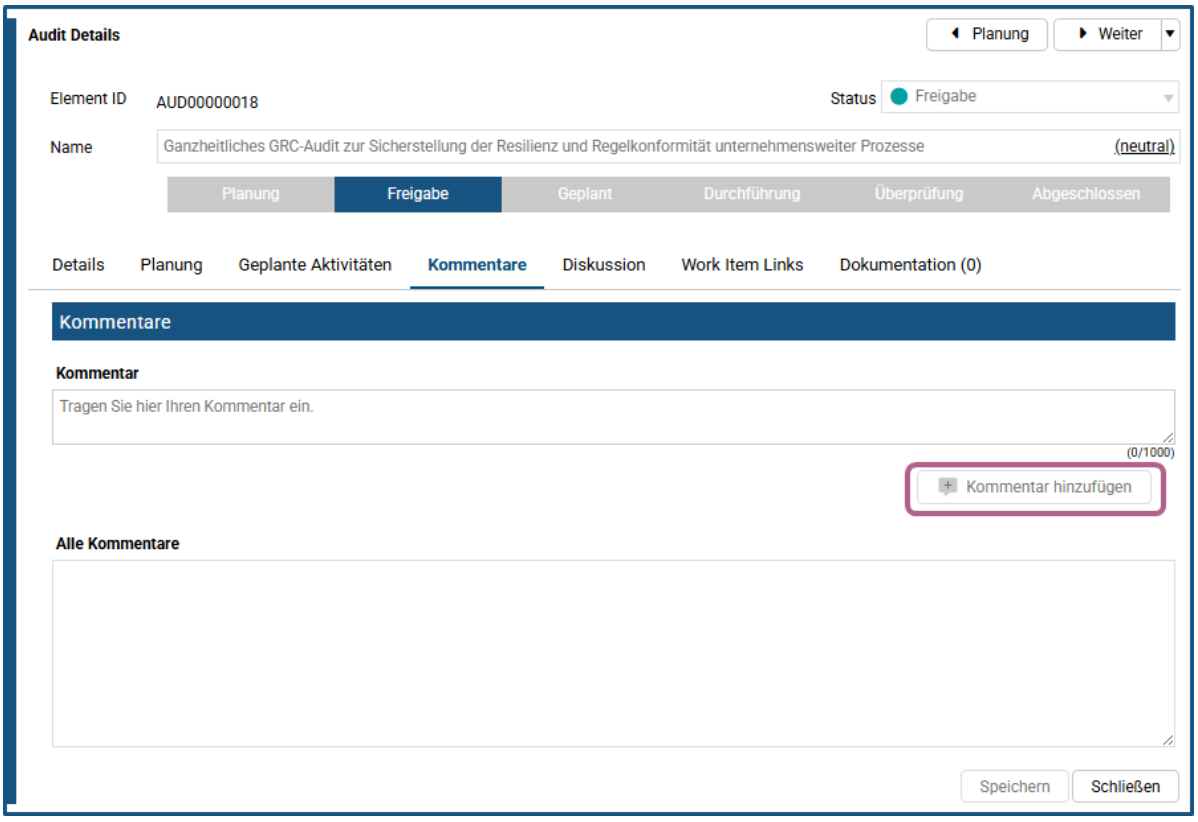
2. Öffnen über Dashboard "Meine aktuellen ToDo´s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber noch eine Freigabe durchzuführen hat.

Schritt 2: Audit überprüfen

Der Freigeber Audit hat in dem geplanten *Audit* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob das *Audit* richtig geplant und der Aufwand des Audits richtig eingeschätzt wurde.

Sollte dies nicht der Fall sein und muss das *Audit* aus Sicht des Freigeber Audit erneut geplant werden, kann der Freigeber Audit einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "Planung" durchführen.



Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzers passen kann der Freigeber Audit weiter in den Status "Geplant" schalten. Der verantwortliche Bearbeiter DS wird mittels Notifikation über den Statuswechsel benachrichtigt.

> Der Status "Geplant" ist ein ruhender Status bis das *Audit* tatsächlich gestartet wird.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.18 Manager

Benutzer mit dem Benutzerprofil 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 Rollen.

Folgende Aufgaben hat das Management in BIC GRC:

- Nachhaltigkeitsrisiko überprüfen & freigeben
- Management Review sichten & freigeben

2.18.1 Nachhaltigkeitsrisiko freigeben

Ein *Nachhaltigkeitsrisiko* wird vom Bearbeiter Risiko erstellt und bewertet, bevor es von unterschiedlichen Instanzen freigegeben wird. Wenn das *Nachhaltigkeitsrisiko* einen besonders hohen Risikowert ausgibt, kann der Manager darüber informiert werden, indem dieses spezifische *Nachhaltigkeitsrisiko* in den Status "Managementfreigabe" geschalten wird.

> Diese Option muss in der "Solution Configuration" freigeschalten werden.

Schritt 1: Navigation zu spezifischem Nachhaltigkeitsrisiko

Der Manager hat zwei Möglichkeiten ein *Nachhaltigkeitsrisiko* zu öffnen.

1. Öffnen über Notifikation

Der Manager bekommt eine E-Mail zugesendet, sobald der Freigeber Risiko den Status des *Nachhaltigkeitsrisikos* zu "Managementfreigabe" wechselt. Der Link zu dem spezifischen *Nachhaltigkeitsrisiko* befindet sich anschließend in der Notifikation.

2. Öffnen über Dashboard "Meine aktuellen ToDo`s"

Im oberen Teil des Dashboards "Meine aktuellen ToDo`s" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigt. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Manager eine Freigabe durchzuführen hat.

> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Nachhaltigkeitsrisiko* automatisch.

Schritt 2: Freigabe durchführen

Der Manager hat in dem erstellten und bewerteten *Nachhaltigkeitsrisiko* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob das *Nachhaltigkeitsrisiko* in einem ausreichenden Ausmaß mitigiert wurde und das Restrisiko für das Unternehmen in seinem Umfang getragen werden kann.

Sollte dies nicht der Fall sein und muss das *Nachhaltigkeitsrisiko* aus Sicht des Managers erneut bewertet werden kann der Manager einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status in "Bruttobewertung" oder in "Nettobewertung" durchführen.

Sollten die Eingaben weitgehend akzeptabel sein kann der Manager direkt in den Status "Aktiv" schalten. Mit dem Statuswechsel ist das *Nachhaltigkeitsrisiko* als abgeschlossen im Risikoinventar aufgenommen.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.18.2 Management Review sichten & freigeben

Ein *Management Review* wird vom Bearbeiter DS erstellt und geplant. Sobald die Durchführung abgeschlossen und überprüft wurde, kann ein *Management Review* dem Manager für die finale Freigabe weitergegeben werden mittels Statusübergang in "Managementfreigabe".

Schritt 1: Navigation zu spezifischen Management Review

Der Manager bekommt eine E-Mail zugesendet, sobald der Bearbeiter DS alle Eingaben im Status "Überprüfung" abgeschlossen hat. Der Link zu dem spezifischen *Management Review* befindet sich in der Notifikation.

Schritt 2: Überprüfung durchführen

Der Manager hat in dem bewerteten *Management Review* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob der *Management Review* in Bezug auf die Bewertung richtig eingeordnet worden ist.

Sollte dies nicht der Fall sein und muss der *Management Review* aus Sicht des Freigebers Risiko erneut bewertet werden, kann der Manager einen Kommentar im Tab "*Kommentar*" hinterlassen und einen Statuswechsel in den Status "Überprüfung" durchführen.

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzers passen kann der Manager weiter in den Status "Abgeschlossen" schalten.

> Der Bearbeiter DS wird über den Statuswechsel in "Abgeschlossen" mittels Notifikation benachrichtigt.

Management Review
MRE00000001

Name		Status
Integrierte Managementbewertung – Standort Deutschland		Abgeschlossen

Planung

Bearbeiter		Datum Management Review
EditorDomainSpecific		08.08.2025

Anwendungsbereich

Standort Deutschland	DE	Unternehmensorganisation

Zweck und Ziele

Ziel dieser Management Review ist es, die Wirksamkeit und Effizienz der implementierten Managementsysteme und Kontrollmechanismen im Standort Deutschland ganzheitlich zu bewerten.

GRC Perspektiven

Enterprise Risk Management, Corporate Sustainability, Information Security Management, Business Continuity Management, Privacy Management, Internal Control

Teilnehmer

ERM EditorDomainSpecific, BCM EditorDomainSpecific, DPM EditorDomainSpecific, ICS EditorDomainSpecific, CSM EditorDomainSpecific, ISM EditorDomainSpecific, AUM EditorDomainSpecific

2.19 Spezielle Benutzerprofile

Neben den standardisierten und fachlichen Benutzerprofilen gibt es ergänzend noch "Spezielle Benutzerprofile". Diese Benutzerprofile haben eine spezifische Aufgabe in BIC GRC.

> "Spezielle Benutzerprofile" können bestimmten Benutzern ergänzend zu deren eigentlichen Benutzerprofilen zugewiesen werden.

Interner Anfrageempfänger:

- Interne Anfrage beantworten & bearbeiten

Berechtigungsanfrageempfänger:

- Berechtigungsanfrage beantworten & bearbeiten

2.19.1 Interne Anfrage beantworten & bearbeiten

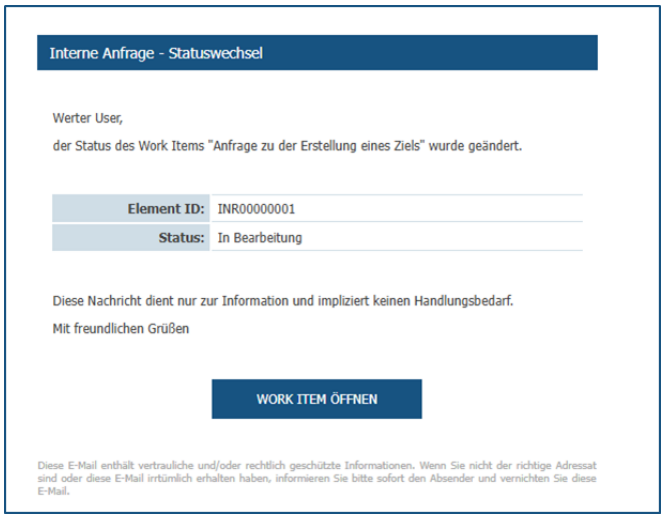
Nachdem ein Standard Benutzer eine *Interne Anfrage* gestellt hat muss ein Benutzer - der ein Mitglied der Gruppe "Internal Request Receiver" ist - diese beantworten.

Schritt 1: Navigation zur Internen Anfrage

Der Empfänger hat zwei Möglichkeiten eine *Internen Anfrage* zu öffnen.

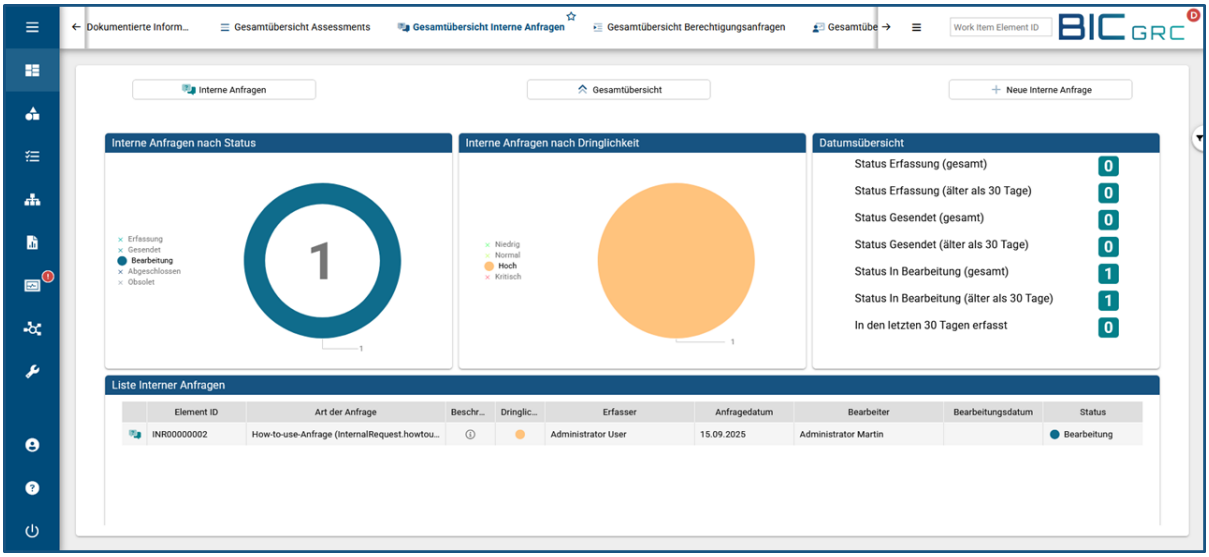
1. Öffnen über Notifikation

Der Empfänger bekommt eine E-Mail zugesendet sobald der Ersteller der *Internen Anfrage* den Status zu "Gesendet" wechselt. Der Link zu der spezifischen *Internen Anfrage* befindet sich in der Notifikation.



2. Öffnen über Dashboard "Internen Anfrage"

Der Empfänger kann in dem Dashboard nach seinen *Internen Anfrage* filtern.

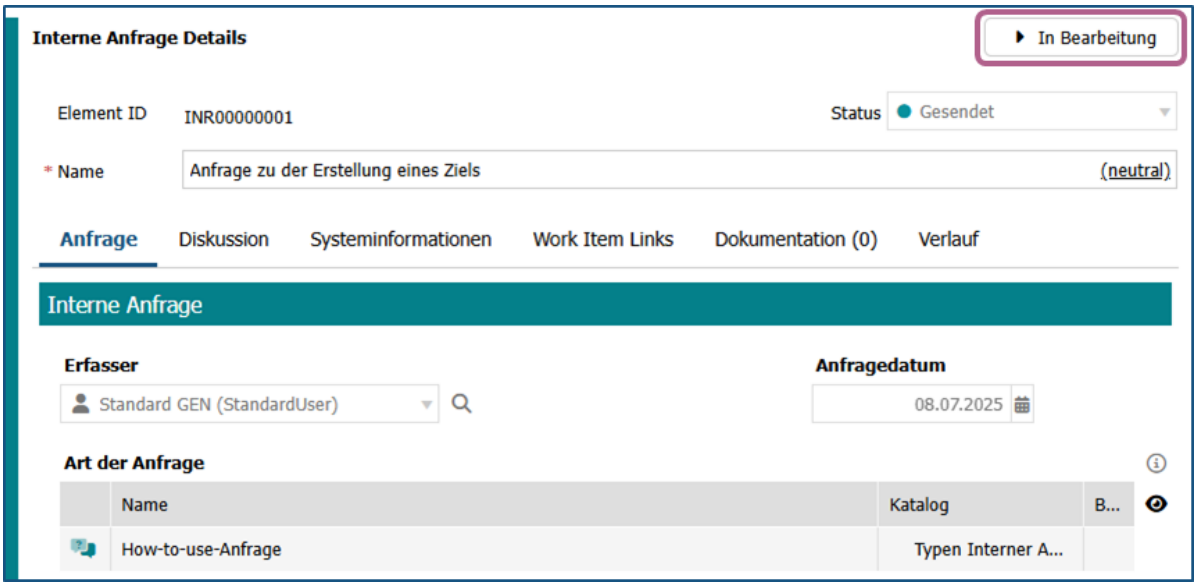


> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich automatisch ein neues Fenster für die *Interne Anfrage*.

Schritt 2: Interne Anfrage sichten

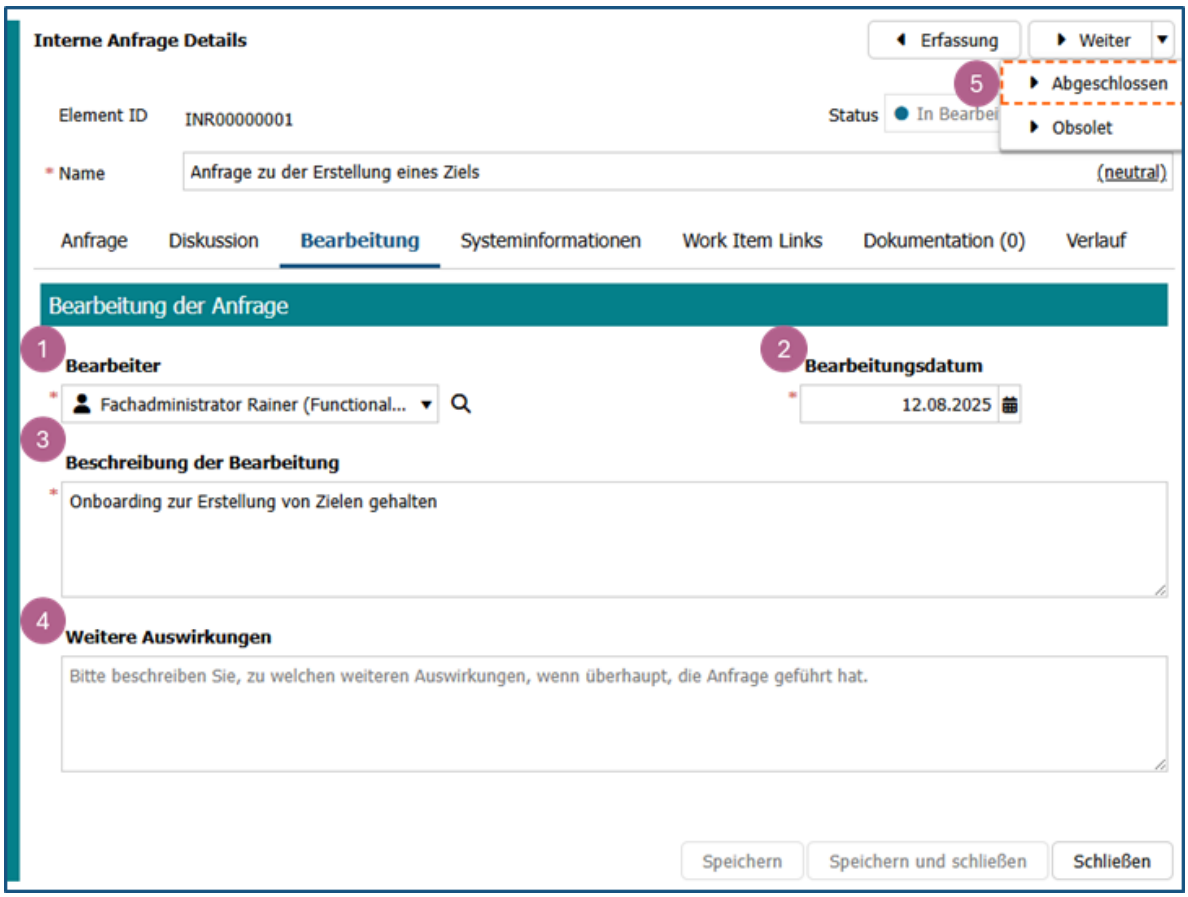
Als erstes sollte der Empfänger einen Statusübergang von "Gesendet" in "Bearbeitung" vornehmen. Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.

Der Empfänger hat in der erstellten *Internen Anfrage* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, wie er mit der *Internen Anfrage* verfahren möchte. Dafür sollte er die Eingaben im Tab "*Anfrage*" sichten bevor er eine Diskussion im Tab "*Diskussion*" startet. Das "*Diskussions*"- Tab soll den Empfänger dabei unterstützen sowohl den richtigen Ansprechpartner für die Diskussion zu finden, als auch um alle Informationen einzuholen, die er notwendigerweise für die Beantwortung der *Internen Anfrage* braucht.



Sollte der Empfänger gleich der Bearbeiter sein kann er in den Tab "*Bearbeitung*" wechseln und mit der Beantwortung der Anfrage beginnen. Sollte er nicht der passende Bearbeiter sein kann der Empfänger im Status "Bearbeitung" einen passenden Bearbeiter auswählen. Dieser wird mittels Notifikation über die Nominierung informiert.

Schritt 3: Interne Anfrage bearbeiten



1. **Bearbeiter**: Der Bearbeiter wird automatisch gesetzt mit dem Benutzer, der vom Ersteller als "Empfänger" eingetragen wurde.
2. **Bearbeitungsdatum**: Der Bearbeiter hat ein Datum anzugeben an dem er die *Interne Anfrage* bearbeitet hat.
3. **Beschreibung der Bearbeitung**: Anschließend hat der Bearbeiter zu beschreiben, wie er die *Interne Anfrage* behandelt und bearbeitet hat.
4. **Weitere Auswirkungen**: Weiters kann eine Angabe gemacht werden zu welchen Folgen die *Interne Anfrage* geführt hat.
5. **Statuswechsel**: Sobald die Informationen angegeben sind kann der Benutzer speichern und einen Statuswechsel zu in "Abgeschlossen" durchführen.

> Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

2.19.2 Berechtigungsanfrage beantworten & bearbeiten

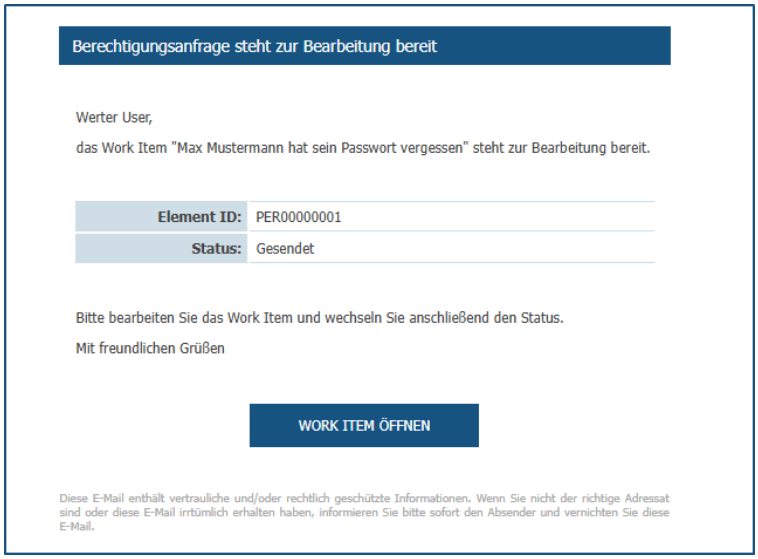
Nachdem ein Standard Benutzer eine *Berechtigungsanfrage* gestellt hat muss ein Benutzer - der ein Mitglied der Gruppe "Permission Request Receiver" ist - diese beantworten.

Schritt 1: Navigation zur Berechtigungsanfrage

Der Empfänger hat zwei Möglichkeiten eine *Berechtigungsanfrage* zu öffnen.

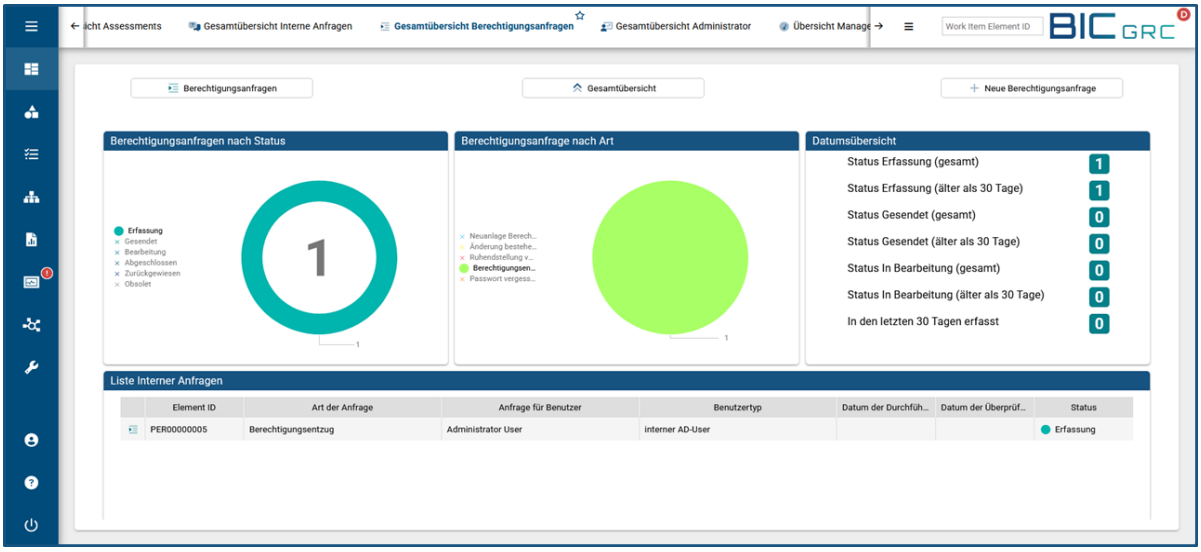
1. Öffnen über Notifikation

Der Empfänger bekommt eine E-Mail zugesendet sobald der Ersteller der *Berechtigungsanfrage* den Status zu "Gesendet" wechselt. Der Link zu der spezifischen *Berechtigungsanfrage* befindet sich in der Notifikation.



2. Öffnen über Dashboard "Internen Anfrage"

Der Empfänger kann in dem Dashboard nach seinen *Berechtigungsanfrage* filtern.



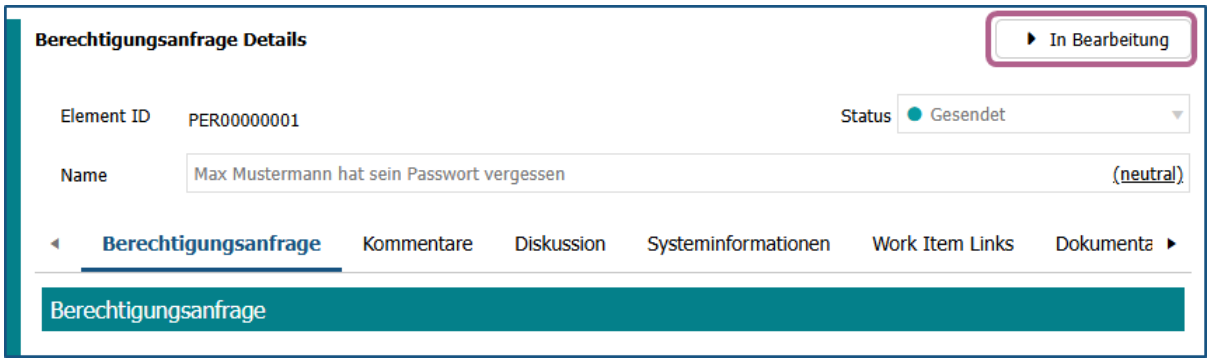
> Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich automatisch ein neues Fenster für die *Berechtigungsanfrage* .

Schritt 2: Berechtigungsanfrage sichten

Als erstes sollte der Empfänger einen Statusübergang von "Gesendet" zu "Bearbeitung" vornehmen.

> Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.

Der Empfänger hat in der erstellten *Berechtigungsanfrage* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, wie er mit der *Berechtigungsanfrage* verfahren möchte. Dafür sollte er die Eingaben im Tab "*Berechtigungsanfrage*" sichten.

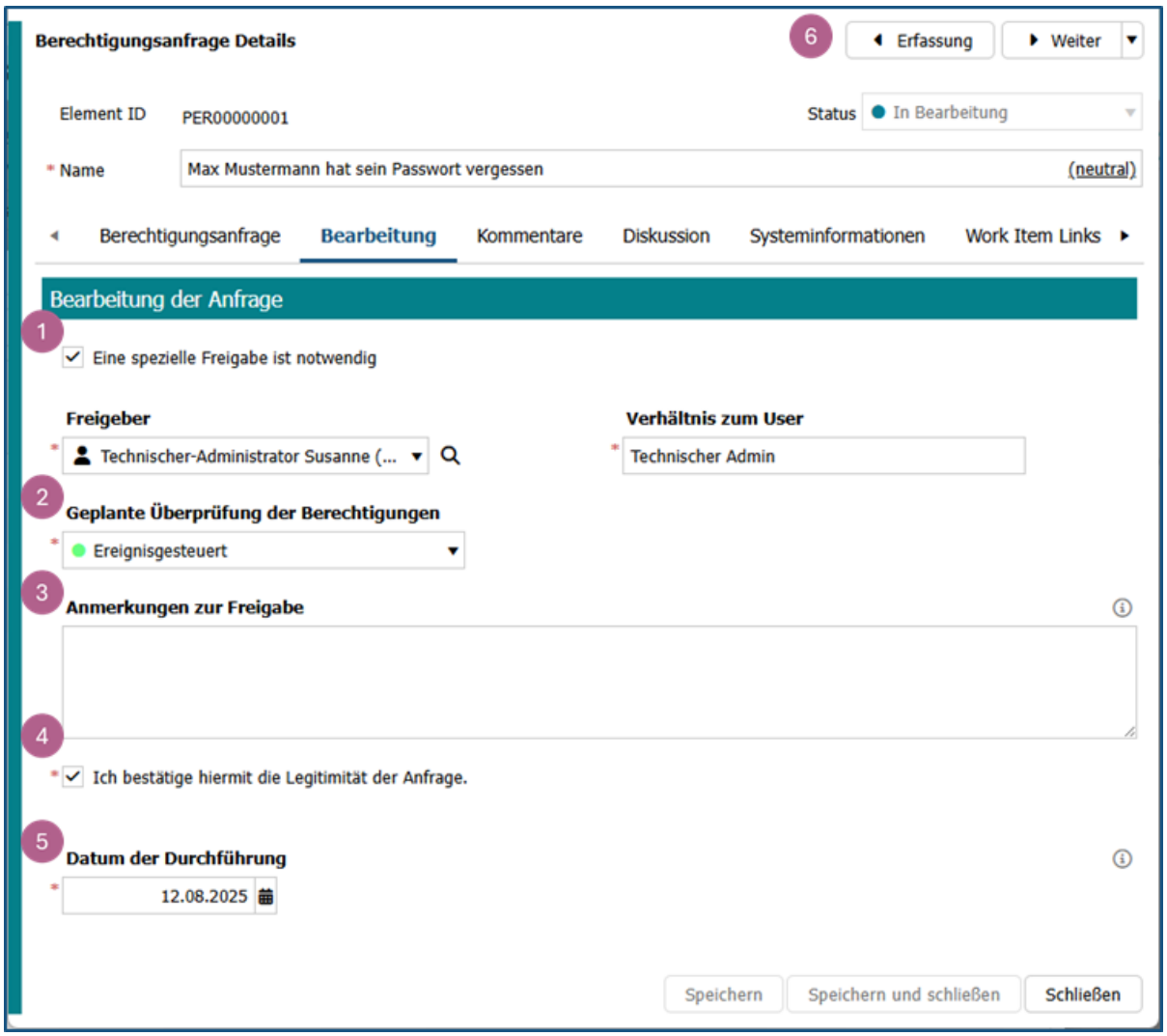


Falls der Anfragenbearbeiter nach der Durchsicht zu der Entscheidung gelangt, dass die Berechtigungsanfrage nicht gerechtfertigt ist kann er die Berechtigungsanfrage zurückweisen. Dafür kann er den Statusübergang in "Zurückgewiesen" durchführen.

> Der Ersteller wird über diesen Statusübergang mittels Notifikation benachrichtigt.

Andernfalls kann der Anfragenbearbeiter mit der Bearbeitung beginnen.

Schritt 3: Berechtigungsanfrage bearbeiten



1 **Spezielle Freigabe?**: Für den Fall dass sich der Anfragenbearbeiter nicht sicher ist, ob er die Berechtigung vergeben kann, sollte er zusätzlich einen "Freigeber" nominieren.

> Der eingetragene "Freigeber" wird mittels Notifikation informiert.

2 **Geplante Überprüfung der Berechtigungen**: Es ist möglich anzugeben, ob und wann eine Überprüfung der neu vergebenen Berechtigungen angestrebt werden sollten.

> Dabei wird automatisch ein Datum gesetzt, wenn nicht "Ereignisgesteuert" ausgewählt wird.

> Der Anfragenbearbeiter wird mittels Scheduler 14 Tage vor der nächsten Evaluierung der Berechtigung automatisch mittels Notifikation benachrichtigt. Dafür muss sich die *Berechtigungsanfrage* im Status "Abgeschlossen" befinden.

3. **Anmerkungen zur Freigabe**: Die Anmerkung bezieht sich auf die Legimität der Berechtigungsvergabe und kann vom Anfragenbearbeiter um alle notwendigen Informationen erweitert werden.
4. **Abnahme**: Nach der Beschreibung der Legitimität muss der Anfragenbearbeiter noch final die zugehörige Checkbox "Ich bestätige hiermit die Legitimität der Anfrage" anklicken. Erst danach wäre ein Statusübergang möglich.
5. **Datum der Durchführung**: Zuletzt muss der Anfragenbearbeiter noch ein Datum angeben wann er die Durchführung vorgenommen hat.
6. **Statuswechsel**: Sobald die Informationen angegeben sind kann der Anfragenbearbeiter speichern und einen Statuswechsel zu in "Abgeschlossen" durchführen.

> Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.

> Nach dem Statusübergang kann das Fenster geschlossen werden.

Disclaimer