

BIC Business Continuity - User Manual

BIC Integrated GRC 2026 Summer

Dokument Version: Juni 2026



Inhaltsverzeichnis

1 Für wen ist dieses User Manual?	11
1.1 Schreibweise	11
1.2 Überblick Symbole	12
1.2.1 Allgemein	12
1.2.2 Dashboard	12
1.2.3 Work Item	12
1 BIC Business Continuity	13
1.3 Standard User	13
1.3.1 Vorfall melden & erstellen	13
Schritt 1: Vorfall erstellen	13
Schritt 2: Details hinterlegen	15
1.3.2 Interne Anfrage definieren & erstellen	16
Schritt 1: Interne Anfrage erstellen	16
Schritt 2: Details hinterlegen	17
Schritt 3: Interne Anfrage abschließen	18
Optional Schritt 4: Diskussion starten	20
1.3.3 Berechtigungsanfrage definieren & erstellen	20
Schritt 1: Berechtigungsanfrage erstellen	20
Schritt 2: Details hinterlegen	22
Schritt 3: Berechtigungsanfrage abschließen	26
1.4 Asseteigner	28
1.5 Asset Manager	28
1.5.1 Assets vorbereiten & pflegen	28
Schritt 1: Navigieren zu Assets	28
Schritt 2: Assets erstellen	29
Schritt 3: Assets tagen	31
Schritt 4: Asseteigenschaften pflegen	32
1.5.2 GRC Framework Elemente für Assessments vorbereiten & zuweisen	32
Schritt 1: GRC Framework Elemente am Asset Typen zuordnen	33
Schritt 2: GRC Framework Elemente am Asset zuordnen	33
1.6 Assessor	34
1.6.1 BSI Business Continuity 200-4 IIA - Assessment erstellen & starten	35
Schritt 1: Navigation zu Assessment	35
Schritt 2: Assessment Details hinterlegen	36
Schritt 3: GRC Framework Element Zuordnungen kontrollieren	37
Schritt 4: Assessment starten	38
1.6.2 BSI Business Continuity 200-4 IIA - Bewertung durchführen & bewerten	38
Schritt 1: Übersicht über Assessment-Schirm	38

Schritt 2: Assessment Details hinterlegen	39
1.6.3 BSI Business Continuity 200-4 IIA - Assessment abschließen & auswerten	40
Schritt 1: Assessment abschließen	40
Schritt 2: Weiteres Vorgehen	42
1.7 Bearbeiter Risiko	42
1.7.1 Bedrohung identifizieren & erstellen	42
Schritt 1: Bedrohung erstellen	42
Schritt 2: Details hinterlegen	44
1.7.2 Schwachstelle identifizieren & erstellen	45
Schritt 1: Schwachstelle erstellen	45
Schritt 2: Details hinterlegen	46
1.7.3 Risikoszenario herleiten & erstellen	47
Schritt 1: Risikoszenario erstellen	47
Schritt 2: Details hinterlegen	49
Schritt 3: Grundlagen festlegen	50
Schritt 4: Kontinuitätsstrategie hinterlegen	53
Schritt 5: Weiteres Vorgehen	54
1.7.4 Ziel definieren & erstellen	55
Schritt 1: Ziel erstellen	55
Schritt 2: Zielsetzung definieren	57
Schritt 3: Weitere Informationen hinterlegen	59
Schritt 4: Update durchführen	60
1.7.5 Zwischenziel definieren & erstellen	61
Schritt 1: Zwischenziel erstellen	61
Schritt 2: Zwischenziel definieren	61
1.7.6 Security-Risiko identifizieren & erstellen	62
Schritt 1: Security-Risiko erstellen	62
Schritt 2: Details hinterlegen	63
1.7.7 Security-Risiko ergänzen & analysieren	65
Optional Schritt 1: Navigation zu spezifischem Security-Risiko nach Fremderstellung	65
Optional Schritt 2: Überprüfung der Eingaben des Erstellers	66
Schritt 3: Zuordnung finalisieren	67
Schritt 4: Eingaben ergänzen	68
Optional - Schritt 5: Risikoanalyse durchführen	70
1.7.8 Security-Risiko beurteilen & bewerten	71
Schritt 1: Bewertung durchführen	71
Schritt 2a: Qualitative Bruttobewertung durchführen	72
Schritt 3a: Qualitative Soll-Bewertung durchführen	73
Schritt 4a: Qualitative Ist-Bewertung durchführen	76
Schritt 2b: Quantitative Bruttobewertung durchführen	77

Schritt 3b: Quantitative Soll-Bewertung durchführen	78
Schritt 4b: Quantitative Ist-Bewertung durchführen	80
1.7.9 Maßnahmenbewertung ableiten & erstellen	81
Schritt 1: Maßnahmenbewertung erstellen	81
Schritt 2: Maßnahme zuordnen	82
Schritt 3: Maßnahmenwirkung dokumentieren	83
Schritt 4: Weiteres Vorgehen	83
1.7.10 Maßnahme identifizieren & erstellen	84
Schritt 1: Maßnahme erstellen aus Maßnahmenbewertung	84
Schritt 2: Details hinterlegen	85
1.7.11 Kontrolle ableiten & erstellen	86
Schritt 1: Kontrolle erstellen aus Security-Risiko	86
Schritt 2: Details hinterlegen	87
1.7.12 Ziel umsetzen & überprüfen	88
Schritt 1: Navigation zu Ziel	89
Schritt 2: Zwischenziele evaluieren	89
Schritt 3: Überprüfung durchführen	89
1.8 Freigeber Risiko	90
1.8.1 Security-Risiko überprüfen & freigeben	90
Schritt 1: Navigation zu spezifischen Security-Risiko	91
Schritt 2: Überprüfung durchführen	91
Schritt 3: Statusübergang durchführen	92
1.9 Bearbeiter Maßnahme	93
1.9.1 Maßnahme definieren & erstellen	93
Schritt 1: Maßnahme erstellen	93
Schritt 2: Details hinterlegen	95
1.9.2 Maßnahme ergänzen & bearbeiten	97
Optional Schritt 1: Navigation zu spezifischer Maßnahme nach Fremderstellung	97
Optional Schritt 2: Überprüfung der Eingaben des Erstellers	98
Schritt 3: Eingaben ergänzen	99
1.9.3 Maßnahme aufbauen & planen	100
Schritt 1: Planung vornehmen	100
1.9.4 Maßnahme verwalten & umsetzen	101
Schritt 1: Navigation zu spezifischer Maßnahme	101
Schritt 2: Umsetzung dokumentieren	102
1.9.5 Optional: Maßnahme überprüfen & verbessern	103
Schritt 1: Navigation zur Maßnahme	104
Schritt 2: Überprüfung durchführen	104
1.9.6 Finding identifizieren & erstellen	106
Schritt 1: Finding aus Maßnahme erstellen	106

Schritt 2: Finding dokumentieren	107
1.9.7 Finding verwalten & behandeln	108
Schritt 1: Navigation zu spezifischem Finding nach Fremderstellung	108
Schritt 2: Finding behandeln	110
1.10 Freigeber Maßnahme	111
1.10.1 Maßnahme überprüfen & freigeben	111
Schritt 1: Navigation zur Maßnahme	111
Schritt 2: Freigabe durchführen	112
1.11 Bearbeiter Kontrolle	113
1.11.1 Kontrolle ableiten & erstellen	114
Schritt 1: Kontrolle erstellen	114
Schritt 2: Details hinterlegen	114
Schritt 3: Zuordnung finalisieren	116
1.11.2 Kontrolle bearbeiten & prüfen	116
Optional Schritt 1: Navigation zu spezifischem Kontrolle nach Fremderstellung	116
Optional Schritt 2: Überprüfung der Eingaben des Erstellers	117
Schritt 3: Kontrolle ergänzen	118
Schritt 4: Kontrolldurchführer & -tester hinterlegen	120
1.11.3 Kontroll-Testings einleiten & erstellen	123
Schritt 1: Navigation zu Kontrolle	124
Schritt 2: Kontroll-Testing erstellen	124
Schritt 3: Details hinterlegen	125
1.11.4 Finding verwalten & behandeln	125
Schritt 1: Navigation zu spezifischem Finding nach Fremderstellung	125
Schritt 2: Finding behandeln	127
1.11.5 Kontroll-Testing überprüfen & freigeben	128
Schritt 1: Navigation zu Kontroll-Testing	128
Schritt 2: Überprüfung durchführen	129
Schritt 3: Statusübergang durchführen	130
1.12 Freigeber Kontrolle	130
1.12.1 Kontrolle überprüfen & freigeben	130
Schritt 1: Navigation zu Kontrolle	130
Schritt 2: Überprüfung durchführen	131
Schritt 3: Statusübergang durchführen	132
1.13 Kontrolldurchführer	132
1.13.1 Kontrolldurchführung erstellen & durchführen	132
Schritt 1: Navigation zu Kontrolle	132
Schritt 2: Durchsicht der Eingaben des Bearbeiters Kontrolle	133
Schritt 3: Kontrolldurchführung erstellen	133
1.14 Tester	135

1.14.1 Kontroll-Testing durchführen & bewerten	136
Schritt 1: Navigation zu Kontrolle	136
Schritt 2: Details hinterlegen	137
1.14.2 Finding identifizieren & erstellen	139
Schritt 1: Finding aus Kontroll-Testing erstellen	139
Schritt 2: Finding dokumentieren	139
1.15 Bearbeiter "Domänenspezifisch"	140
1.15.1 Vorfall bewerten & behandeln	141
Schritt 1: Navigation zu spezifischem Vorfall	141
Schritt 2: Vorfall sichten	142
Schritt 3: Bewertung durchführen	143
Schritt 4: Behandlung definieren	145
Schritt 5: Verlaufsprotokoll dokumentieren	145
Schritt 6: Beurteilung durchführen	146
Schritt 7: Report generieren	147
1.15.2 Business Impact Analyse feststellen & erstellen	148
Schritt 1: Business Impact Analyse aus Essentiellen Prozess erstellen	148
Schritt 2: Details hinterlegen	149
1.15.3 Business Impact Analyse bearbeiten & bewerten	150
Optional Schritt 1: Navigation zu spezifischer Business Impact Analyse nach Fremderstellung	150
Optional Schritt 2: Überprüfung der Eingaben des Erstellers	151
Schritt 3: Bewertung durchführen	151
Schritt 4: Wiederherstellung dokumentieren	154
Schritt 5: Update durchführen	155
1.15.4 Essentiellen Prozess identifizieren & erstellen	156
Schritt 1: Essentiellen Prozess erstellen	156
Schritt 2: Details hinterlegen	157
Schritt 3: Eingaben vervollständigen	158
Schritt 4: Update durchführen	160
1.15.5 Kontinuitätsstrategie herleiten & erstellen	160
Schritt 1: Kontinuitätsstrategie aus Risikoszenario erstellen	161
Schritt 2: Details hinterlegen	161
Schritt 3: Eingaben vervollständigen	163
Schritt 4: Bewertung durchführen	164
1.15.6 Kontinuitätsstrategie bearbeiten & umsetzen	165
Schritt 1: Navigation zu Kontinuitätsstrategie	165
Schritt 2: Bewertung durchführen	166
Schritt 3: Notfallpläne erstellen	167
1.15.7 Notfallplan herleiten & erstellen	167

Schritt 1: Notfallplan erstellen	167
Schritt 2: Notfallplan beschreiben	168
1.15.8 Ressource identifizieren & erstellen	169
Schritt 1: Ressource erstellen	169
Schritt 2: Details hinterlegen	170
Schritt 3: Details ergänzen	171
Schritt 4: Ausfallszenario dokumentieren	172
Schritt 5: Wiederherstellung dokumentieren	173
Schritt 6: Wiederherstellungsaktivität erstellen	176
Schritt 7: Update durchführen	176
1.15.9 Management Review definieren & erstellen	177
Schritt 1: Management Review erstellen	177
Schritt 2: Details definieren	178
Schritt 3: Weitere Informationen hinterlegen	179
Schritt 4: Management Review dokumentieren	181
1.15.10 Management Review durchführen & überprüfen	182
Schritt 1: Navigation zu Management Review	182
Schritt 2: Management Review durchführen	182
Schritt 3: Statusübergang durchführen	184
1.15.11 Finding identifizieren & erstellen	185
Schritt 1: Finding aus Management Review erstellen	185
Schritt 2: Finding dokumentieren	186
1.16 Freigeber "Domänenspezifisch"	187
1.16.1 Business Impact Analyse überprüfen & freigeben	188
Schritt 1: Navigation zu Business Impact Analyse	188
Schritt 2: Business Impact Analyse überprüfen	188
Schritt 3: Statusübergang durchführen	189
1.16.2 Ressource überprüfen & freigeben	189
Schritt 1: Navigation zu Ressource	190
Schritt 2: Ressource überprüfen	190
Schritt 3: Statusübergang durchführen	190
1.16.3 Essentiellen Prozess überprüfen & freigeben	191
Schritt 1: Navigation zu Essentiellen Prozess	191
Schritt 2: Essentiellen Prozess überprüfen	191
Schritt 3: Statusübergang durchführen	191
Schritt 4: Bericht generieren	192
1.16.4 Kontinuitätsstrategie überprüfen & freigeben	192
Schritt 1: Navigation zu Kontinuitätsstrategie	193
Schritt 2: Kontinuitätsstrategie überprüfen	193
Schritt 3: Statusübergang durchführen	193

1.16.5 Notfallplan überprüfen & freigeben	194
Schritt 1: Navigation zu Notfallplan	194
Schritt 2: Notfallplan überprüfen	194
Schritt 3: Statusübergang durchführen	195
Schritt 4: Bericht generieren	195
1.16.6 Notfallübung überprüfen & freigeben	196
Schritt 1: Navigation zu Notfallübung	196
Schritt 2: Notfallplan überprüfen	196
Schritt 3: Statusübergang durchführen	197
1.16.7 Bericht(e) öffnen & generieren	197
1.17 Vorsorgekoordinator	197
1.17.1 Notfallplan definieren & planen	197
Schritt 1: Navigation zu spezifischer Notfallplan nach Fremderstellung	198
Optional Schritt 2: Überprüfung der Eingaben des Erstellers	199
Schritt 3: Eingaben ergänzen	199
1.17.2 Notfallaktivität definieren & erstellen	200
Schritt 1: Notfallaktivität erstellen	200
Schritt 2: Notfallaktivität beschreiben	201
Schritt 3: Notfallaktivität ergänzen	201
1.17.3 Notfallübungen ableiten & erstellen	203
Schritt 1: Notfallübungen erstellen	203
Schritt 2: Notfallübung beschreiben	204
Schritt 3: Notfallübung ergänzen	204
1.17.4 Notfallübung einleiten & durchführen	206
Schritt 1: Navigation zu Notfallübung	206
Schritt 2: Notfallübung starten	207
Schritt 3: Statuswechsel durchführen	208
1.17.5 Finding identifizieren & erstellen	208
Schritt 1: Finding aus Notfallübung erstellen.	208
Schritt 2: Finding dokumentieren	209
1.18 Dokumenteneigner	210
1.18.1 Dokumentierte Information definieren & erstellen	210
Schritt 1: Dokumentierte Information erstellen	210
Schritt 2: Details hinterlegen	212
Schritt 3: Eingaben vervollständigen	213
1.18.2 Dokumentierte Information evaluieren & überprüfen	215
Schritt 1: Navigation zu Dokumentierte Information	216
Schritt 2: Dokumentierte Information sichten	217
Schritt 3: Anmerkung hinterlassen	217
1.19 Dokumentenmanager	218

1.19.1 Dokumentierte Information überprüfen & freigeben	218
Schritt 1: Navigation zur Dokumentierten Information	219
Schritt 2: Dokumentierte Information sichten	219
Schritt 3: Anmerkung hinterlassen	219
1.20 Bearbeiter Audit	221
1.20.1 Audit definieren & erstellen	221
Schritt 1: Audit erstellen	221
Schritt 2: Details hinterlegen	222
Schritt 3: Details ergänzen	224
Schritt 4: Planung hinterlegen	227
Schritt 5: Auditaktivitäten planen	228
Schritt 6: Statuswechsel vornehmen	228
1.20.2 Auditaktivität definieren & planen	228
Schritt 1: Auditaktivität erstellen	229
Schritt 2: Auditaktivität definieren	229
Schritt 3: Weiteres Vorgehen	230
1.20.3 Audit starten & durchführen	231
Schritt 1: Navigation zu Audit	231
Schritt 2: Auditaktivitäten durchführen	232
Schritt 3: Auditaktivitäten abschließen	232
1.20.4 Auditaktivität starten & durchführen	232
Schritt 1: Auditaktivität öffnen	233
Schritt 2: Auditaktivität durchführen	234
Schritt 3: Auditaktivität abschließen	235
1.20.5 Finding identifizieren & erstellen	235
Schritt 1: Finding aus Auditaktivität erstellen	235
Schritt 2: Finding dokumentieren	235
1.20.6 Audit bewerten & abschließen	237
Schritt 1: Audit bewerten	237
1.21 Freigeber Audit	238
1.21.1 Audit überprüfen & freigeben	238
Schritt 1: Navigation zu Audit	238
Schritt 2: Audit überprüfen	239
Schritt 3: Statusübergang durchführen	240
1.22 Manager	240
1.22.1 Security-Risiko freigeben	240
Schritt 1: Navigation zu spezifischem Security-Risiko	240
Schritt 2: Freigabe durchführen	241
1.22.2 Management Review sichten & freigeben	242
Schritt 1: Navigation zu spezifischen Management Review	243

Schritt 2: Überprüfung durchführen	243
Schritt 3: Statusübergang durchführen	243
Schritt 4: Bericht generieren	243
1.23 Spezielle Benutzerprofile	244
1.23.1 Interne Anfrage beantworten & bearbeiten	245
Schritt 1: Navigation zur Internen Anfrage	245
Schritt 2: Interne Anfrage sichten	245
Schritt 3: Interne Anfrage bearbeiten	247
1.23.2 Berechtigungsanfrage beantworten & bearbeiten	248
Schritt 1: Navigation zur Berechtigungsanfrage	248
Schritt 2: Berechtigungsanfrage sichten	249
Schritt 3: Berechtigungsanfrage bearbeiten	250

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

1 BIC Business Continuity

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 Solution 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.

1.3 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:

- [Vorfall melden & erstellen](#)
- [Interne Anfrage definieren & erstellen](#)
- [Berechtigungsanfrage definieren & erstellen](#)

1.3.1 Vorfall melden & erstellen

Das Melden von Vorfällen im Business Continuity-Kontext ist essenziell, um die Fähigkeit zur Aufrechterhaltung kritischer Geschäftsprozesse im Störfall sicherzustellen. Vorfallmeldungen sind hier der Startpunkt für Reaktion, Wiederanlauf und langfristige Verbesserungen.

Die Erstellung von Work Items des Typs *Vorfall* wird bei den aktiven Modulen "Business Continuity" und "Information Security" auch anderen aktiven Modulen ermöglicht. So können Benutzer aus allen Modulen bei Bedarf *Vorfälle* melden und nicht nur Benutzer aus den Bereichen "Business Continuity" und "Information Security".

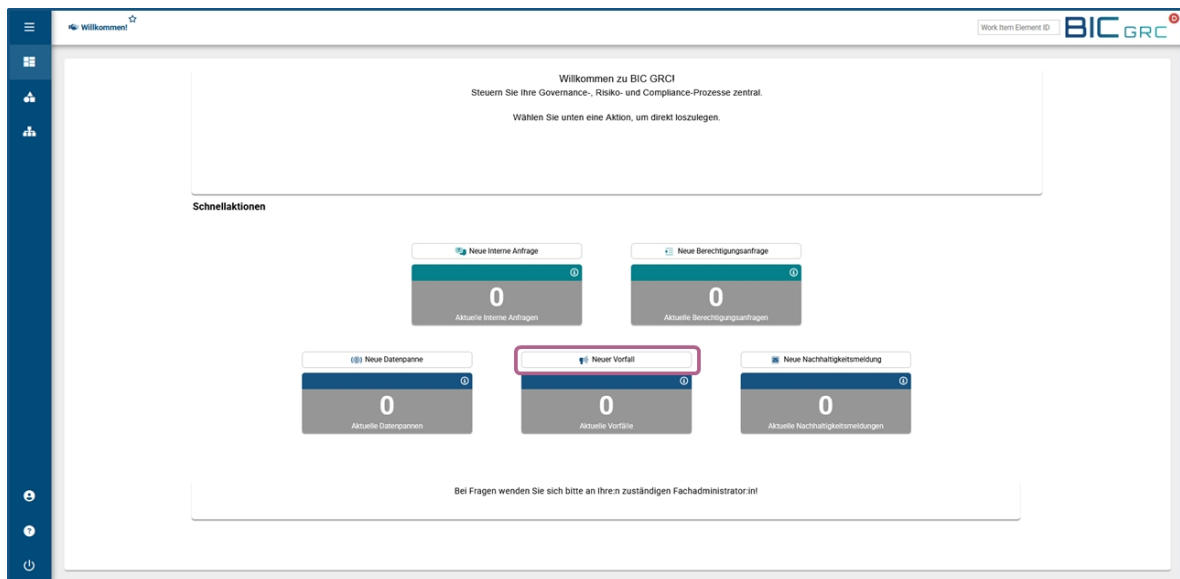
Um dies sicherstellen zu können kann jeder aktive Benutzer in BIC GRC mit dem aktiven Modul Business Continuity einen Vorfall erstellen.

Schritt 1: Vorfall erstellen

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

1. Erstellen über Dashboard

Der Benutzer navigiert über die Menüleiste zu **Dashboards >> Willkommen >> "Neuer Vorfall "**.

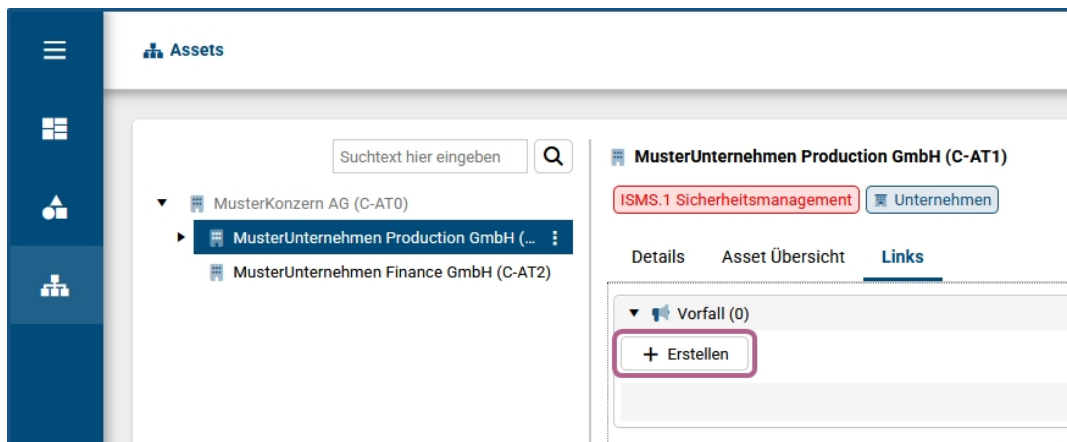


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellen über Asset Übersicht "Links"

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

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

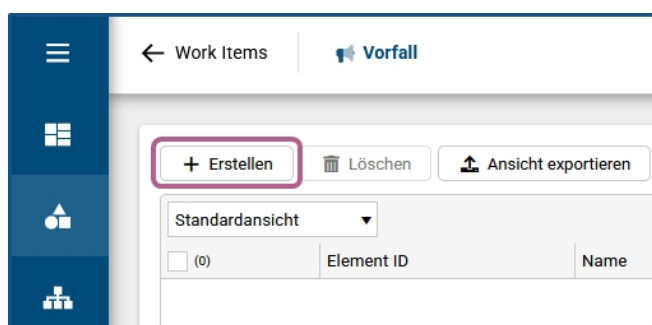


Ein neues Fenster öffnet sich anschließend automatisch.

3. Erstellung über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items >> Vorfall >> "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 *Vorfall* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht den *Vorfall* einzigartig.

2 **Daten zur Meldung:** Es werden zwei verschiedene Daten unterschieden, die zu melden sind. Dabei ist darauf zu achten, dass das Datum von "Entdeckung des Vorfalls" dem Datum von "Eintritt des Vorfalls" nachgelagert sein muss.

Final muss hinterlegt werden durch wen der Vorfall festgestellt wurde. Dabei können mehrere Personen in Textform angegeben werden.

So können auch Personen angegeben werden, die keinen aktiven Benutzer in BIC GRC sind.

3 **Art des Vorfalls:** Der Benutzer hat anzugeben, um welche Art von Vorfall es sich handelt.

4 **Kategorie:** In BIC GRC gibt es vorgefertigte Kategorien, um *Vorfälle* besser einordnen zu können.

Die Kategorien können für das eigene Unternehmen leicht im GRC Framework von berechtigten Personen erweitert werden.

5 **Ausfallszenario:** Aus einem GRC Framework kann der Benutzer wählen, welche "Ausfallszenarien" zu erwarten sind.

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

- 7 **Standort des Vorfalls** : Mittels des Asset-Links kann der Standort des *Vorfalls* genau angegeben werden.

Es werden dem Benutzer nur "Organisationseinheiten" angezeigt, an denen er auch als Standard Benutzer eine Berechtigung besitzt.

- 8 **Beschreibung**: Der *Vorfall* sollte so ausführlich wie möglich dokumentiert werden, inklusive der Angabe aller beteiligten Personen. Wenn Ursache und Auswirkung des *Vorfalls* bekannt sind, sollten auch diese Informationen angegeben werden für Benutzer die im Workflow nachgelagert sind.
- 9 **Beschreibung der Ausnutzbarkeit/Schwachstelle**: Zusätzlich wird empfohlen, mittels einer eigenen Beschreibung die Ausnutzbarkeit bzw. die Schwachstelle genauer zu dokumentieren.
- 10 **Speichern**: Sobald die Informationen angegeben sind kann der Benutzer speichern.

1.3.2 Interne Anfrage definieren & erstellen

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

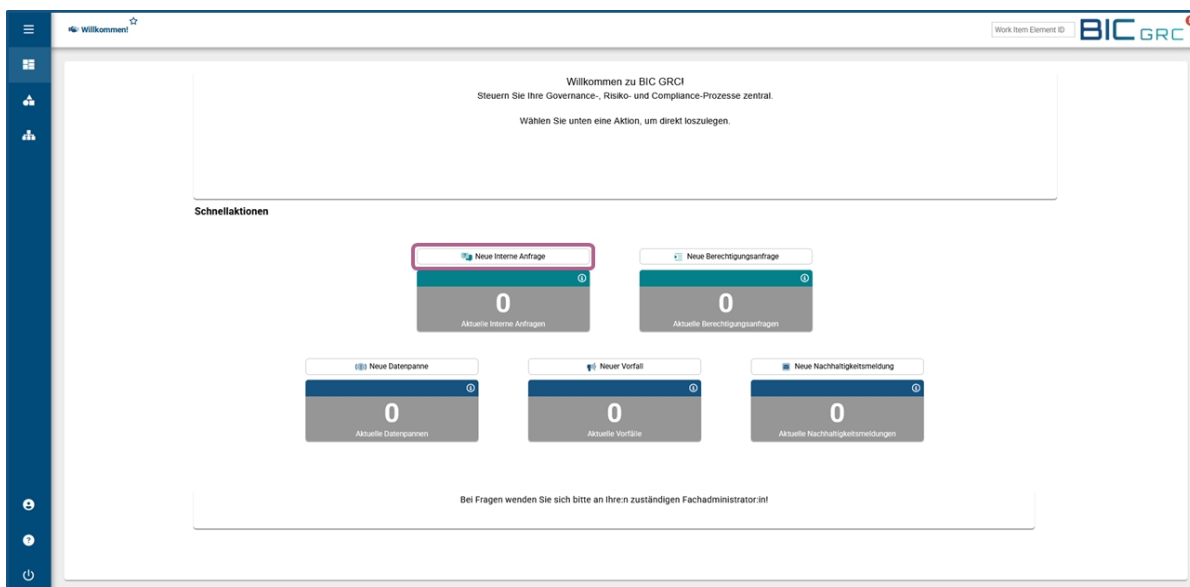
Diese Anfrage kann genutzt werden, um neue Profile oder einzelne Berechtigungen zu beantragen. Auch Anpassungen an bestehenden Profilen können angefragt werden.

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"**.

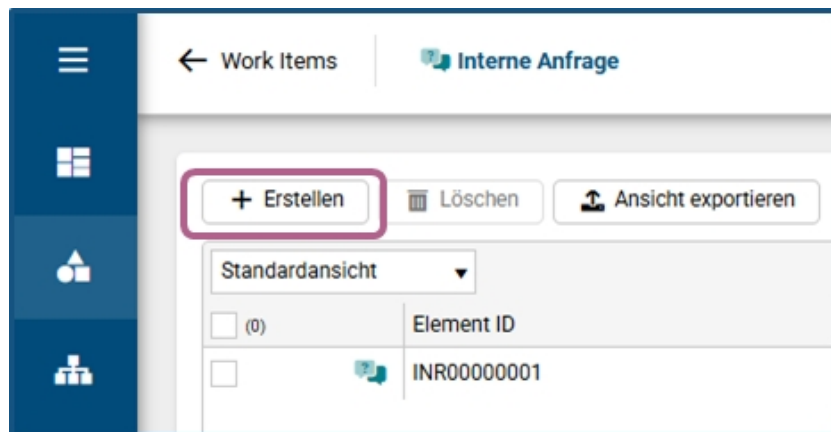


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen

Interne Anfrage Details

Status Erfassung

Name 1 Anfrage zu der Erstellung eines Ziels (neutral)

Anfrage

Diskussion

Interne Anfrage

2

Art der Anfrage

Name	Katalog	B...	
How-to-use-Anfrage	Typen Interner ...		

3

Asset Link

Name	Asset-Typ	Code-Group	B...	
Baltravia	Unternehmensorganisation	Y_BusinessStructure		

4

Beschreibung

Ich muss für meinen Standort ein Ziel definieren und weiß nicht wie ich beginnen soll. Ich bräuchte jemanden, der mich dafür anleitet, da ich am Tag der Einschulung krank war.

5

Dringlichkeit

Niedrig

Normal

Hoch

Kritisch

6

Empfänger

Fachadministrator Rainer (Functional...

7

Sie haben ungespeicherte Änderungen.

Speichern

Speichern und schließen

Schließen

- 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.

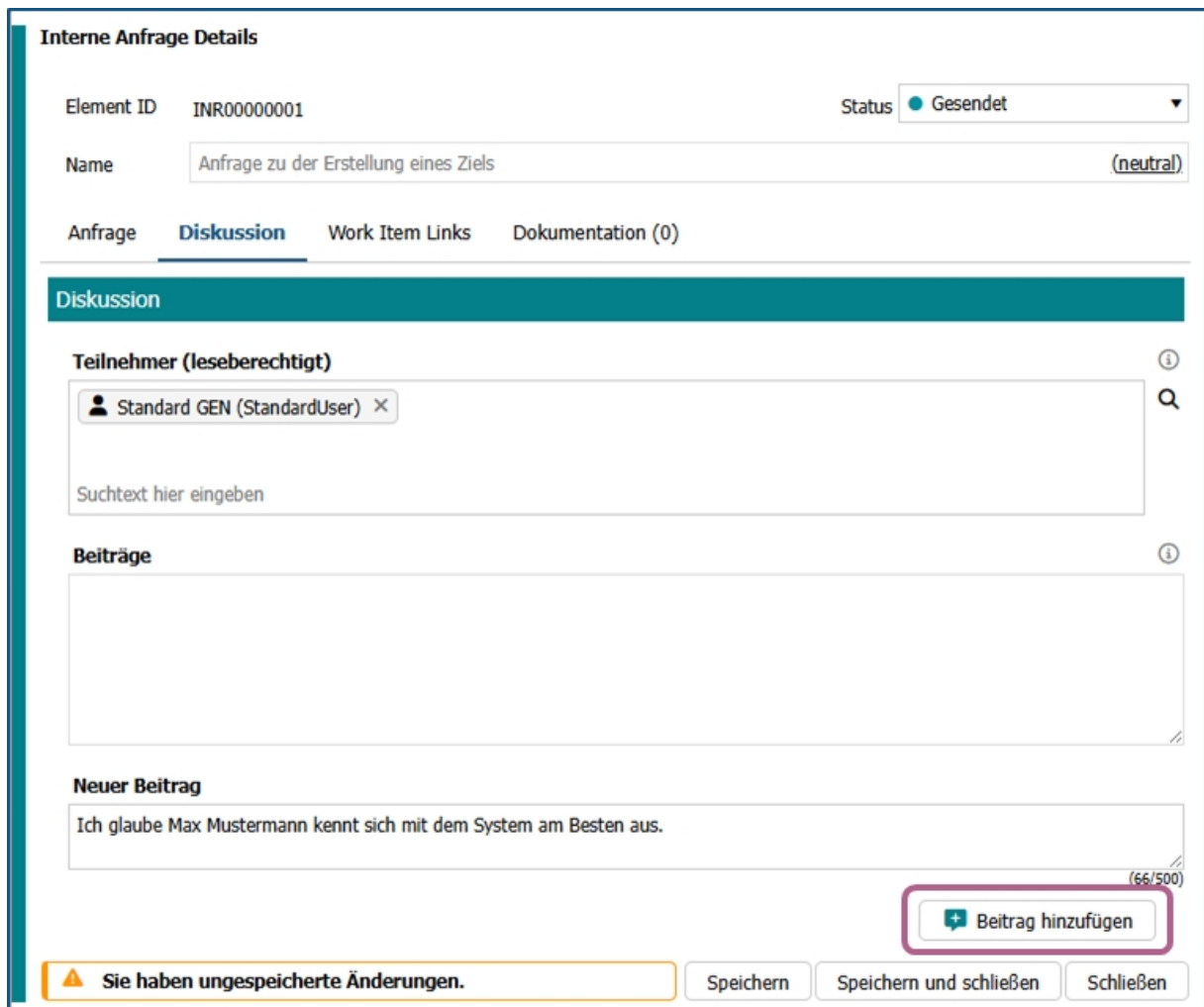
Schritt 3: Interne Anfrage abschließen

Nach dem erstmaligen Speichern wird das Datum der Anfrage automatisch befüllt ¹. Weiters kann – 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 Interne Anfrageempfänger prüft die Anfrage, ergänzt sie bei Bedarf und entscheidet, ob sie genehmigt oder zurückgewiesen wird.

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.



Interne Anfrage Details

Element ID: INR00000001 Status: ● Gesendet

Name: Anfrage zu der Erstellung eines Ziels (neutral)

Anfrage **Diskussion** Work Item Links Dokumentation (0)

Diskussion

Teilnehmer (leseberechtigt)

Standard GEN (StandardUser) x

Suchtext hier eingeben

Beiträge

Neuer Beitrag

Ich glaube Max Mustermann kennt sich mit dem System am Besten aus. (66/500)

Beitrag hinzufügen

Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

1.3.3 Berechtigungsanfrage definieren & erstellen

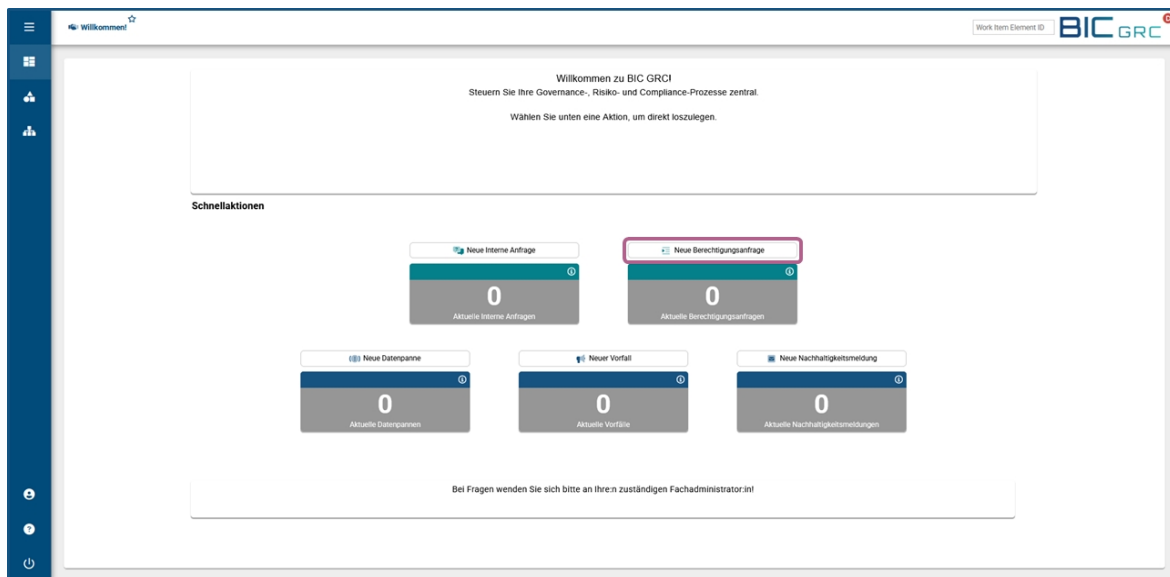
Jeder Benutzer in BIC GRC hat die Möglichkeit eine *Berechtigungsanfrage* zu stellen.

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"**.

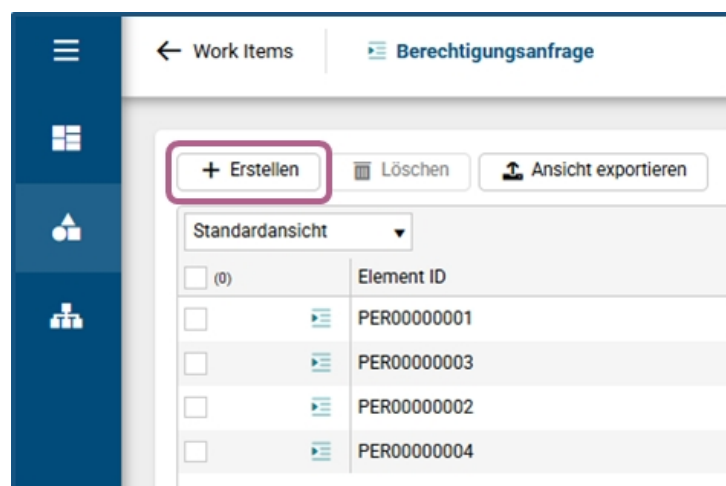


Ein neues Fenster öffnet sich anschließend automatisch.

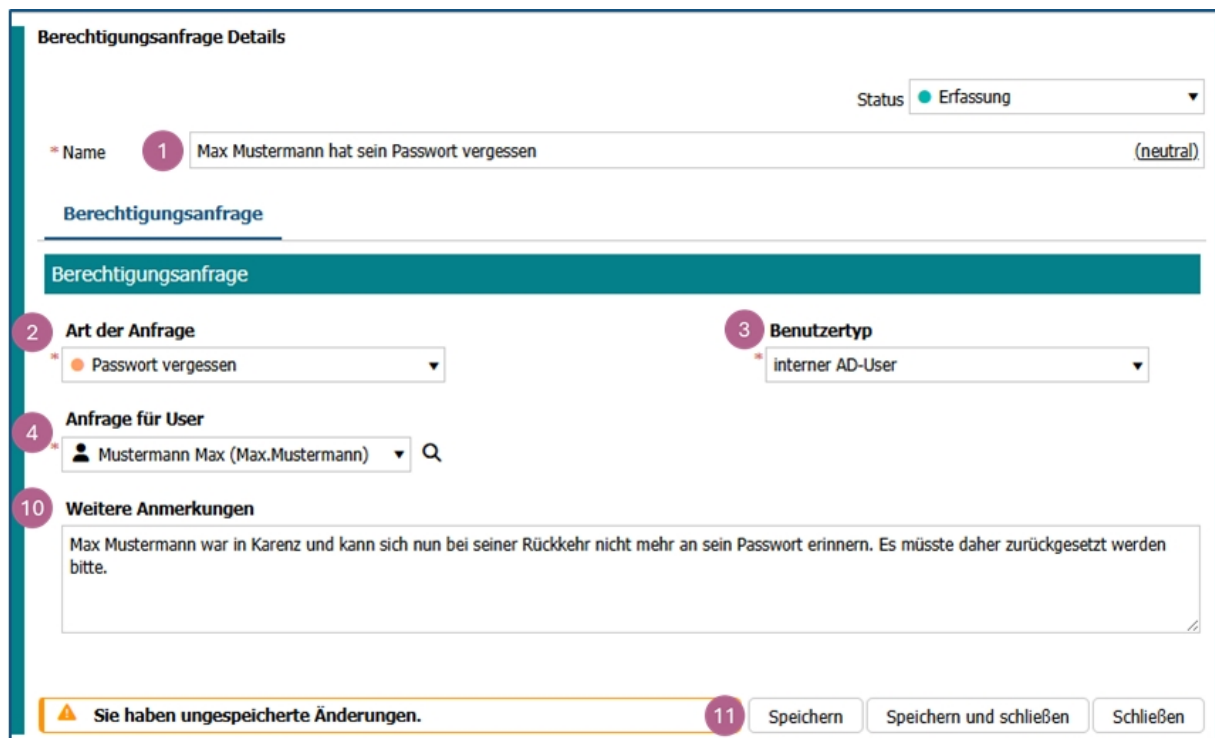
2. Erstellung über Work Item List

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 Neuer Arbeitsvertrag bei Max Musterman (neutral)

Berechtigungsanfrage

Berechtigungsanfrage

2 Art der Anfrage

Neuanlage Berechtigungen

3 Benutzertyp

interner AD-User

Anfrage für User

Mustermann Max (Max.Mustermann)

Q

4 Grundlage der Berechtigungen

neuer Arbeitsvertrag

7 Angefragte Profile

AssetOwner X

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

Berechtigungsanfrage Details

Status ● Erfassung

1 Name Sabine Müller übernimmt eine neue Verantwortung im Bereich Audit (neutral)

Berechtigungsanfrage

2 Art der Anfrage **3** Benutzertyp

● Neuanlage Berechtigungen * interner manueller User

Anfrage für neuen User

5 Nachname Vorname

Müller 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 X

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

11 Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

Berechtigungsanfrage Details

Status Erfassung

* Name 1 Karenz von Max Mustermann (neutral)

Berechtigungsanfrage

Berechtigungsanfrage

2

Art der Anfrage

* Ruhendstellung von Berechtigungen

3

Benutzertyp

* interner AD-User

4

Anfrage für User

* Mustermann Max (Max.Mustermann) Q

6

Grundlage der Berechtigungen

inaktives Arbeitsverhältnis

Ruhendstellung der Berechtigungen

9

von

* 01.07.2025 📅

9

bis

* 30.11.2025 📅

10

Weitere Anmerkungen

Max Mustermann wird bis Ende November in Karenz sein

⚠ 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 kann – 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.

Berechtigungsanfrage Details

Obsolet

Element ID

PER00000001

Status

Erfassung

Name

Max Mustermann hat sein Passwort vergessen

(neutral)

Berechtigungsanfrage

Kommentare

Diskussion

Work Item Links

Dokumentation (0)

Berechtigungsanfrage

Erfasser

Standard GEN (StandardUser)

Art der Anfrage

Passwort vergessen

Anfrage für User

Mustermann Max (Max.Mustermann)

Weitere Anmerkungen

Max Mustermann war in Karenz und kann sich nun bei seiner Rückkehr nicht mehr an sein Passwort erinnern. Es müsste daher zurückgesetzt werden bitte.

Anlage

Dateien hierher ziehen zum Hochladen

Keine Dokumente vorhanden.

1

Bearbeiter

Fachadministrator Rainer (Functional...

Benutzertyp

interner AD-User

3

Senden

Speichern

Speichern und schließen

Schließen

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.

1.4 Asseteigner

Der Begriff „Asseteigner“ bezeichnet ein Benutzerprofil mit Verantwortung für ein oder mehrere Assets innerhalb von BIC GRC. Dabei können in BIC GRC je nach Modul Organisationseinheiten, Primary Assets (Informationen & Prozesse) oder Supporting Assets (z.B. Software, Hardware,...) als Asset gepflegt werden.

Folgende Aufgaben hat ein Asseteigner in BIC GRC:

- [Maßnahmen identifizieren & erstellen](#)

Der Asseteigner wird zu dem Benutzerprofil "Bearbeiter Maßnahme" für die genauen Anweisungen für die Erstellung einer *Maßnahme* weitergeleitet.

1.5 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](#)
- [GRC Framework Elemente für Assessments vorbereiten & zuweisen](#)

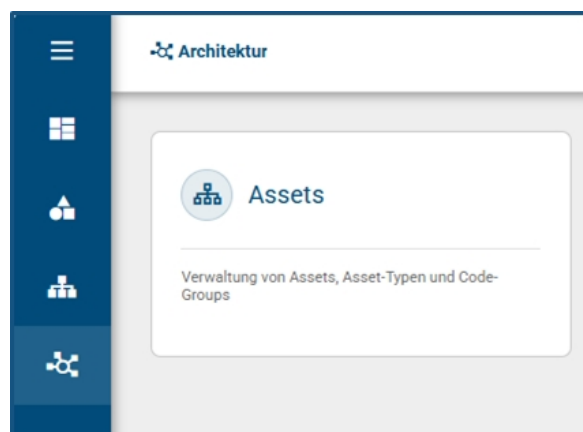
1.5.1 Assets vorbereiten & pflegen

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.

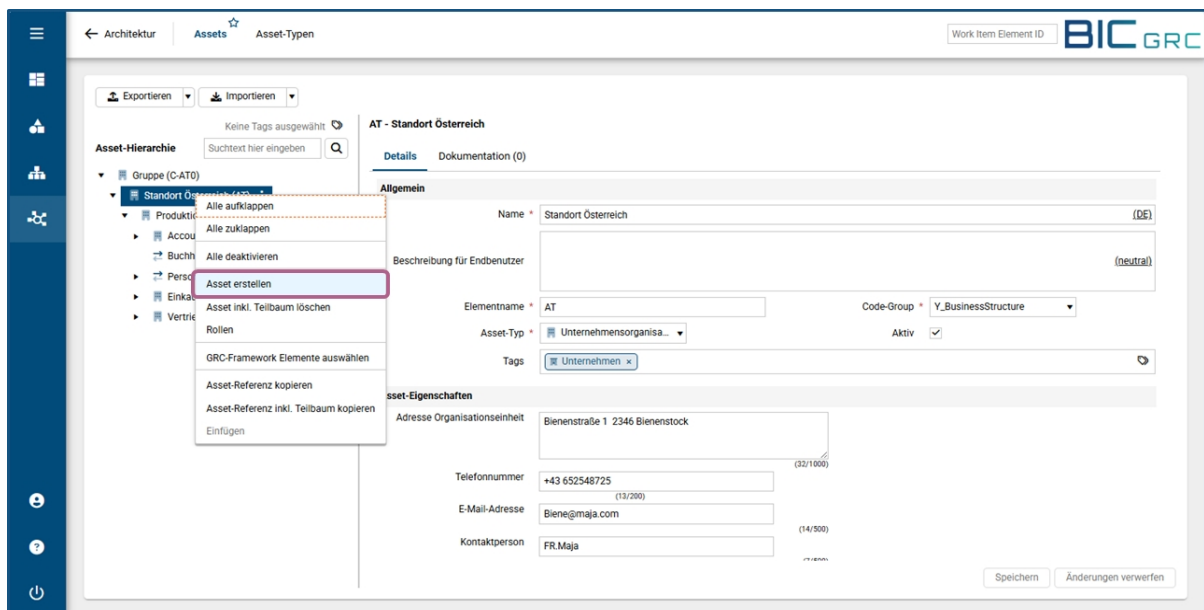
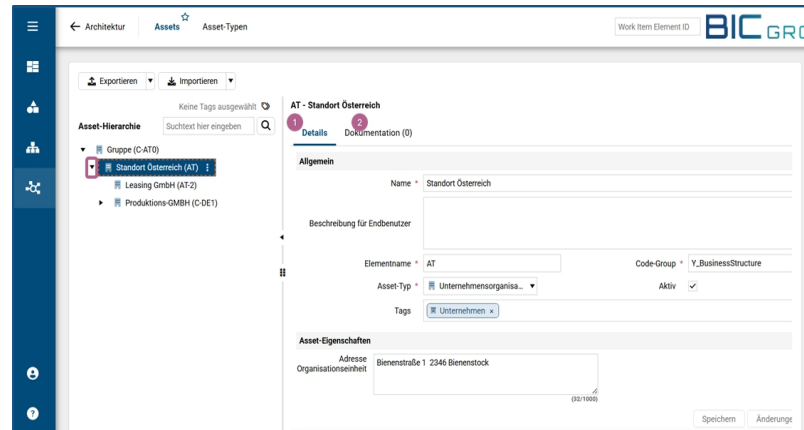
Dabei ist die Ansicht auf Berechtigungsebene beschränkt und kann je nach Benutzer variieren.



Schritt 2: Assets erstellen

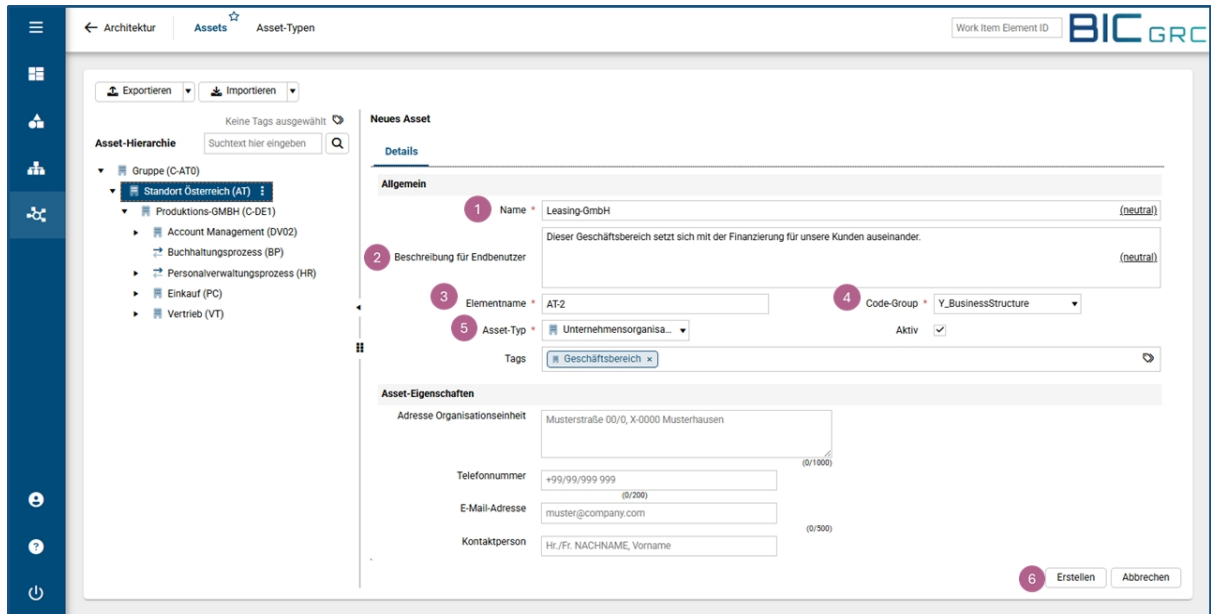
Der Asset Manager bekommt bei dem Menüunterpunkt **Assets** eine zweigeteilte Ansicht:

- 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-Hierarchie einen Geschäftsbereich "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:

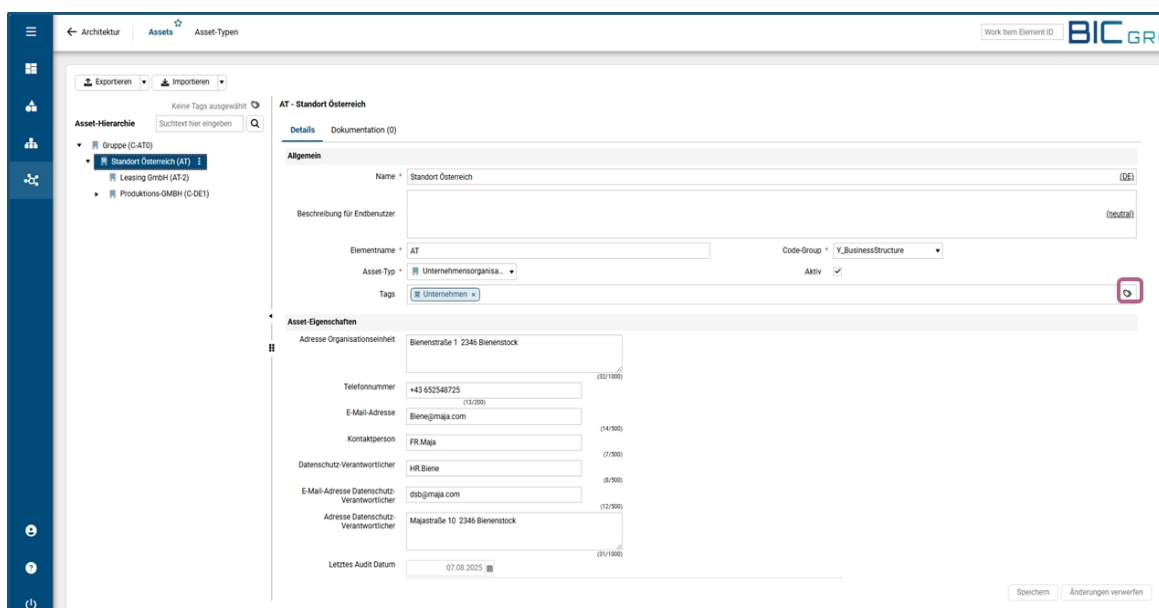
- Unternehmensorganisation: Stellen nach dem obersten Knotenpunkt in der Assesthierarchie die höchstmögliche Ebene/Level da.
- Primary Asset: Sind direkt unter den Unternehmensorganisationen einzuordnen und sind Informationen oder Prozesse.
- Supporting Asset: Stellen alle Elemente da, die den Prozess oder die Information unterstützen.
- 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

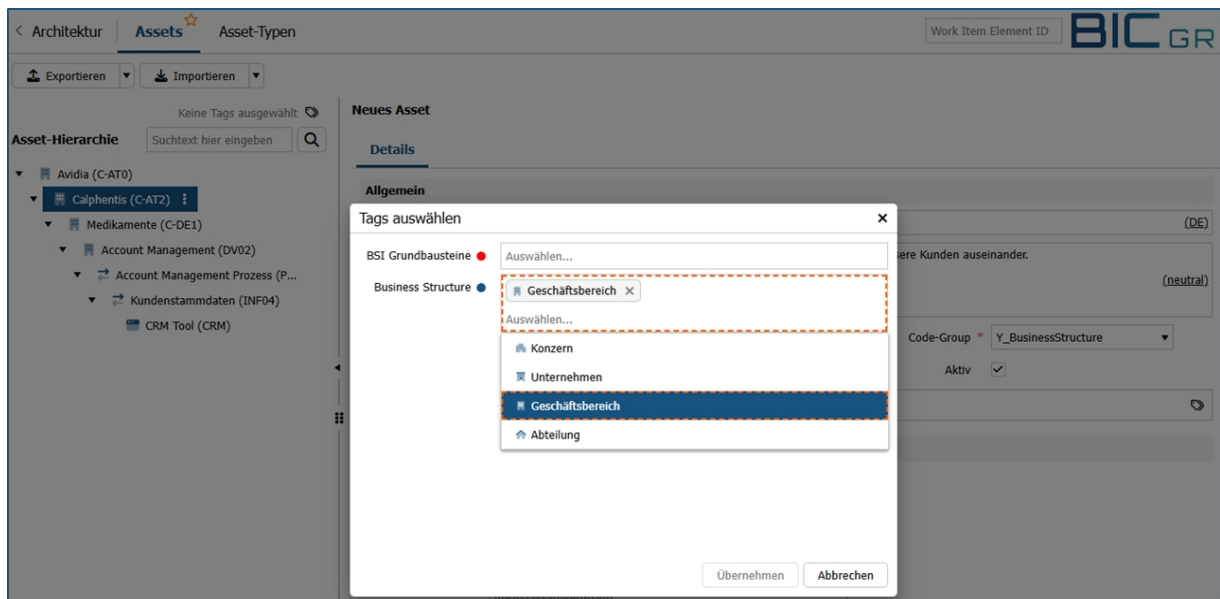
Nach Erstellung des Assets werden passende Tags vergeben. Durch Klick auf das entsprechende Icon  werden alle verfügbaren Tags vorgeschlagen, die dem Asset zugeordnet werden können.



The screenshot shows the 'AT - Standort Österreich' (AT - Austria Location) asset creation form in the BIC GRC system. The form is divided into several sections:

- Asset-Hierarchie:** A tree view on the left showing the hierarchy: Gruppe (CATG) > Standort Österreich (AT) > Leasing GmbH (AT2) > Produktions-GMBH (C-DE1).
- Details:**
 - Allgemein:**
 - Name: Standort Österreich (ID1)
 - Beschreibung für Endbenutzer: (empty field)
 - Elementname: AT
 - Code-Group: V_BusinessStructure
 - Asset-Typ: Unternehmensorganisa...
 - Tags: Unternehmen
 - Asset-Eigenschaften:**
 - Adresse Organisationseinheit: Bienenstraße 1 2346 Bienenstock
 - Telefonnummer: +43 652548725 (12/1000)
 - E-Mail-Adresse: Biene@maja.com (13/200)
 - Kontaktperson: FR Maja (14/300)
 - Datenschutz-Verantwortlicher: HR Biene (17/200)
 - E-Mail-Adresse Datenschutz-Verantwortlicher: dsb@maja.com (18/300)
 - Adresse Datenschutz-Verantwortlicher: Majasträße 10 2346 Bienenstock (19/1000)
 - Letztes Audit Datum: 07.08.2025

Buttons at the bottom right: Speichern, Änderungen verwerfen.



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: Asseeteigenschaften pflegen

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

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

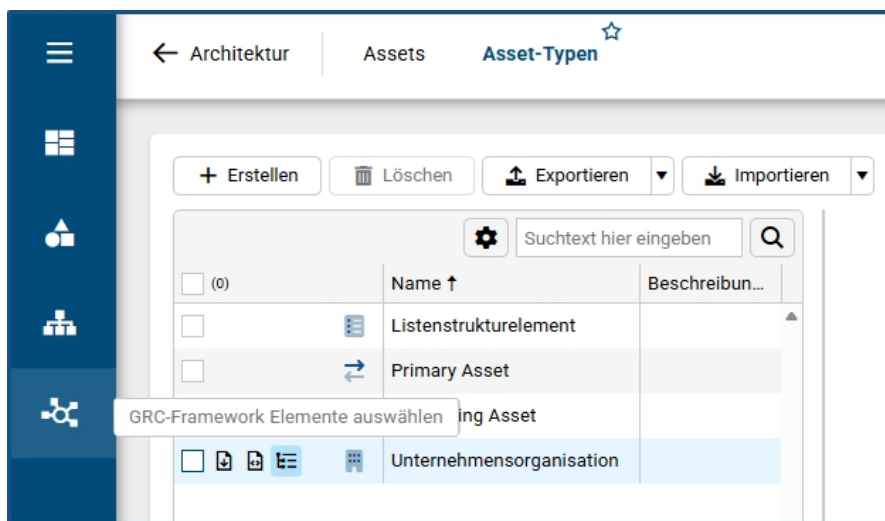
"Primary Assets" haben auch Asseeteigenschaften, diese sollen aber nicht vom Asset Manager bearbeitbar werden, sondern werden durch unterschiedliche Mechanismen von BIC GRC automatisch befüllt.

1.5.2 GRC Framework Elemente für Assessments vorbereiten & zuweisen

In BIC GRC werden Assessments durchgeführt. Assessments sind dabei immer im Kontext eines Assets zu betrachten. Sollten daher GRC Framework Elemente im Rahmen eines Assessments für einen bestimmten Asset Typen abgefragt werden, muss dies vor dem Start eines Assessments hinterlegt worden sein.

Schritt 1: GRC Framework Elemente am Asset Typen zuordnen

Über die Menüleiste **Administration >> Assets >> Reiter "Asset Typen"** kann der Asset Manager zu den Asset Typen navigieren.



Über das Icon  neben dem Namen des Asset Typen auf der linken Seite oder den Button "Exportieren" kann die Auswahl "Auswahl von GRC-Framework Elementen" getroffen werden.

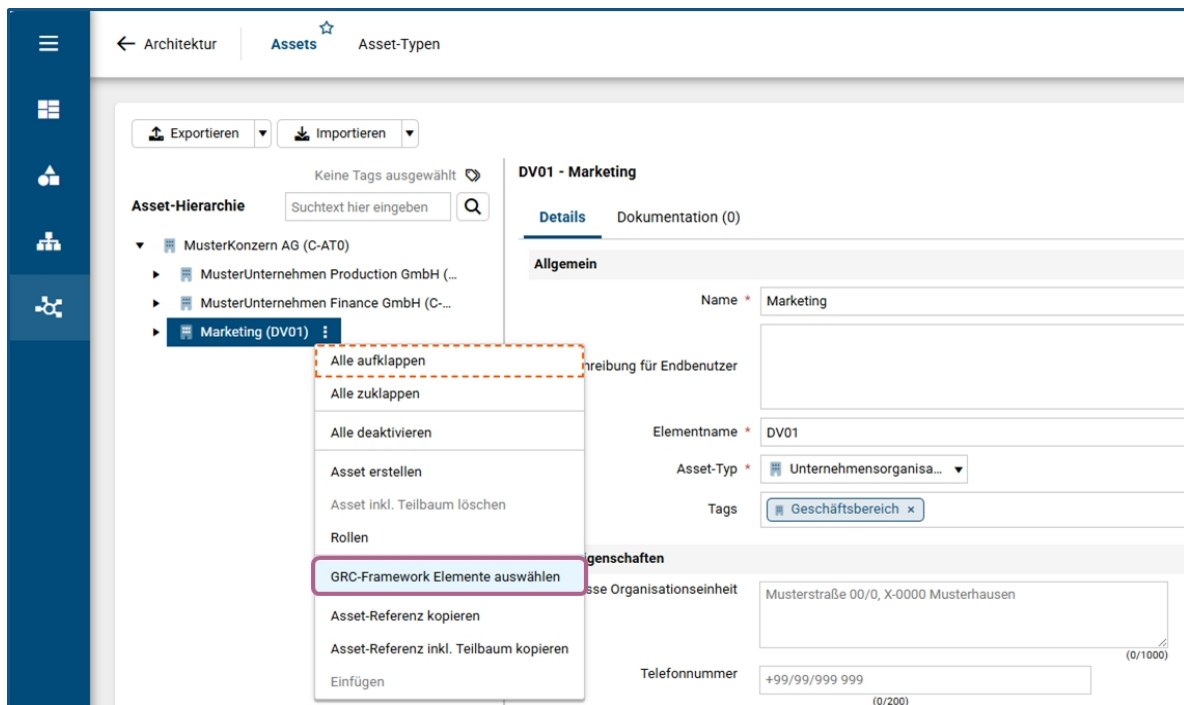
Anschließend wird dem Asset Manager eine Liste von Assessments bzw. deren Phasen angezeigt die in einer oder mehreren Modulen in BIC GRC aktiv sind.

Für weitere Informationen kann im BIC GRC Administratoren Handbuch nachgeschlagen werden.

Schritt 2: GRC Framework Elemente am Asset zuordnen

Über die Menüleiste **Administration >> Assets >> Reiter "Assets"** kann der Asset Manager ergänzend zu den Asset Typen auch an den Assets Zuordnungen zu GRC Framework Elementen machen.

Mittels Rechts-Klick auf ein Asset bzw. Klick auf die drei Punkte neben dem Asset Namen  auf der linken Seite können bei den Typen "Unternehmensorganisationseinheit" oder "Supporting Asset" der Menüpunkt "GRC-Framework Elemente auswählen" Elemente hinzugefügt werden.



Anschließend wird dem Assemanager eine Liste von Assessments bzw. deren Phasen angezeigt die in einer oder mehreren Modulen in BIC GRC aktiv sind.

1.6 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 BSI Business Continuity 200-4 IIA .

Folgende Aufgaben hat ein Assessor in BIC GRC:

BSI Business Continuity 200-4 IIA

- [Assessment erstellen & starten](#)
- [Bewertung durchführen & bewerten](#)
- [Assessment abschließen & auswerten](#)

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](#)
- [Security-Risiko identifizieren & erstellen](#)

1.6.1 BSI Business Continuity 200-4 IIA - Assessment erstellen & starten

Ein Assessment vom Typ „BSI IT- Grundschutz“ ist ein wertvolles Instrument zur Standortbestimmung und Weiterentwicklung des unternehmensweiten Business Continuity Managements nach dem neuen BSI-Standard 200- 4. Es orientiert sich speziell an den Anforderungen der Umsetzungsstufe IIA („Erweiterte Basis-Absicherung“) des BSI.

Das Assessment soll einen klaren Überblick über vorhandene Stärken und bestehende Lücken im Unternehmen schaffen.

Der Assessor hat im Assessment "BSI Business Continuity 200-4 IIA" die Aufgabe der Erstellung des Assessments und der Durchführung.

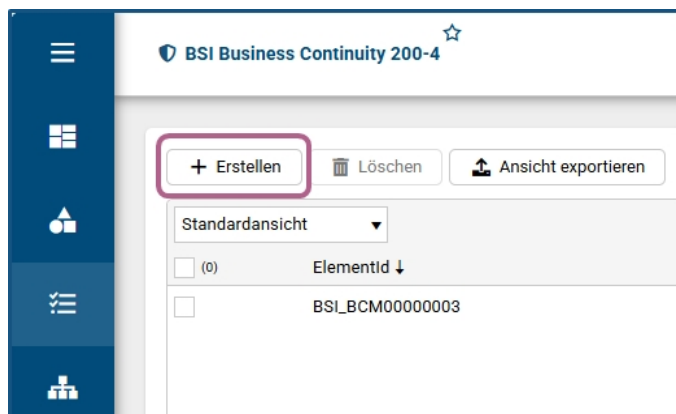
Folgende Tätigkeiten sollten vor der Erstellung des Assessments für ein spezifische Asset stattgefunden haben:

- [Asset Manager - Assets vorbereiten & pflegen](#)
- [Asset Manager - GRC Framework Elemente für Assessments vorbereiten & zuweisen](#)

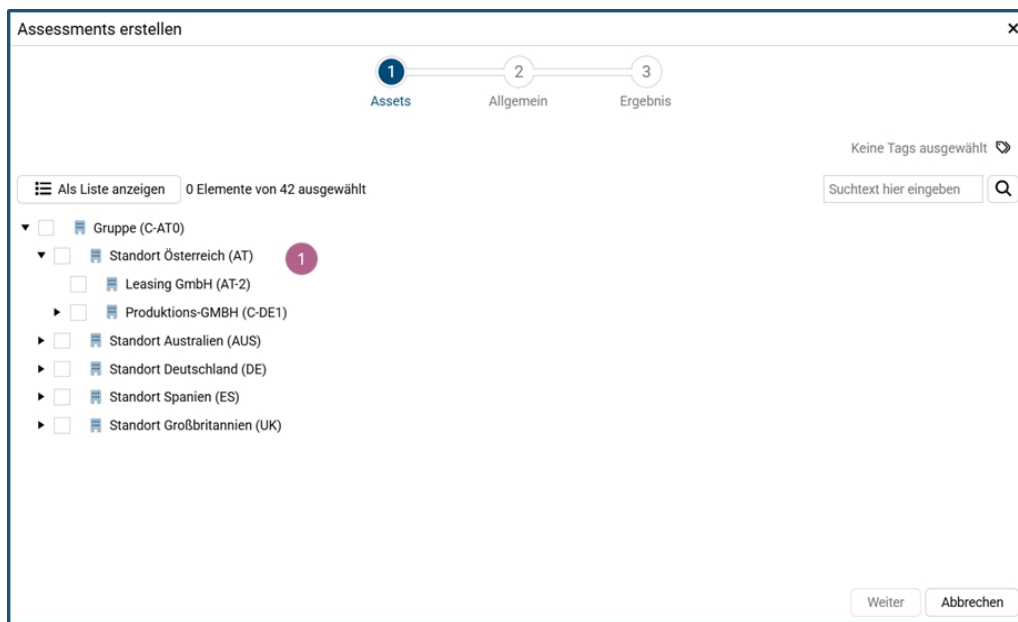
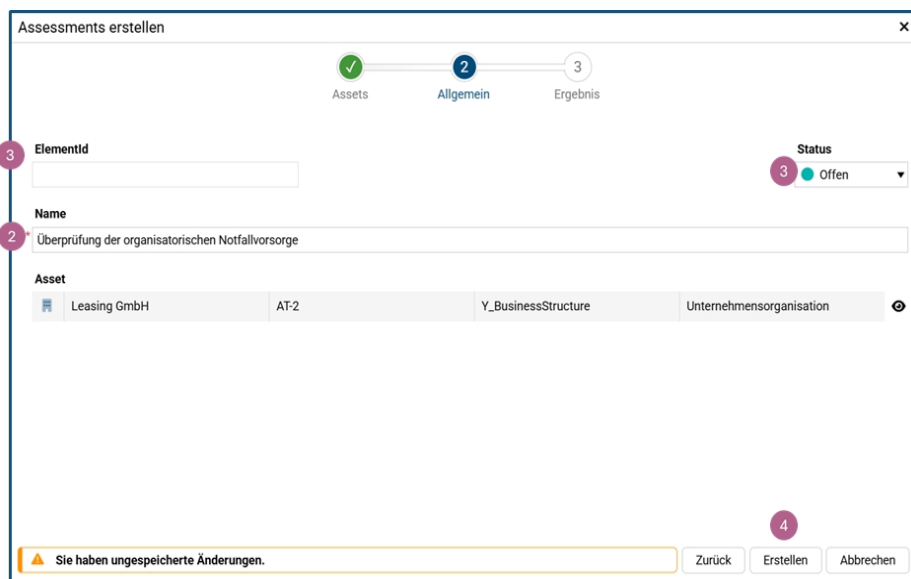
Schritt 1: Navigation zu Assessment

Der Assessor erstellt ein Assessment des Types "BSI Business Continuity 200- 4 IIA" über die Menüleiste **Assessments >> "Erstellen"** oder **Assets >> Auswahl einer Unternehmenseinheit oder Supporting Assets >> Links >> Öffnen des Reiters "BSI Business Continuity 200-4 IIA" >> "Erstellen"**.

Assessments dieses Typen können auf einem "Supporting Asset" oder 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 "BSI IT-Grundschutz" erstellen möchte.

Sobald ein Asset mittels einer Checkbox ausgewählt wurde kann zu dem nächsten Schritt navigiert werden.

Das Asset wird nach der Auswahl automatisch im Assessment verlinkt und kann nicht mehr geändert werden.

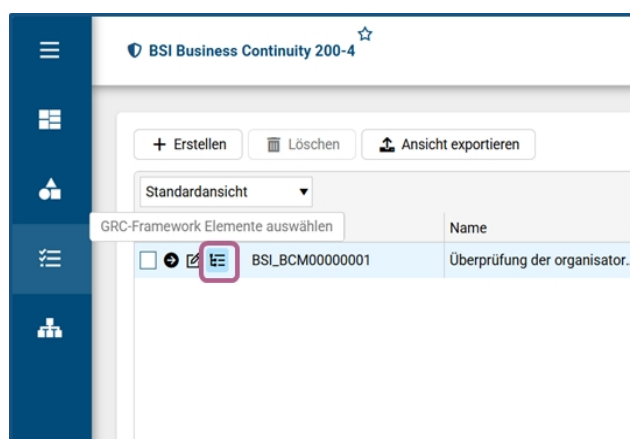
2 Name: Als nächster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Assessment* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist das *Assessment* einzigartig.

- 3 **Element ID und Status:** Die Element ID ist nicht bearbeitbar und setzt einen Wert nach dem "Erstellen" automatisch. Der Status ist und bleibt in "Bewertung" bis alle notwendigen Eingaben im Assessment gemacht wurden. Erst wenn alle Eingaben gemacht wurden kann der Status in "Abgeschlossen" gesetzt werden.
- 4 **Speichern:** Nachdem diese Eingaben gemacht wurden kann das Assessment erstellt 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 Angaben die im Assessment schon "Aktiviert" sind wurden am Asset bzw. Asset Typ angegeben von berechtigten Personen und anschließend für das Assessment automatisch freigeschalten.

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 "Kontroll-Assessment" auf Richtigkeit bzw. ob Ergänzungen zu der bisherigen Selektionen notwendig sind bevor er auf "Speichern" klickt.



Nach der Ergänzung durch den Assessor werden nicht nur die vom Asset übernommenen GRC Framework Elemente aktiviert, sondern auch die zusätzlich hinzuselektierten Elemente.

Sollte der Assessor später noch GRC Framework Elemente hinzufügen, wenn z.B. schon die Bewertung 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

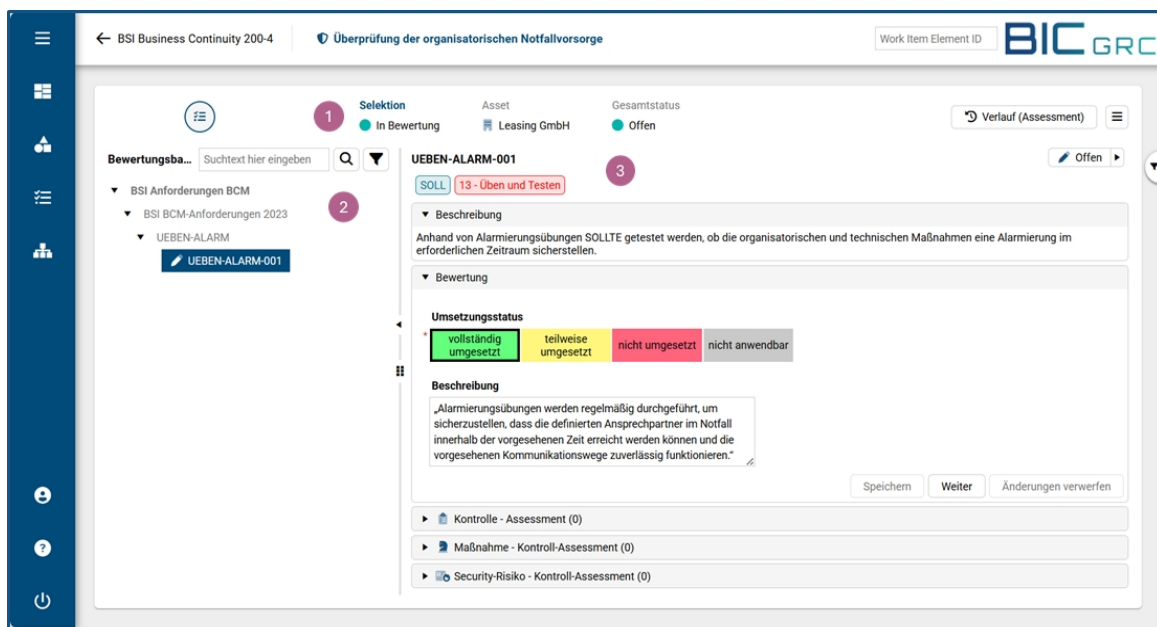
Nachdem das Assessment erstellt und die GRC Framework Elemente kontrolliert wurden kann das Assessment gestartet werden. Dafür klickt der Assessor auf das Icon .

Die weiteren Schritte findet der Assessor unter [Assessor - Bewertung durchführen & bewerten](#).

1.6.2 BSI Business Continuity 200-4 IIA - Bewertung durchführen & bewerten

Nachdem der Assessor das Assessment zu "BSI IT-Grundschutz" für ein bestimmtes Supporting Asset oder eine Organisationseinheit gestartet hat kann er die "Kontroll-Phase" starten.

Schritt 1: Übersicht über Assessment-Schirm



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

Der Assessor findet Basisinformation wie Status und Asset im oberen Bereich ¹.

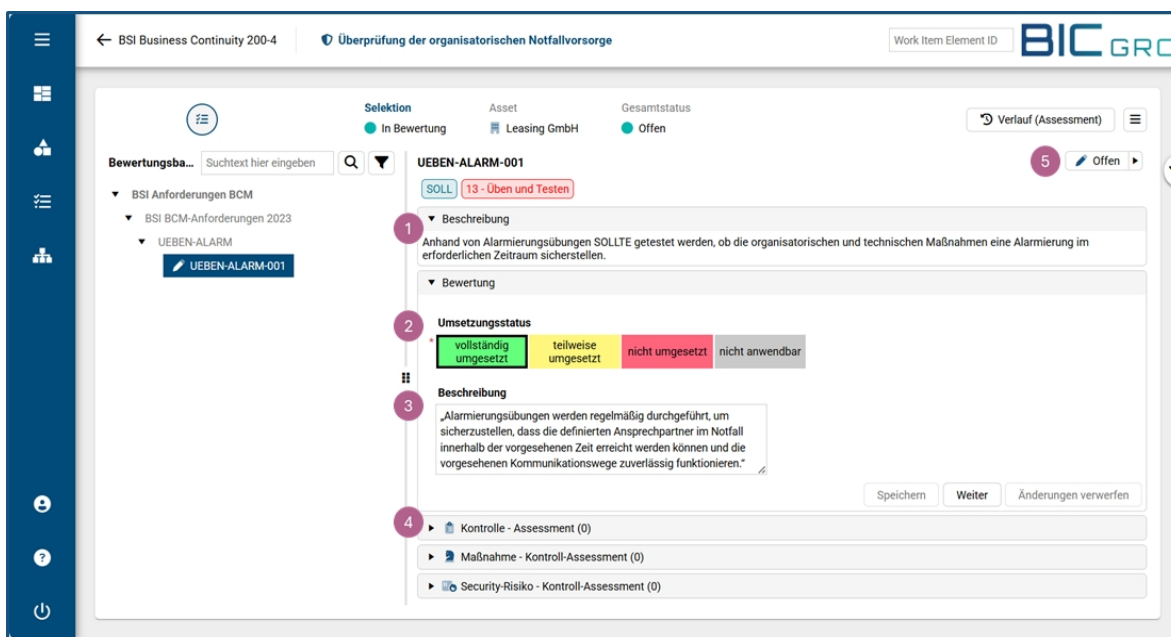
Auf der linken Seite des Fensters findet er den zu bewertenden GRC Framework ². Im Assessment zu "BSI Business Continuity 200-4 IIA" muss der Assessor alle aktivierten GRC Framework Elemente bewerten. Dabei kann der GRC Framework mittels Klick auf das Icon  geöffnet werden.

Der Assessor kann in der Bewertung zu dem GRC Framework "BSI Anforderungen BCM" nur die untersten Elemente des GRC Frameworks bewerten.

Zu bewertende GRC Framework Elemente haben das Icon , abgeschlossene GRC Framework Elemente das Icon .

Auf der rechten Seite des Fensters findet der Assessor die Hauptmaske ³, 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 "BSI Anforderungen BCM" 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 **Umsetzungsstatus:** Der "Umsetzungsstatus" soll widerspiegeln wie weit die Umsetzung einer bestimmten Anforderung, Maßnahme oder Aufgabe ist.

Sollte die Anforderung, Maßnahme oder Aufgabe noch nicht "vollständig umgesetzt", aber anwendbar sein, wird empfohlen ein Work Item *Security-Risiko* zu erstellen bzw. zu verlinken.

- 3 **Beschreibung:** Anschließend kann der Assessor noch eine zusätzliche Beschreibung hinterlegen.

- 4 **Zuordnungen:** Der Assessor kann im Rahmen der Bewertung die Erstellung bzw. die Zuordnungen zu folgenden Work Items machen:

- Kontrolle
- Maßnahme
- Security-Risiko

Security-Risiken können sich ergeben weil beispielsweise noch keine Umsetzung der Maßnahme stattgefunden hat.

Bei der Erstellung des *Security-Risikos* aus dem Assessment wird der Asset-Link automatisch befüllt.

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

Sobald der Statusübergang einer Bewertung abgeschlossen wurde kann die Bewertung nicht mehr verändert werden.

Nachdem alle Bewertungen auf der linken Seite des Fensters das Icon  haben, wechselt der Status der ganzen Phase automatisch in den Status "Abgeschlossen".

Weitere Schritte sind unter [Assessor - Assessment abschließen & auswerten](#) zu finden.

1.6.3 BSI Business Continuity 200-4 IIA - Assessment abschließen & auswerten

Nachdem der Assessor das Assessment zu "BSI Business Continuity 200-4 IIA" für ein bestimmtes Supporting Asset oder eine "Organisationseinheit" [gestartet](#) sowie die [Bewertung finalisiert](#) hat kann mit dem letzten Schritt begonnen werden - das Assessment abschließen.

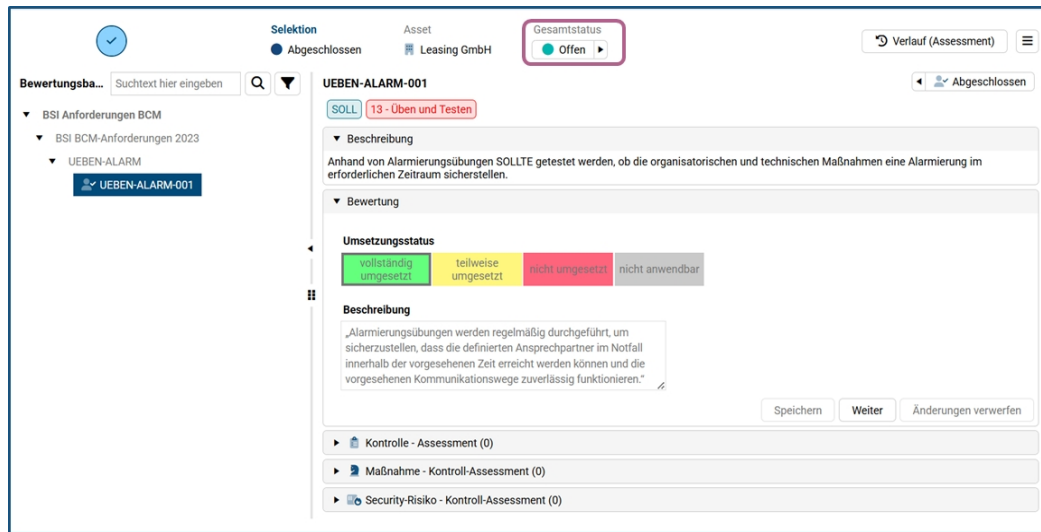
Schritt 1: Assessment abschließen

Um das Assessment abschließen zu können muss die ganze Phase des Assessments abgeschlossen sein.

Das Assessment schließen kann dabei nur der Assessor.

Das Assessment kann über zwei Wege abgeschlossen werden.

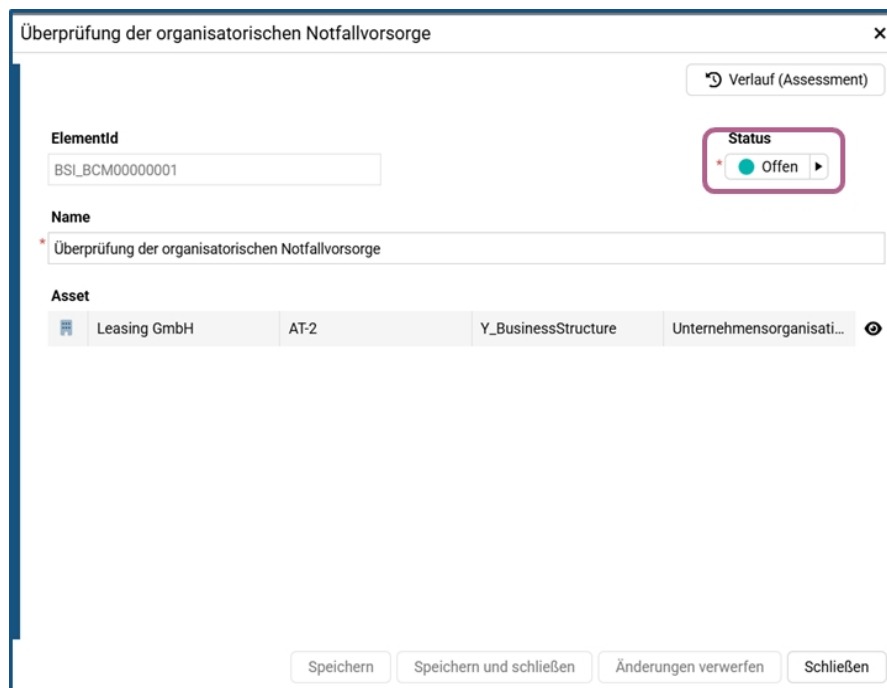
1. Abschluss in der Phase



Der Assessor kann direkt in der Phase einen Statuswechsel vornehmen.

Der Status wird nur angezeigt, wenn beide Phasen abgeschlossen sind. 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: Weiteres Vorgehen

Das Assessment kann jederzeit wieder geöffnet werden. Dafür kann der Assessor den Status wieder in "Bewertung" setzen (siehe oben Schritt 1). Anschließend muss manuell auch wieder die Phase geöffnet werden, um sie überprüfen zu können.

Der Assessor wird nicht automatisch informiert, wenn eine neue Bewertung erforderlich wäre.

1.7 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:

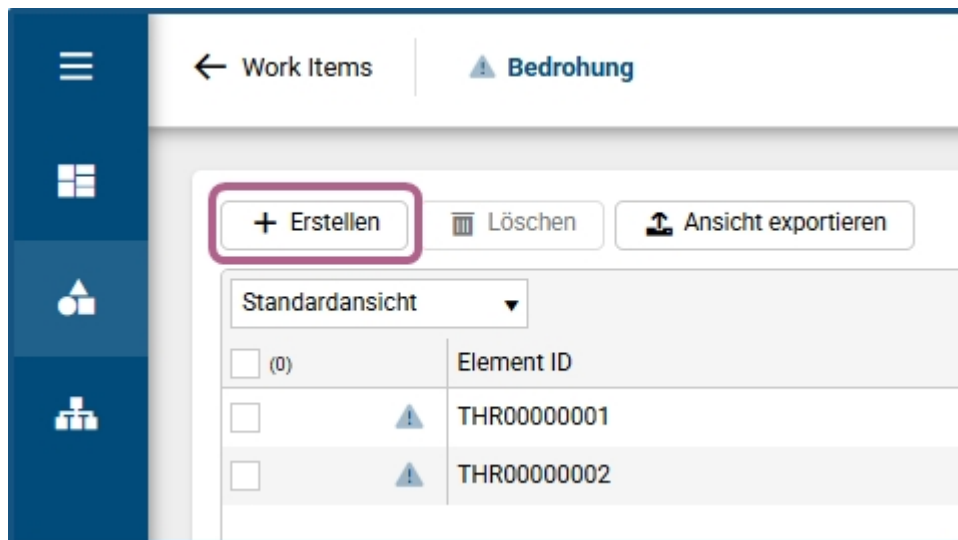
- [Security-Risk identifizieren & erstellen](#)
- [Security-Risiko ergänzen & analysieren](#)
- [Security-Risiko beurteilen & bewerten](#)
- [Maßnahmenbewertung ableiten & erstellen](#)
- [Maßnahmen identifizieren & erstellen](#)
- [Kontrolle ableiten & erstellen](#)
- [Ziel umsetzen & überprüfen](#)

1.7.1 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

Bedrohung Details

Status Entwurf

* Name **1** Cyberangriff auf IT-Dienstleister (z. B. Ransomware) (neutral)

Beschreibung Diskussion

Beschreibung der Bedrohung

2 **Bearbeiter**

* User Demo (ERM_DemoUser)

3 **Bedrohungstyp**

Beabsichtigte Bedrohung

4 **Beschreibung der Bedrohung**

Ein externer IT-Dienstleister, auf dessen Systeme das Unternehmen für zentrale digitale Services angewiesen ist, wird Ziel eines Cyberangriffs (z. B. Ransomware, DDoS, gezielte Sabotage). Dadurch kommt es zu teilweise oder vollständigem Ausfall der angebotenen Dienste und Infrastrukturen.

(290/5000)

4 **Beschreibung der Angriffsvektoren**

Kompromittierung von Admin-Zugängen beim Dienstleister
Einschleusung von Malware über Third-Party-Komponenten oder ungeschützte Schnittstellen
Distributed Denial of Service (DDoS) auf Hosting-Plattformen
Social Engineering (z. B. Phishing-Kampagnen auf Dienstleister-Mitarbeitende)

(284/5000)

4 **Beschreibung der Exploits**

Einsatz von Ransomware (z. B. LockBit, Cl0p) auf produktiven Systemen
Ausnutzung bekannter Schwachstellen (z. B. Log4j, Fortinet-Schwachstellen, Exchange Zero Days)
Umgehung von Authentifizierungsmechanismen über fehlerhafte API-Implementierung
Fehlende Segmentierung innerhalb der Systeme des Dienstleisters

(311/5000)

Sie haben ungespeicherte Änderungen. **6** Speichern Speichern und schließen Schließen

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.

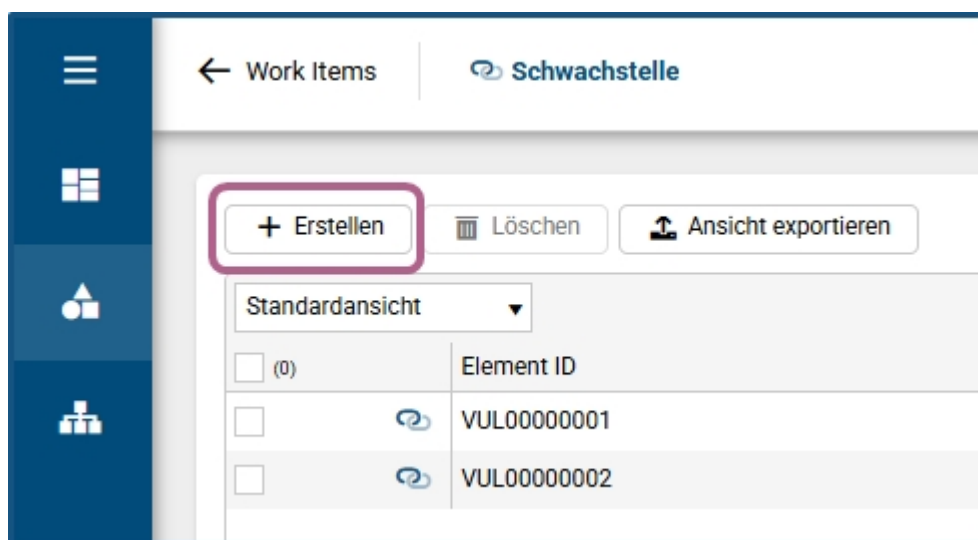
Es wird niemand über die Erstellung und "Aktivierung" der *Bedrohung* informiert.

1.7.2 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

Schwachstelle Details Weiter

Element ID: VUL00000002 Status: Entwurf

Name 1 Fehlende Sicherheits- und Resilienzanforderungen in Dienstleisterverträgen (neutral)

Beschreibung Diskussion Work Item Links Dokumentation (0)

Beschreibung der Schwachstelle

Bearbeiter 2
 * EditorRisk ERM (ERM_EditorRisk) 🔍

Beschreibung der Schwachstelle 3
 * Im bestehenden Vertrag mit dem IT-Dienstleister fehlen verbindliche Anforderungen hinsichtlich Sicherheitsmaßnahmen, Business Continuity, Patchmanagement und Meldepflichten im Schadensfall. Es gibt keine definierten SLAs zur Wiederherstellungszeit oder zur Integrität der übermittelten Daten. Eine Notfallstrategie für den Dienstleisterwechsel existiert nicht. (360/5000)

Beschreibung der Angriffsfläche 3
 Externe Hosting-Infrastruktur, auf der geschäftskritische Anwendungen betrieben werden
 Administrationsschnittstellen (z. B. Web-Portale, APIs) ohne zusätzliche Zugriffskontrolle
 Unzureichend kontrollierte Drittkomponenten, die über den Dienstleister betrieben werden
 Kundendatenbanken oder Konfigurationsdaten, die beim Dienstleister liegen (343/5000)

4 Dateien hierher ziehen zum Hochladen
 Keine Dokumente vorhanden. +

5 Speichern Speichern und schließen Schließen

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.

1.7.3 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"**.

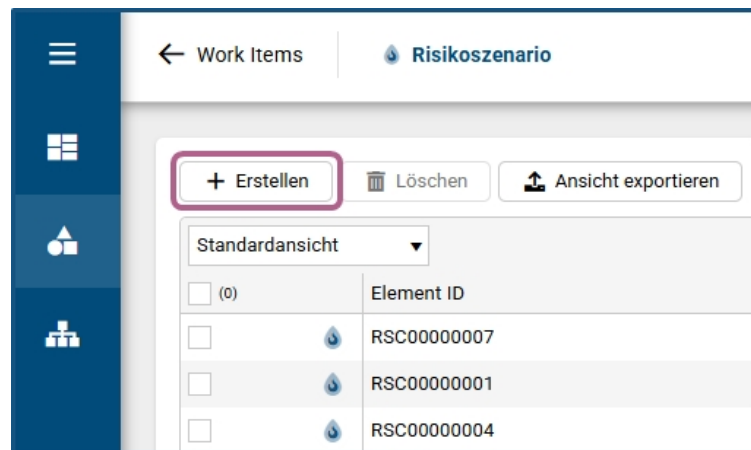


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung 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

Risikoszenario Details

Status: Erfassung

Name 1 Ausfall eines geschäftskritischen IT-Dienstleisters (neutral)

Übersicht

Szenarioübersicht

3 Betroffene Schutzziele

Vertraulichkeit X Integrität X Verfügbarkeit X

Auswählen...

2 GRC Perspektiven

Enterprise Risk Management X Internal Control X Information Security Management X

Privacy Management X Business Continuity Management X

Auswählen...

4 Szenariobeschreibung

Ein externer IT-Dienstleister, auf dessen Infrastruktur wesentliche Geschäftsfunktionen basieren, fällt unerwartet aus oder ist über einen längeren Zeitraum nicht leistungsfähig. Dies führt zu Beeinträchtigungen interner Prozesse und der digitalen Servicebereitstellung für Kunden oder Partner.

5 Ausfallszenarien

Name	Katalog	B...	
Ausfall von IT & Kommunikationssystemen	Ausfallszenarien		
Ausfall von Dienstleistern	Ausfallszenarien		

6 Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

- 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 freigeschalteten Modulen.

Es ist möglich, dass durch die Aktivierung unterschiedlicher Module ergänzende

Attribute angezeigt werden.

3

Betroffene Schutzziele: Der Bearbeiter kann drei Schutzziele festlegen:

- Vertraulichkeit: Schutz vor unbefugtem Zugriff auf Informationen.
- Integrität: Schutz vor unbemerkter oder unautorisierter Veränderung von Informationen.
- Verfügbarkeit: Sicherstellung, dass Informationen und Systeme bei Bedarf verfügbar sind.

4

Szenariobeschreibung: Das *Risikoszenario* sollte so ausführlich wie möglich dokumentiert und beschrieben werden, sodass auch andere Perspektiven einen Zusammenhang erkennen können.

5

Ausfallszenarien: Aus einem GRC Framework kann der Bearbeiter wählen, welche "Ausfallszenarien" zu erwarten sind.

6

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.

Risikoszenario Details

Weiter

Element ID

RSC00000003

Status

Erfassung

Name

Ausfall eines geschäftskritischen IT-Dienstleisters

(neutral)

Übersicht

Grundlage

Diskussion

Work Item Links

Dokumentation (0)

Risikoidentifikation

1

Verwendete Methoden

Name	Katalog	B...	
Business Impact Analyse	Identifikationsmethoden		

Alle zugeordneten Objekte anzeigen (3)

2

Andere Methoden

Interview und Risiko-Identifikationsmatrix (RIM)

3

Anlage

Dateien hierher ziehen zum Hochladen

Keine Dokumente vorhanden.

Risikoanalyse

4

Mögliche Ursachen

Unerwartete Insolvenz des Dienstleisters

Cyberangriff auf das Rechenzentrum oder den Applikationsbetrieb des Dienstleisters

Vertragswidrige Leistungsreduktion oder SLA-Verletzung

Risikoarten nach Herkunft

Name	Elementname	B...	
Technisches Risiko	RiskTypes.01origin.01		

Alle zugeordneten Objekte anzeigen (3)

Mögliche Auswirkungen

Eingeschränkter oder vollständiger Verlust digitaler Kundenzugänge

Reputationsschaden durch Unerreichbarkeit oder Datenprobleme

Verzögerung interner Prozessabläufe (z. B. Vertragsabschlüsse, Servicebearbeitung)

5

Risikoarten nach Auswirkung

Name	Elementname	B...	
Reputationsrisiko	RiskTypes.02impact....		

Sie haben ungespeicherte Änderungen.

Speichern

Speichern und schließen

Schließen

- 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*

GBTEC Austria GmbH

51/252

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 Benutzer 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 *Security-Risiko* übernommen werden. Die Informationen werden übernommen und angezeigt, wenn mittels der Konfiguration die Anzeige der Risikoanalyse im *Security-Risiko* erlaubt ist.

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

- einem Risikokatalog oder
- einer Bedrohung und einer Schwachstelle

angegeben werden.

Eines der beiden Anforderungen muss ausgefüllt sein, um das *Risikoszenario* in "Aktiv" schalten zu können.

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.

Risikoszenario Details

Weiter

Element ID

RSC00000003

Status

Erfassung

Name

Ausfall eines geschäftskritischen IT-Dienstleisters

(neutral)

Übersicht

Grundlage

Diskussion

Work Item Links

Dokumentation (0)

6 Risikohierleitung

Risikokatalog

Elementname	Name
BSI_IT_BaselineProtection.G11	G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen

Kontrollkatalog

Elementname	Name
BSIRequirementsGrundschatz.BSI.PB.OPS.01.01.01.A18_S	OPS.1.1.1.A18 Planung des Einsatzes von Dienstleistenden ...
BSIRequirementsGrundschatz.BSI.PB.OPS.03.02.A05_B	OPS.3.2.A5 Erstellung eines Sicherheitskonzepts für die Out...

Schwachstelle

Name	Status	B...
Fehlende Sicherheits- und Resilienzanforderungen in Dienstleisterverträgen	Aktiv	

Bedrohung

Name	Status	B...
Cyberangriff auf IT-Dienstleister (z. B. Ransomware)	Aktiv	

Sie haben ungespeicherte Änderungen.

7

Speichern

Speichern und schließen

Schließen

Schritt 4: Kontinuitätsstrategie hinterlegen

Sobald sich das *Risikoszenario* im Status "Aktiv" befindet, kann von einem Bearbeiter DS (nicht Bearbeiter Risiko) eine "Kontinuitätsstrategie" verlinkt werden.

Dabei ist das Work Item *Risikoszenario* der Ausgangspunkt für den weiteren Workflow für das Modul Business Continuity. Die nächsten Schritte sind unter [Bearbeiter_DS_-_Kontinuitätsstrategie herleiten & erstellen](#) zu finden.

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.

1.7.4 Ziel definieren & erstellen

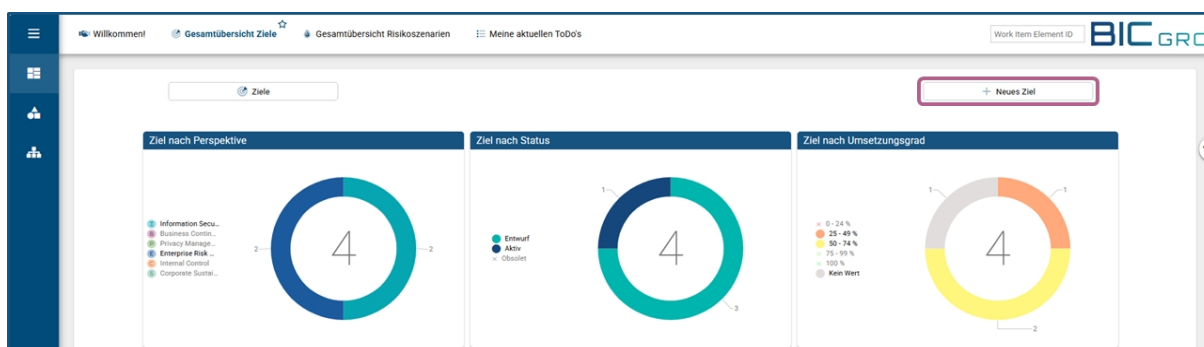
In BIC GRC ist es möglich *Ziele* zu definieren und in unterschiedlichen Kontexten zu verknüpfen. Hierzu kann der Bearbeiter Risiko das Work Item *Ziel* erstellen.

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 Security-Risiko

Der Bearbeiter Risiko kann aus dem *Security-Risiko* 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.

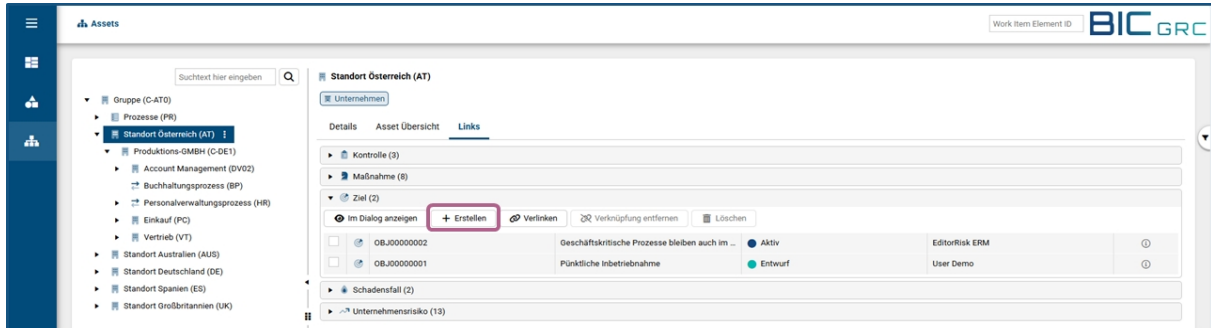


Ein neues Fenster öffnet sich anschließend automatisch.

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.

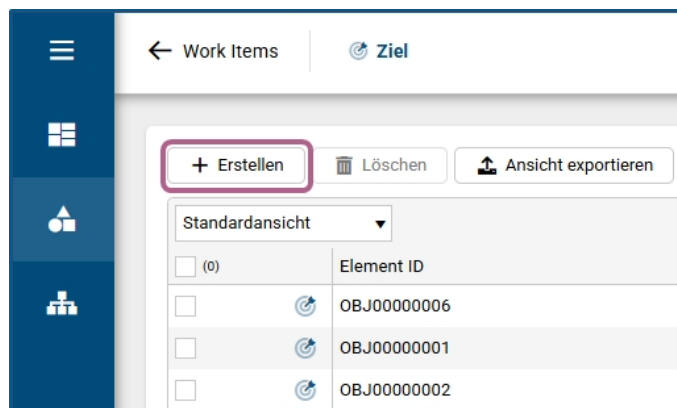


Ein neues Fenster öffnet sich anschließend automatisch.

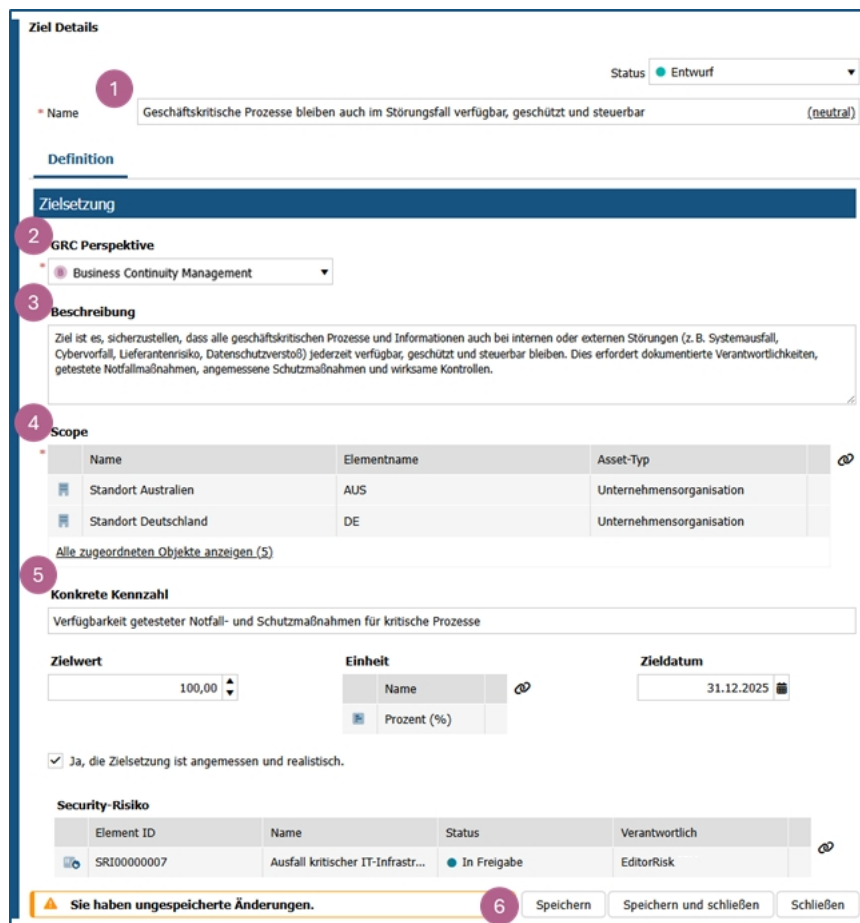
4. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Zielsetzung definieren



Ziel Details

Status: Entwurf

1 **Name**: Geschäftskritische Prozesse bleiben auch im Störfall verfügbar, geschützt und steuerbar (neutral)

Definition

Zielsetzung

2 **GRC Perspektive**: Business Continuity Management

3 **Beschreibung**: Ziel ist es, sicherzustellen, dass alle geschäftskritischen Prozesse und Informationen auch bei internen oder externen Störungen (z. B. Systemausfall, Cybervorfall, Lieferantenrisiko, Datenschutzverstoß) jederzeit verfügbar, geschützt und steuerbar bleiben. Dies erfordert dokumentierte Verantwortlichkeiten, getestete Notfallmaßnahmen, angemessene Schutzmaßnahmen und wirksame Kontrollen.

4 **Scope**

Name	Elementname	Asset-Typ
Standort Australien	AUS	Unternehmensorganisation
Standort Deutschland	DE	Unternehmensorganisation

Alle zugeordneten Objekte anzeigen (5)

5 **Konkrete Kennzahl**

Verfügbarkeit getesteter Notfall- und Schutzmaßnahmen für kritische Prozesse

Zielwert: 100,00 **Einheit**: Prozent (%) **Zieldatum**: 31.12.2025

☒ Ja, die Zielsetzung ist angemessen und realistisch.

Security-Risiko

Element ID	Name	Status	Verantwortlich
SR100000007	Ausfall kritischer IT-Infrastr...	In Freigabe	EditorRisk

6 **Bottom Buttons**: Sie haben ungespeicherte Änderungen. Speichern, Speichern und schließen, Schließen

- 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 freigeschalteten 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 konkreten "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 "Zielfadens" 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

Ziel Details

6
Weiter

Element ID: OBJ00000002

Status: ● Entwurf

* Name: Geschäftskritische Prozesse bleiben auch im Störfall verfügbar, geschützt und steuerbar (neutral)

1
 * Überprüfungszyklus: ● Zu einem bestimmten Datum

* Nächste Überprüfung: 15.08.2025

Definition
Überprüfung
Diskussion
Work Item Links
Dokumentation (0)

2
Zwischenziele

R...	Name	Status	Aktuell...	B...
1	Kritische Prozesse sind dokumentiert, bewertet und notfallfähig abgesich...	● Aktiv	50 %	

3
Annahmen & Methode

Die Zielerreichung basiert auf einer systematischen Erhebung aller geschäftskritischen Prozesse, ihrer Bewertung nach Schutzbedarf (Verfügbarkeit, Vertraulichkeit, Integrität) sowie der Bewertung vorhandener Maßnahmen aus Sicht BCM, ISMS, Datenschutz, IKS und Risiko. Die Erfüllung wird anhand eines Zielprozesskatalogs mit definierter Kennzahl gemessen (z. B. Schutzabdeckung, getestete Notfallpläne).

4
Dokumentierte Information

Keine Zuordnung vorhanden.

4
Strategische Maßnahmen

Name	Status	B...
regelmäßige Ausfalltests	● Entwurf	

4
Kontrolle

Name	Status	B...
Regelmäßiger Notfalltest mit dem IT-Dienstleister	● Planung	

5
Mögliche Risiken

Unternehmensrisiko

Element ID	Name	Status	Verantwortlich
RSK00000016	Ausfall eines geschäftskri...	● Nettobewertung	EditorRisk ERM

Speichern
Speichern und schließen
Schließen

- 1 **Überprüfungszyklus:** Der Bearbeiter muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft ein *Ziel* zurück in den Status "Entwurf" geschaltet 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" geschaltet 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.

1.7.5 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

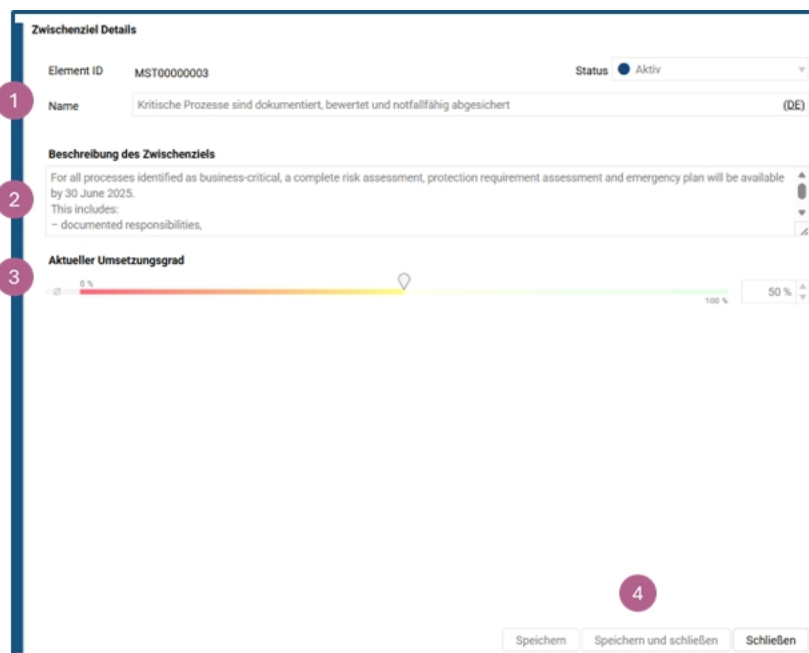
Ein *Zwischenziel* kann nur mittels Erstellung aus dem Work Item *Ziel* durch den verantwortlichen Bearbeiter erfolgen.

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

Zwischenziele					
R...	Name	Status	Aktuell...	B...	
1	Kritische Prozesse sind dokumentiert, bewertet und notfallfähig abgesichert	Aktiv	20 %		

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

Schritt 2: Zwischenziel definieren



Zwischenziel Details

Element ID: MST00000003 Status: Aktiv

1 **Name:** Kritische Prozesse sind dokumentiert, bewertet und notfallfähig abgesichert (DE)

2 **Beschreibung des Zwischenziels:**
For all processes identified as business-critical, a complete risk assessment, protection requirement assessment and emergency plan will be available by 30 June 2025.
This includes:
- documented responsibilities,

3 **Aktueller Umsetzungsgrad:** 0 % to 100 % (Slider at 20 %)

4 **Buttons:** Speichern, Speichern und schließen, Schließen

- 1 Name:** Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für das *Zwischenzielerfolg*en.
- 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.

1.7.6 Security-Risiko identifizieren & erstellen

Nachdem ein Risiko in der Domäne Business Continuity identifiziert wurde, kann ein neues Work Item *Security-Risiko* vom Bearbeiter Risiko erstellt werden.

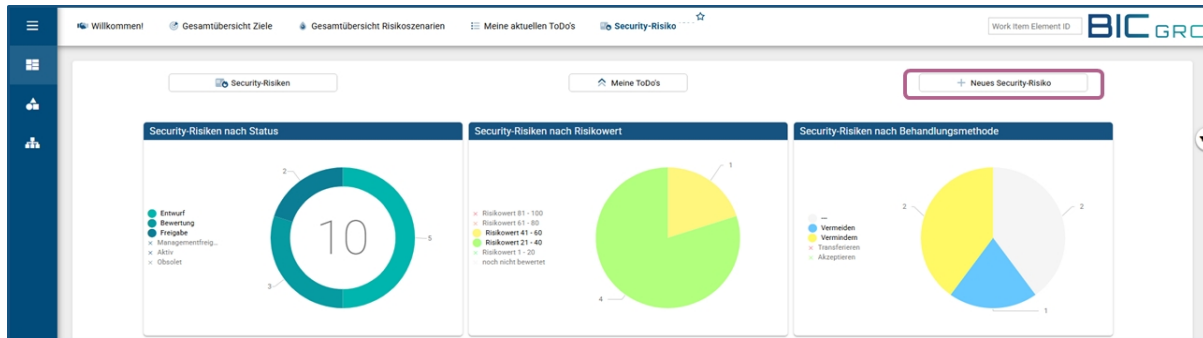
Schritt 1: Security-Risiko erstellen

Der Bearbeiter kann in BIC GRC an mehreren Stellen *Security-Risiken* erstellen.

1. Erstellen über Dashboard "Security-Risiko"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Security-Risiko BCM >> "Neues Security-Risiko"**

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

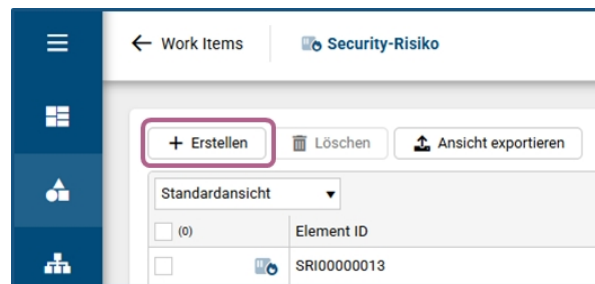


Ein neues Fenster öffnet sich anschließend automatisch.

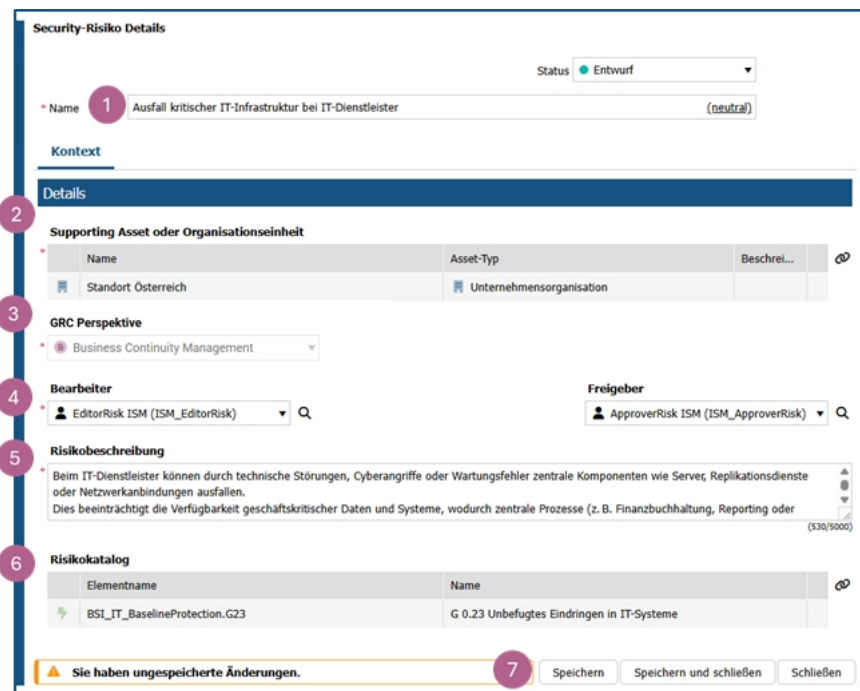
2. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen



The screenshot shows the 'Security-Risiko Details' form with the following steps highlighted:

- Name:** The 'Name' field is highlighted with a red circle. The value is 'Ausfall kritischer IT-Infrastruktur bei IT-Dienstleister'.
- Kontext:** The 'Kontext' section is highlighted with a red circle.
- Supporting Asset oder Organisationseinheit:** The 'Supporting Asset oder Organisationseinheit' table is highlighted with a red circle. It contains one row with 'Standort Österreich' and 'Unternehmensorganisation'.
- GRC Perspektive:** The 'GRC Perspektive' dropdown is highlighted with a red circle. The value is 'Business Continuity Management'.
- Bearbeiter:** The 'Bearbeiter' dropdown is highlighted with a red circle. The value is 'EditorRisk ISM (ISM_EditorRisk)'.
- Freigeber:** The 'Freigeber' dropdown is highlighted with a red circle. The value is 'ApproverRisk ISM (ISM_ApproverRisk)'.
- Risikobeschreibung:** The 'Risikobeschreibung' field is highlighted with a red circle. The value is 'Beim IT-Dienstleister können durch technische Störungen, Cyberangriffe oder Wartungsfehler zentrale Komponenten wie Server, Replikationsdienste oder Netzverbindungen ausfallen. Dies beeinträchtigt die Verfügbarkeit geschäftskritischer Daten und Systeme, wodurch zentrale Prozesse (z. B. Finanzbuchhaltung, Reporting oder (530/5000))'.
- Risikokatalog:** The 'Risikokatalog' table is highlighted with a red circle. It contains one row with 'BSI_TT_BaselineProtection.G23' and 'G 0.23 Unbefugtes Eindringen in IT-Systeme'.

At the bottom, there is a warning message: 'Sie haben ungespeicherte Änderungen.' and buttons for 'Speichern', 'Speichern und schließen', and 'Schließen'.

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

2 **Asset-Zuordnung:** Der Bearbeiter Risiko kann an dieser Stelle entweder ein "Supporting Asset" oder eine "Organisationseinheit" wählen.

Wird das *Security-Risiko* über "2. Erstellen über Asset Übersicht Links" erstellt, wird der Link zum Asset automatisch gesetzt von BIC GRC.

Assets des Typen "Primary Asset" werden von BIC GRC nicht unterstützt. Der Benutzer wird eine Fehlermeldung beim ersten Speicherversuch bekommen, sollte ein "Primary Asset" hinterlegt 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](#).

3

GRC Perspektive: Dadurch bedingt, dass sich das *Security-Risiko* aus drei Perspektiven - Informationssicherheit, Datenschutz und Business Continuity - ergeben kann, muss der Bearbeiter Risiko angeben aus welcher Perspektive das Risiko entstanden ist.

Das *Security-Risiko* wird bei Aktivierung der anderen Module auch anderen Perspektiven angezeigt und kann verlinkt werden. Die ursprüngliche Perspektive eines *Security-Risikos* kann allerdings nicht mehr verändert werden.

Um es dem Bearbeiter zu erleichtern, die richtige Perspektive auszuwählen, gibt es im Hintergrund einen Filter die sein Benutzerprofil an dem Asset identifiziert. Abhängig von den Berechtigungen können dem Bearbeiter somit ein oder mehrere Perspektiven angezeigt werden, für dass das *Security-Risiko* erstellt werden soll.

4

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

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

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

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

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 *Security-Risiko* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

5 Risikobeschreibung: Anschließend ist eine Beschreibung des *Security-Risikos* zu hinterlegen, wobei auch Informationen zu Ursache und Wirkung interessant sein können. Alle User, die im Workflow des *Security-Risikos* nachgelagert sind, orientieren sich an dieser Beschreibung, daher sollte sie so viele notwendige Informationen und Daten wie möglich enthalten.

6 Risikokatalog: Zusätzlich muss eine Zuordnung zu einer Kategorie des "Risikokatalogs" vorgenommen werden.

Der Risikokatalog führt zu den GRC Frameworks von "BSI - Elementare Gefährdungen" und "Generische Risiken"

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

Der Bearbeiter kann anschließend mit dem nächsten Schritt [Security-Risiko ergänzen & analysieren](#) fortfahren.

1.7.7 Security-Risiko ergänzen & analysieren

Ein *Security-Risiko* 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 *Security-Risiko* informiert. Die folgenden Schritte 1 & 2 beziehen sich auf die Schritte nach der Erstellung durch einen anderen Benutzer.

Optional Schritt 1: Navigation zu spezifischem Security-Risiko nach Fremderstellung

Der Bearbeiter hat zwei Möglichkeiten, ein zu bearbeitendes *Security-Risiko* 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 *Security-Risiko* befindet sich in der Notifikation.

Security-Risiko wurde angelegt

Werter User,

das Work Item "Ausfall kritischer IT-Infrastruktur bei IT-Dienstleister" wurde angelegt.

Element ID:	SRI00000008
Status:	Entwurf

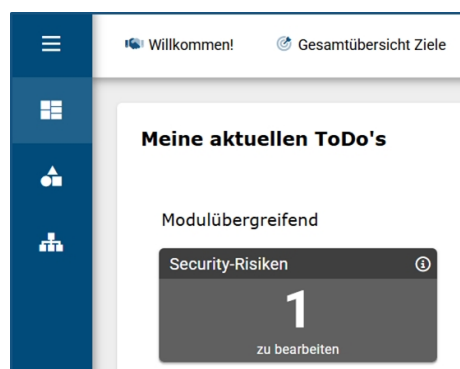
Diese Nachricht dient nur zur Information und impliziert keinen Handlungsbedarf.

Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

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.

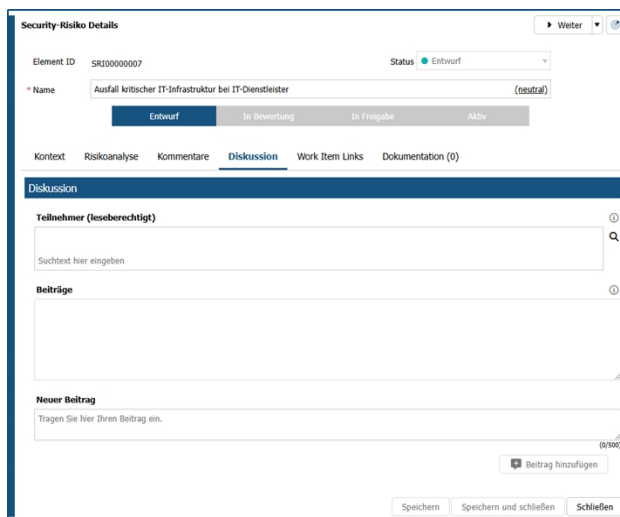


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Security-Risiko* automatisch. Der Bearbeiter steigt direkt in den Tab "*Kontext*" des *Security-Risikos* ein.

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 *Security-Risiko* zu dem Tab "*Kontext*" zu gehen, um die Detailsangaben 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.

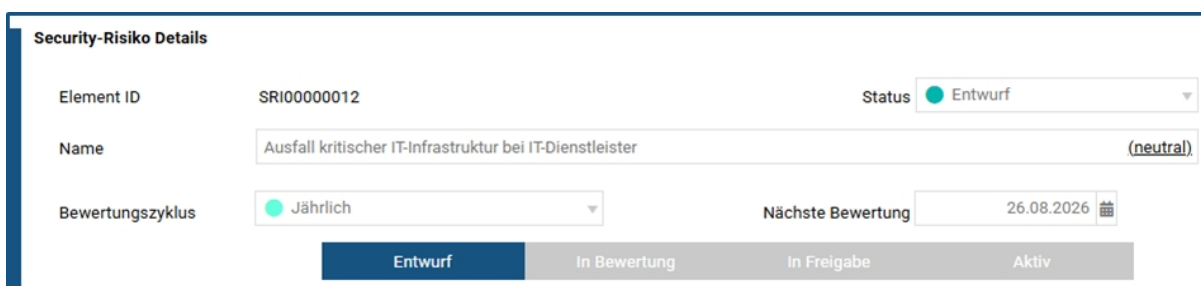


Schritt 3: Zuordnung finalisieren

Der Bearbeiter sollte das *Security-Risiko* regelmäßig dahingehend überprüfen, ob das *Security-Risiko* 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.

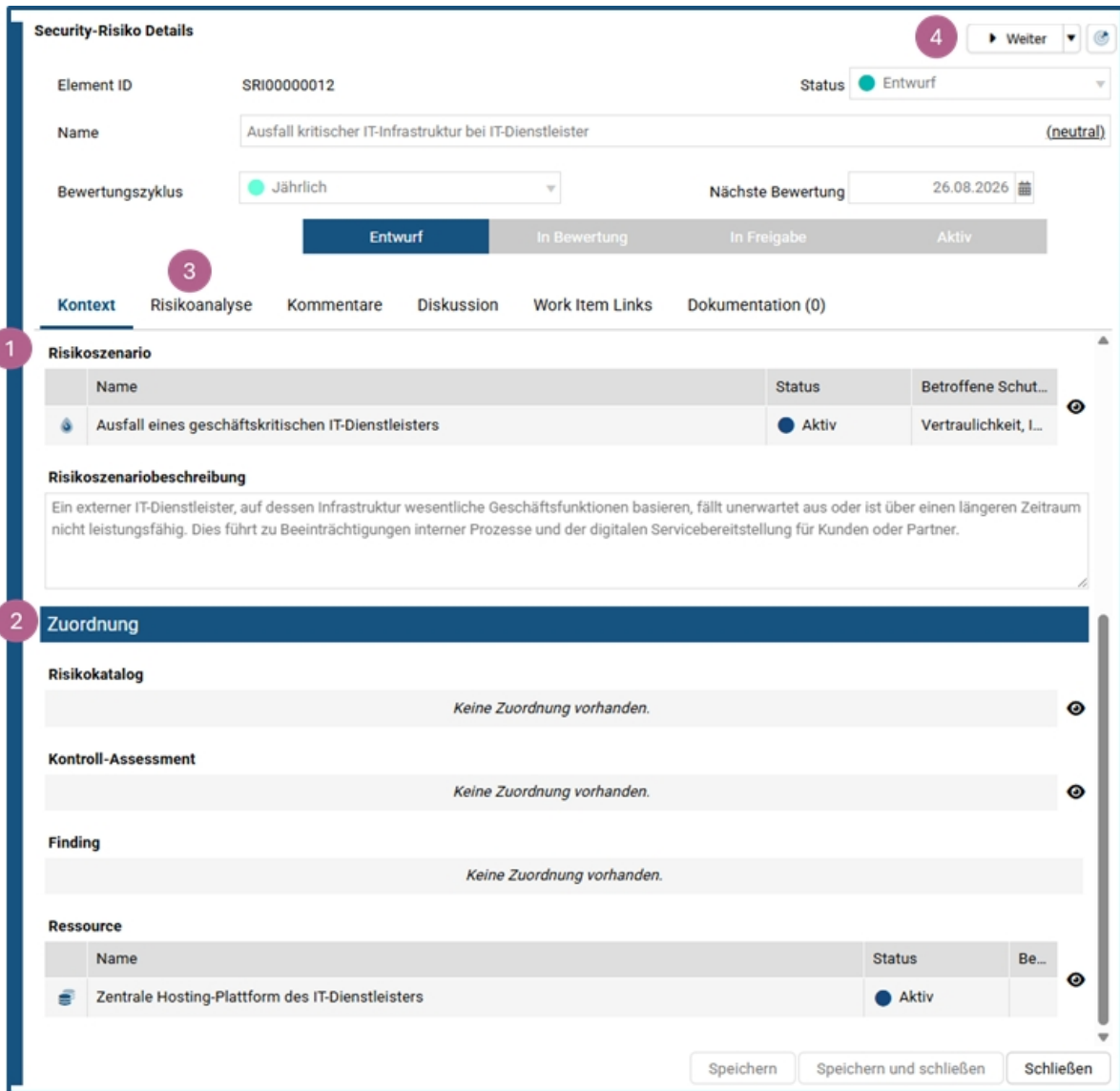
An dem Tag der "Nächsten Bewertung" wird das *Security-Risiko* im Status "Aktiv" in den Status "Bewertung" geschaltet und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.



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

Wenn das *Security-Risiko* 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 4: Eingaben ergänzen



- 1 **Risikoszenario:** Wird das *Security-Risiko* 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.

Wird ein *Risikoszenario* verlinkt, wird dem Bearbeiter unter dem "Risikoszenario"-Link ein zusätzliches Beschreibungsfeld eingeblendet, dass eine vom *Risikoszenario* übernommen Risikoszenariobeschreibung beinhaltet.

Es ist nicht vorgesehen *Risikoszenarien* aus einem *Security-Risiko* zu erstellen. *Risikoszenarien* sollten schon feststehen.

Für die Zuordnung von *Risikoszenarien* wurde ein Filter hinterlegt, sodass dem Bearbeiter Risiko nur *Risikoszenarien* angezeigt werden, die eine passende Perspektive aufweisen und sich im Status "Aktiv" befinden.

- 2 **Zuordnung:** Der Bearbeiter kann Verlinkungen zu weiteren Work Items bzw. Assessments durchführen.

Normalerweise werden diese Verlinkungen von alleine gesetzt, wenn die Erstellung des *Security-Risikos* durch eine der unten stehenden Work Items bzw. Assessments erfolgt.

- **Kontroll- Assessment:** Der Link zu einem spezifischem Assessment wird automatisch ausgefüllt von BIC GRC, wenn das *Security-Risiko* aus einem passenden Assessment erstellt wurde. Sollte das *Security-Risiko* schon vor dem Assessment bestehen kann das "Kontroll-Assesement" im Nachgang verlinkt werden.
- **Finding:** Sollten *Findings* zu einem *Security-Risiko* führen können diese hier verlinkt werden.

Dem Bearbeiter werden nur *Findings* angezeigt die sich im Status "Behandlung" oder "Abgeschlossen" befinden.

- **Vorfall:** Ein *Security-Risiko* kann aus einem *Vorfall* resultieren. Im *Vorfall* gibt es einen Button "Security-Risiko erstellen" für diesen Fall. Der Link im *Security-Risiko* zu einem *Vorfall* wird anschließend automatisch von BIC GRC mit dem passenden *Vorfall* befüllt.

Sollte der Bearbeiter einen *Vorfall* verlinken, werden nur *Vorfälle* angezeigt die sich zumindest im Status "Gemeldet" oder weiter befinden.

- **Ressource:** Der Bearbeiter sollte *Ressourcen* verlinken, wenn es eine Abhängigkeit zwischen dem *Security-Risiko* und der *Ressource* im Business Continuity Kontext gibt.

Dem Bearbeiter werden nur *Ressourcen* angezeigt die sich im Status "Aktiv" befinden.

Es ist nicht vorgesehen, dass Kontroll-Assessments, *Findings*, *Ressource* oder *Vorfälle* aus dem *Security-Risiko* erstellt werden, sondern es wird nur eine Verlinkung von BIC GRC erlaubt.

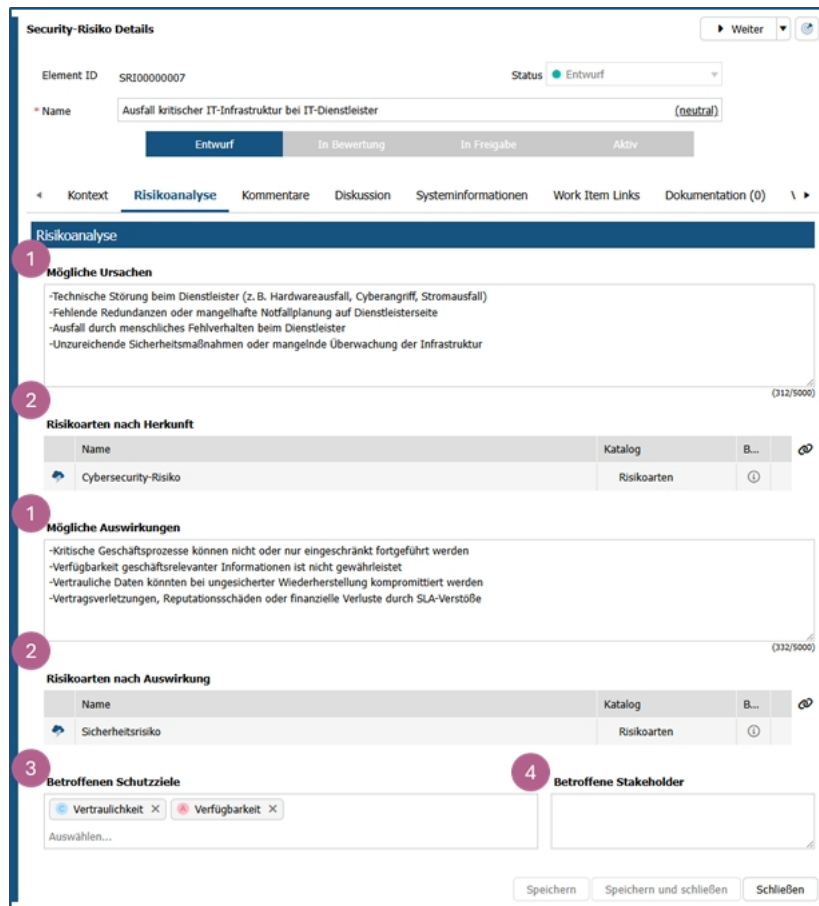
- 3 Optional Schritt 4 - **Risikoanalyse** - beachten

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

Der Bearbeiter kann anschließend mit dem nächsten Schritt [Security-Risiko beurteilen & bewerten](#) fortfahren.

Optional - Schritt 5: 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 *Security-Risiken* einzustellen.



1 **Mögliche Ursache bzw. Auswirkung:** Um das *Security-Risiko* 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 *Security-Risikos* vorzunehmen.

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 *Security-Risiko* schon eine Verlinkung vorgenommen, werden die bestehenden Eingaben von "Risikoart nach Herkunft" und "Risikoart nach Auswirkung" nicht überschrieben.

- 3 **Betroffene Schutzziele:** Dieses Listenattribut gibt dem Bearbeiter die Möglichkeit auf dem Security-Risiko CIA-Werte (Vertraulichkeit, Integrität, Verfügbarkeit) zu hinterlegen.

Diese Information wird nicht aus dem *Risikoszenario* übernommen.

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

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

1.7.8 Security-Risiko beurteilen & bewerten

Ein *Security-Risiko* wird von einem Ersteller identifiziert & erstellt und von einem Bearbeiter Risiko ergänzt & analysiert.

Schritt 1: Bewertung durchführen

Sobald sich das *Security-Risiko* im Status "Bewertung" befindet, kann mit der Bewertung des *Security-Risiko* in dem Tab "Bruttbewertung" 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:

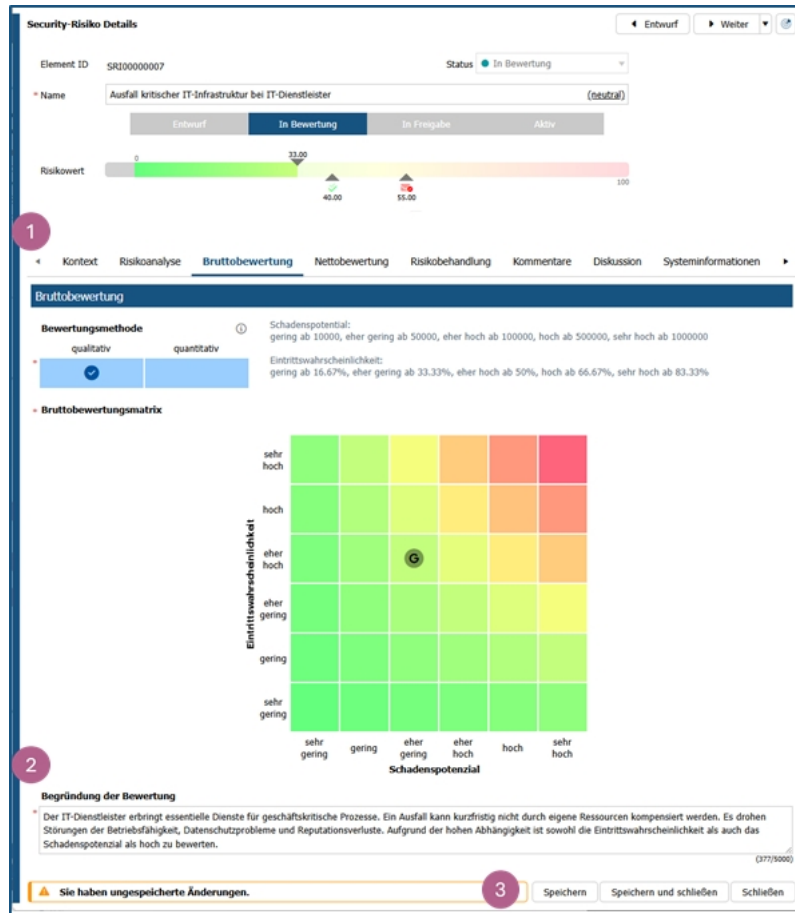
- (a) Qualitativ
- (b) Quantitativ



Im Sinne der Lesbarkeit werden "Schritt 2: Bruttbewertung durchführen", "Schritt 3: Soll-Bewertung durchführen" und "Schritt 4: Ist-Bewertung 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 **Bruttobewertung:** Der Bearbeiter hinterlegt per Klick in der Heatmap ein Icon (G), in dessen Wertebereich sich das *Security-Risiko* seiner Meinung nach ohne Steuerung, also ohne *Maßnahme*, befindet.
- 2 **Begründung:** Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu dieser Bewertung gekommen ist.
- 3 **Speichern:** Sobald die Informationen angegeben sind kann der Bearbeiter Risiko speichern.

Sobald der Bearbeiter gespeichert hat wird ihm ein weiterer Tab "Nettobewertung" angezeigt. Zu diesem muss er für den nächsten Schritt navigieren.

Schritt 3a: Qualitative Soll-Bewertung durchführen

Security-Risiko Details

Entwurf

Weiter

Element ID

SRJ00000007

Status

In Bewertung

Name

Ausfall kritischer IT-Infrastruktur bei IT-Dienstleister (neutral)

Entwurf

In Bewertung

In Freigabe

Aktiv

Risikowert

0

33.00

40.00

55.00

100

Kontext

Risikoanalyse

Bruttobewertung

Nettobewertung

Risikobehandlung

Kommentare

Diskussion

Systeminformationen

Nettobewertung

sehr hoch

hoch

eher hoch

eher gering

gering

sehr gering

sehr gering

gering

eher gering

eher hoch

hoch

sehr hoch

Eintrittswahrscheinlichkeit

Schadenspotenzial

1

2

Soll-Bewertung

Ist-Bewertung

Begründung der Soll-Bewertung

Ziel der geplanten Maßnahme ist es, durch Redundanzen, Verträge mit Ausfallregelungen und regelmäßige Tests mit dem Dienstleister die Eintrittswahrscheinlichkeit deutlich zu reduzieren. Ein Restrisiko durch das Schadenspotenzial bleibt bestehen, falls ein Ausfall dennoch eintritt.

281/5

Speichern

Speichern und schließen

Schließen

GBTEC Austria GmbH

73/252

Security-Risiko Details Entwurf Weiter ↺ ↻

Element ID: SRI00000007 Status: In Bewertung

* Name: (neutral)

Entwurf **In Bewertung** In Freigabe Aktiv

Risikowert: 0 33.00 40.00 55.00 100

◀ Kontext Risikoanalyse Bruttobewertung Nettobewertung **Risikobehandlung** Kommentare Diskussion System ▶

Risikobehandlung

3 **Behandlungsmethode** ⓘ

Vermeiden **Vermindern** Transferieren Akzeptieren

4 **Mitigierende Kontrollen**

Name	Status	B...	
Regelmäßiger Notfalltest mit dem IT-Dienstleister	Aktiv	ⓘ	+

5 **Mitigierende Maßnahmen**

Name	Status	B...	
Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister	Bewertet	ⓘ	+

⚠ Sie haben ungespeicherte Änderungen. 6 Speichern Speichern und schließen Schließen

- 1 **Soll-Bewertung:** Dem Bearbeiter wird erneut eine Heatmap angezeigt, wo er zwei Icons für Soll-Bewertung (T) und Ist-Bewertung (C) angibt.

Sobald der Bearbeiter Risiko das Soll-Bewertung Icon (T) in der Heatmap gesetzt hat, wird im ein weiterer Tab "Risikobehandlung" angezeigt.

- 2 **Begründung der Soll-Bewertung:** Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu diesem Zielwert gekommen ist.

- 3 **Risikosteuerung:** Nun wechselt der Bearbeiter in den Tab "Risikobehandlung".
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. Verlagerung von IT-Systemen in zertifizierte Rechenzentren mit hoher Ausfallsicherheit.
- Vermindern: Das Risiko wird durch Maßnahmen vermindert, die sowohl auf die Ursache als auch auf die Wirkung Einfluss nehmen, z.B. Aufbau redundanter Netzwerkverbindungen für kritische Standorte.
- 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 Security-Risiko effizient oder effektiv vermeiden, vermindern oder transferieren, muss das Restrisiko akzeptiert werden.

Der Bearbeiter kann ein *Security-Risiko* 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.

- 4 **Mitigierende Kontrollen:** Der Bearbeiter sollte "Mitigierende Kontrollen" [ableiten & erstellen](#) oder verlinken, wenn er die Behandlungsmethode "Vermindern" oder "Transferieren" auswählt.

Der Bearbeiter kann nur Kontrollen verlinken, die sich nicht im Status "Inaktiv" oder "Obsolet" befinden.

- 5 **Mitigierende Maßnahmen:** Der Bearbeiter sollte "Mitigierende Maßnahmen" [ableiten & erstellen](#), wenn er die Behandlungsmethode "Vermindern" oder "Transferieren" auswählt. Um den tatsächlichen Einfluss einer Maßnahme auf ein *Security-Risiko* abzubilden, hat der Bearbeiter Risiko eine *Maßnahmenbewertung* zu erstellen.

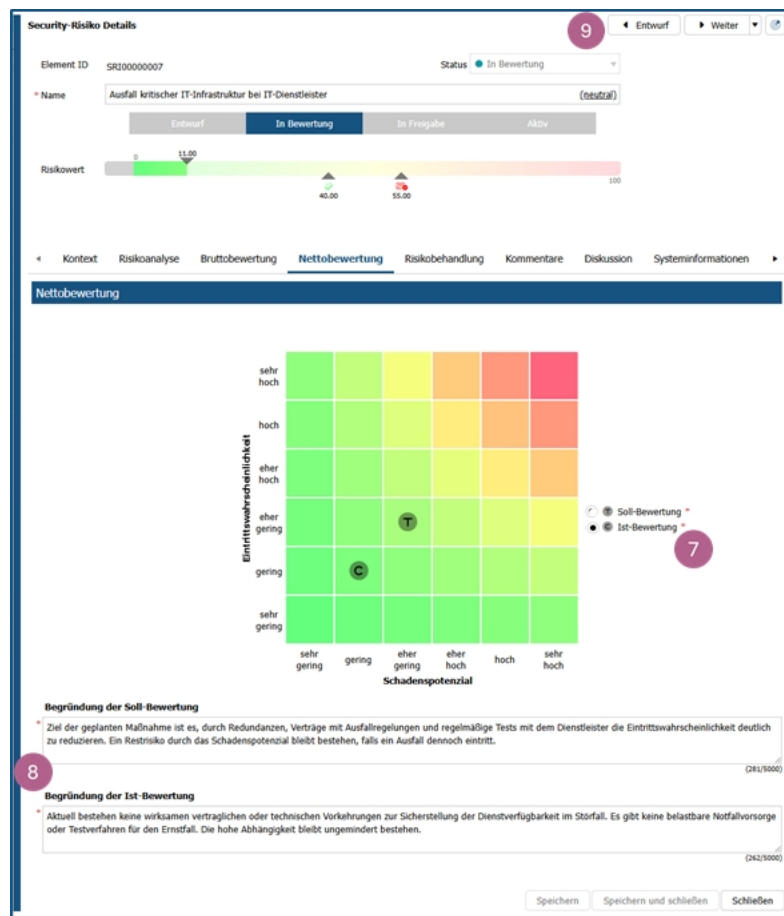
Ein Verlinkung ist nicht möglich.

Für die Mitigation des *Security-Risiko* können mehrere *Maßnahmenbewertungen* aus dem *Security-Risiko* heraus erstellt werden.

- 6 **Speichern:** Sobald die Informationen angegeben sind, kann der Bearbeiter Risiko speichern.

Sobald der Bearbeiter gespeichert hat wird ihm ein weiterer Tab "Nettobewertung" angezeigt. Zu diesem muss er für den nächsten Schritt navigieren.

Schritt 4a: Qualitative Ist-Bewertung durchführen



- 7 **Ist-Bewertung:** Dem Bearbeiter sollte nach der Eingabe der Risikobehandlung in den Tab "Nettobewertung" zurückkehren und mit der Ermittlung der "Ist-Bewertung" fortfahren.

Der Bearbeiter Risiko sollte die "Ist-Bewertung" in Relation der Brutto-Bewertung und den bisher gesetzte Maßnahmen und Kontrollen setzen. Je nachdem wie weit die *Maßnahmen* schon wirken, um den Soll-Zustand zu erreichen, sollte das Icon (C) in der Heatmap gesetzt werden.

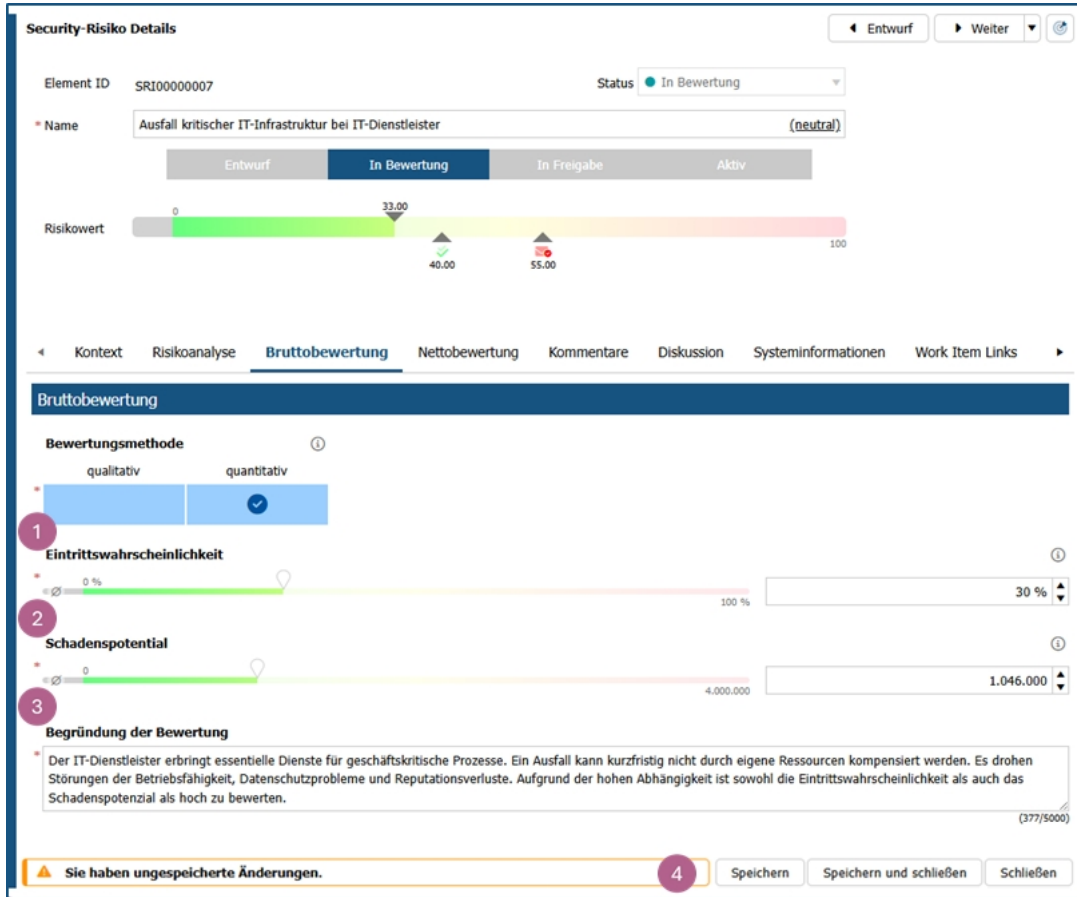
Die Ist-Bewertung des *Security-Risikos* wird **nicht** automatisch mittels Formel hinterlegt, sondern muss manuell eingetragen werden, da in BIC GRC die Interdependenzen zwischen *Maßnahmen* bzw. *Kontrollen* nicht berücksichtigt werden.

- 8 **Begründung der Ist-Bewertung:** Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu diesem aktuellen Wert gekommen ist.

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

Schritt 2b: Quantitative Bruttobewertung durchführen

Bei der quantitativ Risikobewertung wird eine monetäre Bewertung durchgeführt. Die Bewertung erfolgt dabei mittels eines konkreten Wertes.



- 1 **Eintrittswahrscheinlichkeit:** Im ersten Schritt hat der Bearbeiter die Eintrittswahrscheinlichkeit zu bestimmen mit der das *Security-Risiko* auftreten kann.
- 2 **Schadenspotential:** Bei dem "Schadenspotential" kann ein monetärer Wert hinterlegt werden

Durch den Slider kann der Wert gesetzt oder durch das Zahlenfeld manuell geschrieben werden.

Der maximale Wert der im Slider angezeigt wird vom Management bestimmt.

- 3 **Begründung:** Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu dieser Bewertung gekommen ist.
- 4 **Speichern:** Sobald die Informationen angegeben sind, kann der Bearbeiter Risiko speichern.

Sobald der Bearbeiter gespeichert hat wird ihm ein weiterer Tab "Nettobewertung"

angezeigt. Zu diesem muss er für den nächsten Schritt navigieren.

Schritt 3b: Quantitative Soll-Bewertung durchführen

Security-Risiko Details Entwurf Weiter

Element ID: SRI00000007 Status: In Bewertung

* Name: Ausfall kritischer IT-Infrastruktur bei IT-Dienstleister (neutral)

Entwurf **In Bewertung** In Freigabe Aktiv

Risikowert: 0 27.00 40.00 55.00 100

Kontext Risikoanalyse Bruttobewertung **Nettobewertung** Risikobehandlung Kommentare Diskussion Systeminformationen

Nettobewertung

1 **Soll-Eintrittswahrscheinlichkeit**

* 0 % 100 % 20 %

Soll-Schadenspotential

* 0 4.000.000 463.000

2 **Begründung der Soll-Bewertung**

* Ziel der geplanten Maßnahme ist es, durch Redundanzen, Verträge mit Ausfallregelungen und regelmäßige Tests mit dem Dienstleister die Eintrittswahrscheinlichkeit deutlich zu reduzieren. Ein Restrisiko durch das Schadenspotential bleibt bestehen, falls ein Ausfall dennoch eintritt.

(281/5000)

Security-Risiko Details Entwurf Weiter

Element ID: SRI00000007 Status: In Bewertung

* Name: Ausfall kritischer IT-Infrastruktur bei IT-Dienstleister (neutral)

Entwurf **In Bewertung** In Freigabe Aktiv

Risikowert: 0 33.00 40.00 55.00 100

Kontext Risikoanalyse Bruttobewertung **Nettobewertung** **Risikobehandlung** Kommentare Diskussion Syster

Risikobehandlung

3 **Behandlungsmethode**

Vermeiden Vermindern **Transferieren** Akzeptieren

4 **Mitigierende Kontrollen**

Name	Status	B...	
Regelmäßiger Notfalltest mit dem IT-Dienstleister	Aktiv	1	+ -

5 **Mitigierende Maßnahmen**

Name	Status	B...	
Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister	Bewertet	1	+ -

6 **Sie haben ungespeicherte Änderungen.** Speichern Speichern und schließen Schließen

- 1 **Soll- Bewertung:** Dem Bearbeiter werden jeweils zwei Eintrittswahrscheinlichkeit und Schandespotenzial Attribute für die Soll- und Ist-Bewertung angezeigt.

Sobal der Bearbeiter Risiko die Soll-Werte ausgefüllt hat, wird im ein weiterer Tab "Risikobehandlung" angezeigt.

- 2 **Begründung der Soll- Bewertung:** Nach der Soll- Bewertung muss eine Begründung eingegeben werden, wie der Bearbeiter zu diesem Zielwert gekommen ist.

- 3 **Risikosteuerung:** Nun wechselt der Bearbeiter in den Tab "Risikobehandlung".

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. Verlagerung von IT- Systemen in zertifizierte Rechenzentren mit hoher Ausfallsicherheit.
- Vermindern: Das Risiko wird durch Maßnahmen vermindert, die sowohl auf die Ursache als auch auf die Wirkung Einfluss nehmen, z.B. Aufbau redundanter Netzwerkverbindungen für kritische Standorte.
- 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 Security-Risiko effizient oder effektiv vermeiden, vermindern oder transferieren, muss das Restrisiko akzeptiert werden.

Der Bearbeiter kann ein *Security-Risiko* 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.

- 4 **Mitigierende Kontrollen:** Der Bearbeiter sollte "Mitigierende Kontrollen" [ableiten & erstellen](#) oder verlinken, wenn er die Behandlungsmethode "Vermindern" oder "Transferieren" auswählt.

Der Bearbeiter kann nur Kontrollen verlinken, die sich nicht im Status "Inaktiv" oder "Obsolet" befinden.

- 5 **Mitigierende Maßnahmen:** Der Bearbeiter sollte "Mitigierende Maßnahmen" [ableiten & erstellen](#), wenn er die Behandlungsmethode "Vermindern" oder "Transferieren" auswählt. Um den tatsächlichen Einfluss einer Maßnahme auf ein Security-Risiko abzubilden, hat der Bearbeiter Risiko eine Maßnahmenbewertung zu erstellen.

Ein Verlinkung ist nicht möglich.

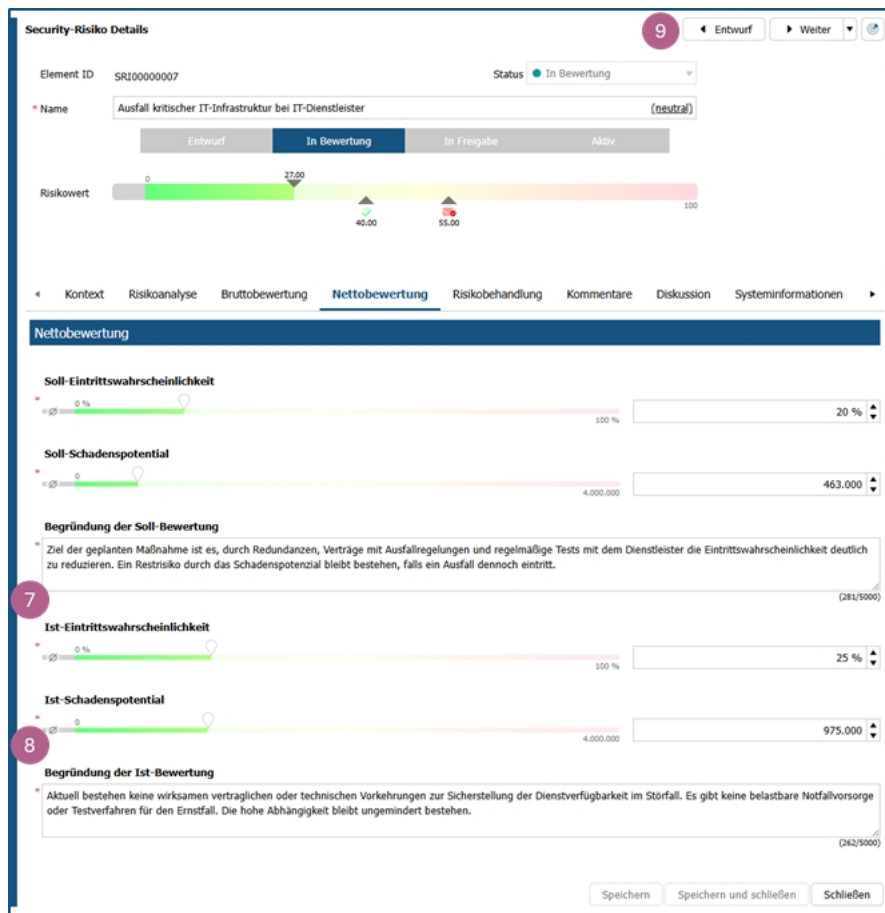
Für die Mitigation des *Security-Risiko* können mehrere *Maßnahmenbewertungen* aus

dem *Security-Risiko* heraus erstellt werden.

6 Speichern: Sobald die Informationen angegeben sind, kann der Bearbeiter Risiko speichern.

Sobald der Bearbeiter gespeichert hat wird ihm ein weiterer Tab "Nettobewertung" angezeigt. Zu diesem muss er für den nächsten Schritt navigieren.

Schritt 4b: Quantitative Ist-Bewertung durchführen



7 Ist-Bewertung: Dem Bearbeiter sollte nach der Eingabe der Risikobehandlung in den Tab "Nettobewertung" zurückkehren und mit der Ermittlung der "Ist-Bewertung" fortfahren.

Der Bearbeiter Risiko sollte die "Ist-Bewertung" in Relation der Brutto-Bewertung und den bisher gesetzte Maßnahmen und Kontrollen setzen. Jenachdem wie weit die *Maßnahmen* schon wirken, um den Soll- Zustand zu erreichen, sollten die Werte für Eintrittswahrscheinlichkeit und Schadenspotenzial in der Ist-Bewertung festgelegt werden.

Die Ist- Bewertung des *Security-Risikos* wird **nicht** automatisch mittels Formel hinterlegt, sondern muss manuell eingetragen werden, da in BIC GRC die Interdependenzen zwischen *Maßnahmen* bzw. *Kontrollen* nicht berücksichtigt

werden.

- 8 **Begründung der Ist-Bewertung:** Anschließend muss eine Begründung eingegeben werden, wie der Bearbeiter zu diesem aktuellen Wert gekommen ist.
- 9 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang "Freigabe" durchgeführt.

Der nächste Status wird von [Freigeber Risiko - Security-Risiko überprüfen & freigeben](#) durchgeführt. Der eingetragene Freigeber Risiko wird mittels Notifikation über den Statuswechsel informiert.

Nach Eingabe aller notwendigen Informationen kann das Work Item gespeichert und ein Statusübergang durchgeführt werden, bevor das Fenster geschlossen wird.

1.7.9 Maßnahmenbewertung ableiten & erstellen

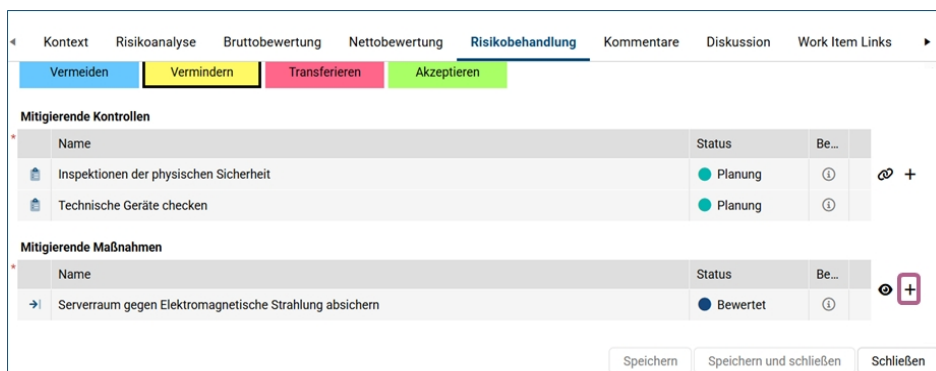
Nach der Erstellung eines *Security-Risikos* bedarf es *Maßnahmen*, um das *Security-Risiko* zu mitigieren. Um nicht für jedes *Security-Risiko* individuelle *Maßnahmen* erstellen zu müssen, die sich dann im System doppelt wiederfinden, besteht die Möglichkeit über *Maßnahmenbewertung*, eine Verbindung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

Diese *Maßnahmenbewertung* stellt den tatsächlichen Einfluss einer *Maßnahme* auf ein spezifisches *Security-Risiko* fest.

Schritt 1: Maßnahmenbewertung erstellen

Die *Maßnahmenbewertung* kann nur mittels Erstellung aus dem Work Item *Security-Risiko* 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.



Risikobehandlung			
Vermeiden Vermindern Transferieren Akzeptieren			
Mitigierende Kontrollen			
Name	Status	Be...	
Inspektionen der physischen Sicherheit	Planung	①	⌵ +
Technische Geräte checken	Planung	①	
Mitigierende Maßnahmen			
Name	Status	Be...	
→ Serverraum gegen Elektromagnetische Strahlung absichern	Bewertet	①	⌵ +
			Speichern Speichern und schließen Schließen

Die *Maßnahmenbewertung* wird nicht in einem neuen Fenster geöffnet, sondern ist Teil des *Security-Risikos*.

Schritt 2: Maßnahme zuordnen



Work Item: MEV00000011 - regelmäßige Ausfalltests

Maßnahmenbewertung Details

Maßnahmenzuordnung

Maßnahme	Name	Status	B...
	regelmäßige Ausfalltests	Entwurf	

Beschreibung

Durchführung geplanter, dokumentierter und wiederkehrender Tests zur Reaktion auf Ausfälle geschäftskritischer IT-Dienstleister, inkl. Kommunikation, Umschaltung auf Ausweichsysteme und Verfügbarkeitsprüfung.

Speichern Speichern und schließen Schließen

- 1 **Maßnahme verlinken:** Zuerst muss der Bearbeiter ein Work Item des Typs *Maßnahme* verlinken , die das spezifische *Security-Risiko* 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 *Security-Risiko* wirkt.
- 4 **Speichern:** Anschließend kann die *Maßnahmenbewertung* gespeichert werden, damit weitere Attributfelder angezeigt werden.

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

Schritt 3: Maßnahmenwirkung dokumentieren

Maßnahmenbewertung Details

Maßnahmenzuordnung

Maßnahme

Name	Status	B...
regelmäßige Ausfalltests	Entwurf	

Beschreibung

Durchführung geplanter, dokumentierter und wiederkehrender Tests zur Reaktion auf Ausfälle geschäftskritischer IT-Dienstleister, inkl. Kommunikation, Umschaltung auf Ausweichsysteme und Verfügbarkeitsprüfung.

Maßnahmenreduktion

Maßnahme wirkt auf

Eintrittswahrscheinlichkeit ☒ Schadenspotenzial ☐

Reduktionsrate

2025

0% 10% 20% 30% 50% 70% 90% 100%

Speichern Speichern und schließen Schließen

- 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 *Security-Risiko* 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.

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

Wenn das *Security-Risiko* in den Status "Obsolet" geschaltet wird, wird auch die *Maßnahmenbewertung* in "Obsolet" gesetzt. Dasselbe Verhalten ergibt sich, wenn die *Maßnahme* in den Status "Obsolet" geschaltet wird.

Zurück zu dem Schritt [Bearbeiter Risiko - Security-Risiko beurteilen & bewerten](#).

1.7.10 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

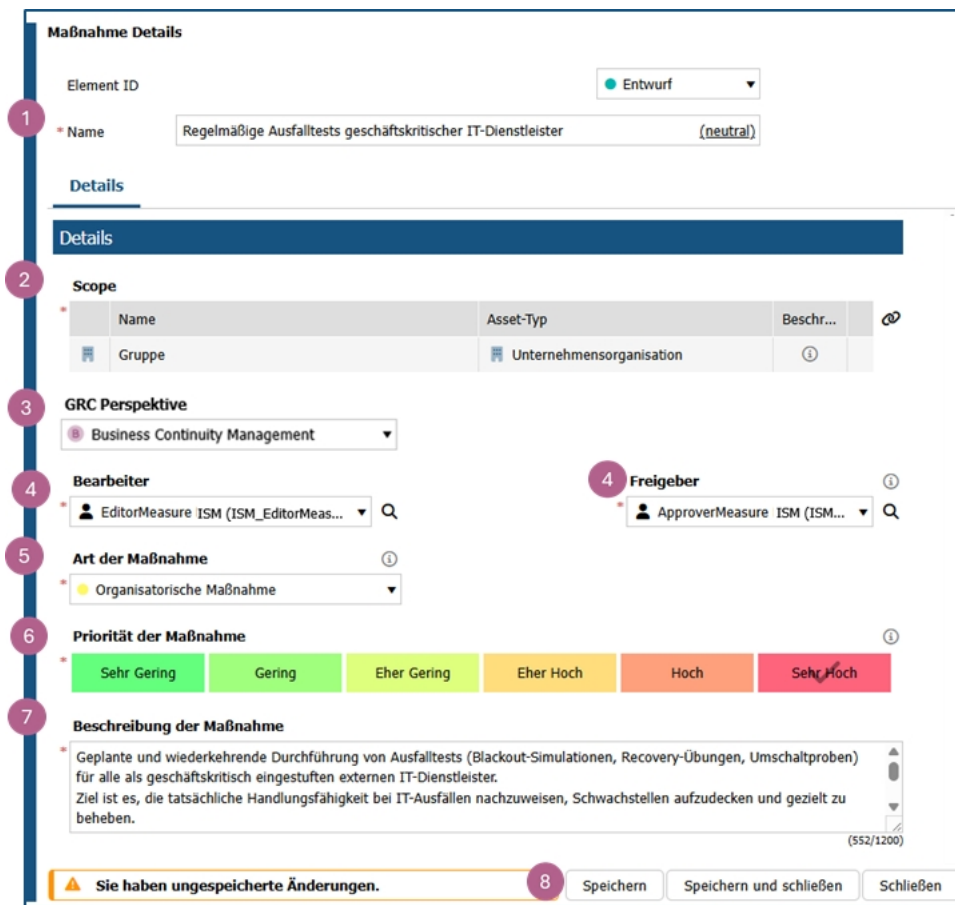
Die *Maßnahme* kann von einem Bearbeiter aus einem *Security-Risiko* bzw. einer *Maßnahmenbewertung* heraus erstellt werden, indem er im *Security-Risiko* und anschließend in der *Maßnahmenbewertung* auf das Icon  klickt.

Maßnahmenzuordnung

Maßnahme

	Name	Status	B...	
	regelmäßige Ausfalltests	 Entwurf		 

Schritt 2: Details hinterlegen



Maßnahme Details

Element ID: Entwurf

1 * Name: Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Details

2 **Scope**

Name	Asset-Typ	Beschr...	
Gruppe	Unternehmensorganisation		

3 **GRC Perspektive**

Business Continuity Management

4 **Bearbeiter**

EditorMeasure ISM (ISM_EditorMeas...

4 **Freigeber**

ApproverMeasure ISM (ISM...

5 **Art der Maßnahme**

Organisatorische Maßnahme

6 **Priorität der Maßnahme**

Sehr Gering Gering Eher Gering Eher Hoch Hoch Sehr Hoch

7 **Beschreibung der Maßnahme**

Geplante und wiederkehrende Durchführung von Ausfalltests (Blackout-Simulationen, Recovery-Übungen, Umschaltproben) für alle als geschäftskritisch eingestuft externen IT-Dienstleister. Ziel ist es, die tatsächliche Handlungsfähigkeit bei IT-Ausfällen nachzuweisen, Schwachstellen aufzudecken und gezielt zu beheben.

8 Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

- 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. [Security- Risiko beurteilen & bewerten](#) fortfahren.

1.7.11 Kontrolle ableiten & erstellen

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

Schritt 1: Kontrolle erstellen aus Security-Risiko

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

Kontrollen			
Name	Status	B...	
Regelmäßiger Notfalltest mit dem IT-Dienstleister	In Planung		

Ein neues Fenster öffnet sich anschließend automatisch.

Schritt 2: Details hinterlegen

Kontrolle Details

In Planung

Name

1 Regelmäßiger Notfalltest mit dem IT-Dienstleister (neutral)

Zuordnung

Details

2 Scope

Name	Asset-Typ	Beschr...
Gruppe	Unternehmensorganisation	

3 GRC Perspektive

Business Continuity Management

4 Bearbeiter

EditorControl

5 Kontrollebene

Entity Level Control

6 Art der Kontrolle

Hauptkontrolle

8 Freigeber

ApproverControl

7 Beschreibung der Kontrolle

Die Kontrolle stellt sicher, dass in regelmäßigen Abständen (mind. jährlich) ein dokumentierter Notfalltest gemeinsam mit dem geschäftskritischen IT-Dienstleister durchgeführt wird. Dabei wird das Szenario eines IT-Ausfalls simuliert (Blackout-Simulation), um die Wirksamkeit der Notfallkonzepte, Kommunikationswege und Wiederanlaufstrategien zu prüfen. Der Test umfasst alle betroffenen Fachbereiche und wird durch definierte Erfolgsparameter (z. B. Wiederanlaufzeit,

Sie haben ungespeicherte Änderungen.

8 Speichern Speichern und schließen Schließen

- 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.
- Scope:** Um den Bereich der Anzeigeverfügbarkeit der *Kontrolle* einzuschränken, muss es einem Asset in der Asset Hierarchie zugeordnet werden.
- GRC-Perspektive:** Die Perspektive wird automatisch aus dem *Security-Risiko* 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 [Security-Risiko beurteilen & bewerten](#) fortfahren.

1.7.12 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.

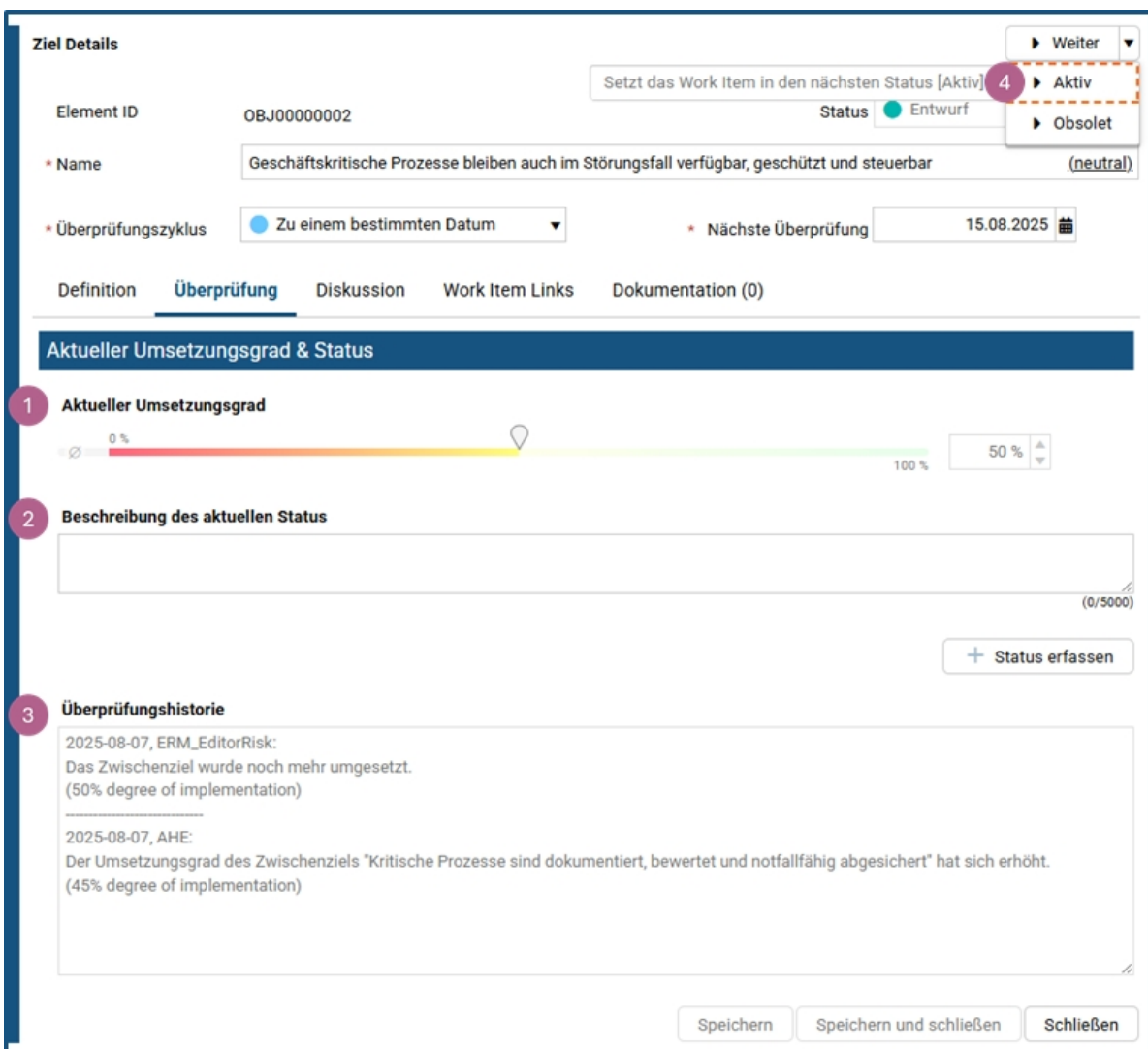
An dem Tag an dem das Datum erreicht wird, wird der Status automatisch zu "Entwurf" gewechselt und der Bearbeiter bekommt erneut eine E-Mail zugesendet. Der Link zu dem spezifischen *Ziel* befindet sich in der Notifikation.

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



Ziel Details

Element ID: OBJ00000002

Status: Entwurf

Name: Geschäftskritische Prozesse bleiben auch im Störfall verfügbar, geschützt und steuerbar (neutral)

Überprüfungszyklus: Zu einem bestimmten Datum

Nächste Überprüfung: 15.08.2025

Definition | **Überprüfung** | Diskussion | Work Item Links | Dokumentation (0)

Aktueller Umsetzungsgrad & Status

1 **Aktueller Umsetzungsgrad**

0 % 100 % 50 %

2 **Beschreibung des aktuellen Status**

(0/5000)

+ Status erfassen

3 **Überprüfungshistorie**

2025-08-07, ERM_EditorRisk:
Das Zwischenziel wurde noch mehr umgesetzt.
(50% degree of implementation)

2025-08-07, AHE:
Der Umsetzungsgrad des Zwischenziels "Kritische Prozesse sind dokumentiert, bewertet und notfallfähig abgesichert" hat sich erhöht.
(45% degree of implementation)

Speichern | Speichern und schließen | Schließen

- 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.

1.8 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 *Security-Risiken* managen müssen.

Folgende Aufgaben hat ein Freigeber Risiko in BIC GRC:

- [Security-Risiko 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](#)
- [Security-Risiko 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.

1.8.1 Security-Risiko überprüfen & freigeben

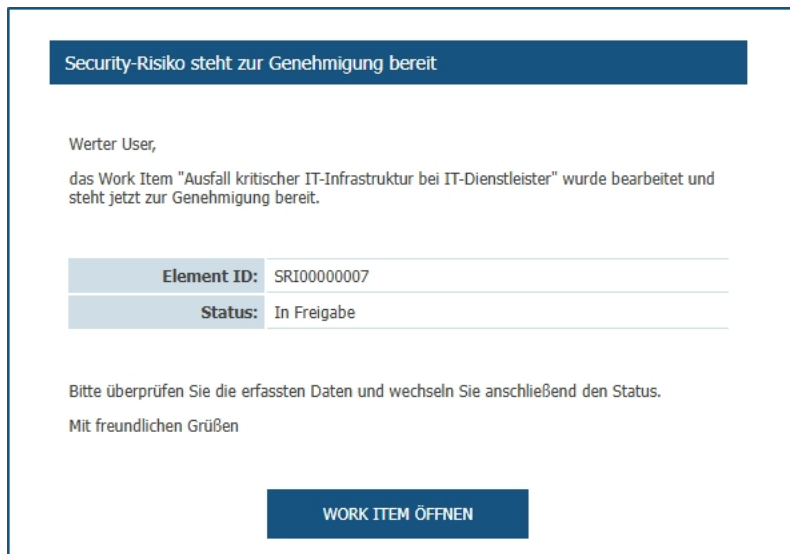
Ein *Security-Risiko* wird vom Bearbeiter Risiko erstellt und bewertet. Sobald die Bewertung abgeschlossen und überprüft wurde, kann ein *Security-Risiko* dem Freigeber Risiko weitergegeben werden mittels Statusübergang in "Freigabe".

Schritt 1: Navigation zu spezifischen Security-Risiko

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

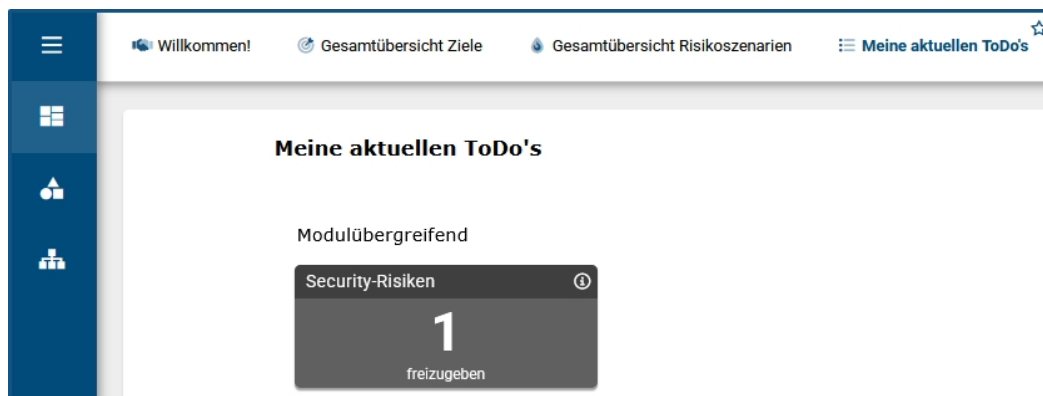
1. Öffnen über Notifikation

Der Freigeber Risiko bekommt eine E-Mail zugesendet, sobald der Bearbeiter Risiko alle Eingaben im Status "Behandlung" abgeschlossen hat. Der Link zu dem spezifischen *Security-Risiko* 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.

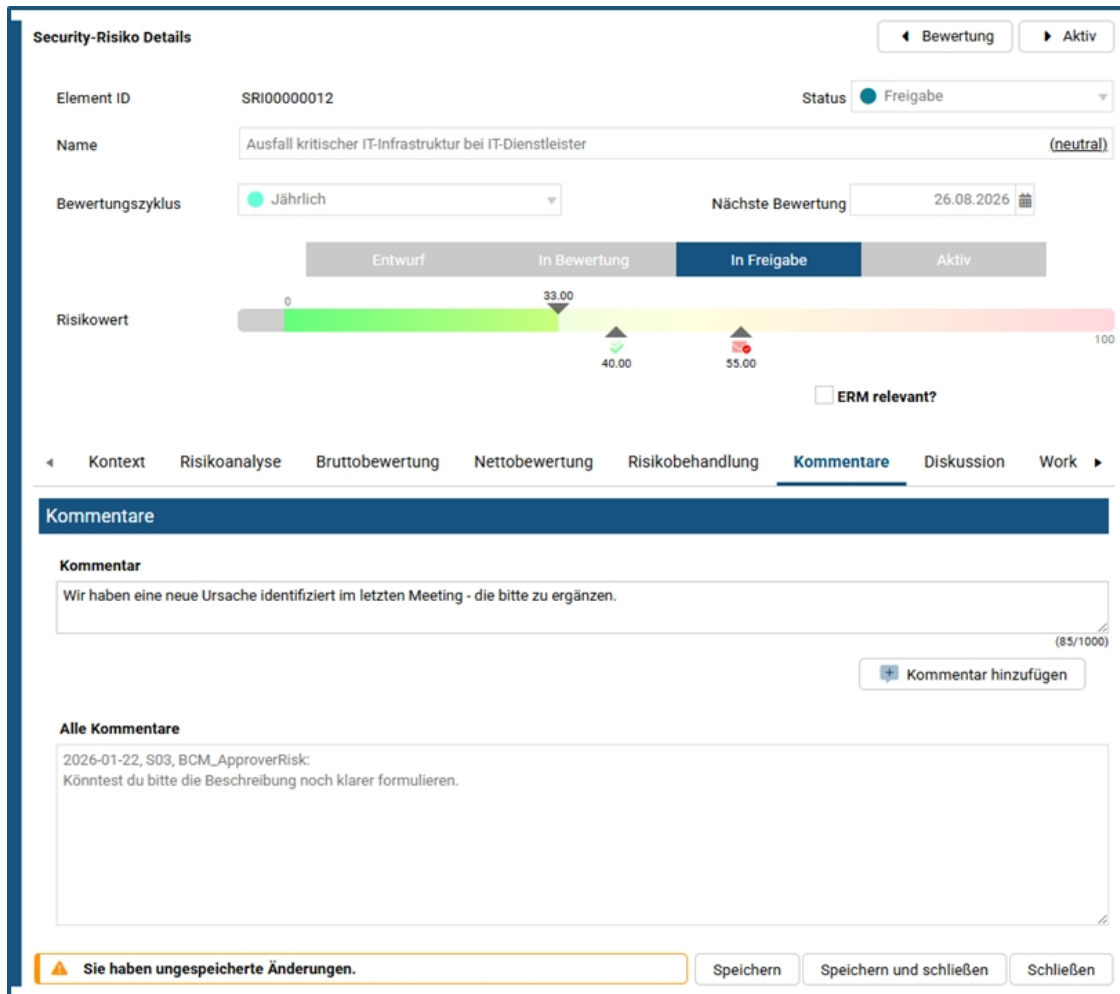


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für das *Security-Risiko* automatisch.

Schritt 2: Überprüfung durchführen

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

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



Sollte zudem das *Security-Risiko* besonders hoch sein oder das *Security-Risiko* 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 "Managementfreigabe" 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 "Managementfreigabe" benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.9 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](#)

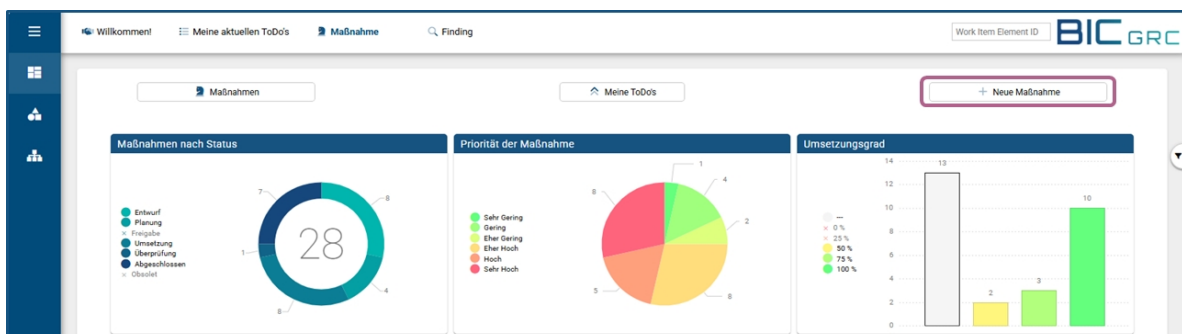
1.9.1 Maßnahme definieren & erstellen

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 .

Maßnahmenzuordnung				
Maßnahme				
	Name	Status	B...	
	regelmäßige Ausfalltests	Entwurf		 

3. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.

Work Items		Maßnahme	
		 Erstellen	 Löschen
		Ansicht exportieren	
		Standardansicht	
☐	(0)	Element ID	
☐		MEA00000008	
☐		MEA00000042	

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

Maßnahme Details

Element ID Entwurf

* Name **1** Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Details

2 Scope

Name	Asset-Typ	Beschr...
Gruppe	Unternehmensorganisation	

3 GRC Perspektive

* Business Continuity Management

4 Bearbeiter

* EditorMeasure BCM (BCM_EditorMea... Q

4 Freigeber

* ApproverMeasure BCM (BC... Q

5 Art der Maßnahme

* Organisatorische Maßnahme

6 Priorität der Maßnahme

Sehr Gering Gering Eher Gering Eher Hoch Hoch **Sehr Hoch**

7 Beschreibung der Maßnahme

* Geplante und wiederkehrende Durchführung von Ausfalltests (Blackout-Simulationen, Recovery-Übungen, Umschaltproben) für alle als geschäftskritisch eingestuft externen IT-Dienstleister. Ziel ist es, die tatsächliche Handlungsfähigkeit bei IT-Ausfällen nachzuweisen, Schwachstellen aufzudecken und gezielt zu beheben.

(552/1200)

8 ⚠ Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

- 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 freigeschalteten 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 die *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.

1.9.2 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.

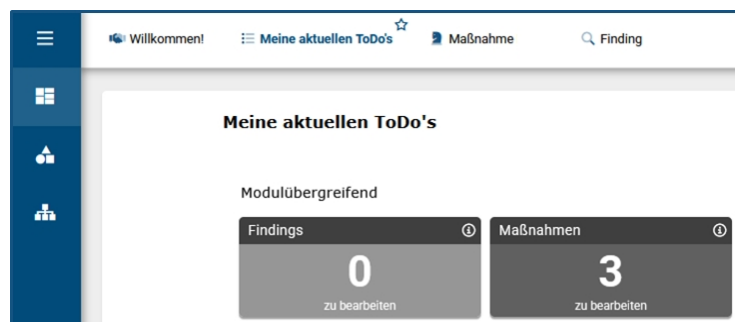
1. Öffnen über Notifikation

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.

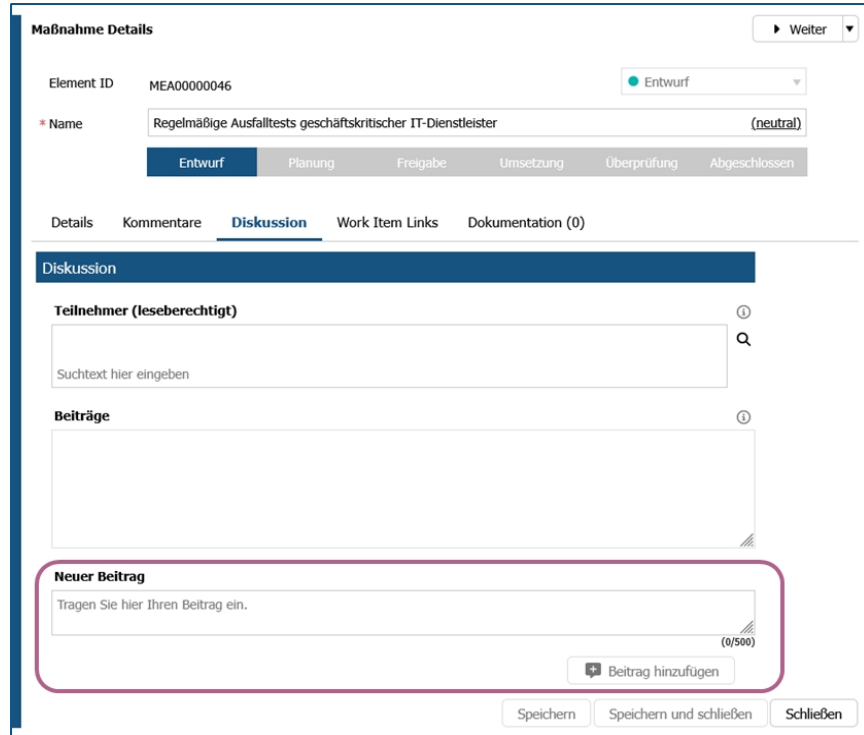


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Maßnahme* automatisch.

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 Detailsangaben 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.



Maßnahme Details ► Weiter ▼

Element ID: MEA00000046 Entwurf ▼

* Name: Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Entwurf Planung Freigabe Umsetzung Überprüfung Abgeschlossen

Details Kommentare **Diskussion** Work Item Links Dokumentation (0)

Diskussion

Teilnehmer (leseberechtigt) ⓘ

Suchtext hier eingeben 🔍

Beiträge ⓘ

Neuer Beitrag

Tragen Sie hier Ihren Beitrag ein. (0/500)

Beitrag hinzufügen

Speichern Speichern und schließen Schließen

Schritt 3: Eingaben ergänzen

Maßnahme Details

Element ID: MEA00000046

Name: Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Status: Entwurf

Details | Kommentare | Diskussion | Work Item Links | Dokumentation (0)

Risikostufen: Sehr Gering, Gering, Etwas Gering, Etwas Hoch, Hoch, Sehr Hoch

Beschreibung der Maßnahme

* Geplante und wiederkehrende Durchführung von Ausfalltests (Blackout-Simulationen, Recovery-Übungen, Umschaltproben) für alle als geschäftskritisch eingestuften externen IT-Dienstleister. Ziel ist es, die tatsächliche Handlungsfähigkeit bei IT-Ausfällen nachzuweisen, Schwachstellen aufzudecken und gezielt zu beheben. (552/1200)

Referenzen

1 **Dokumentierte Informationen**

Name	Status	Besc
Verfahrensanweisung zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse	Aktiv	

2 **Kontroll-Assessment**

Keine Zuordnung vorhanden.

3 Statuswechsel: Entwurf, In Planung, Obsolet

Speichern | Speichern und schließen | Schließen

- 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.

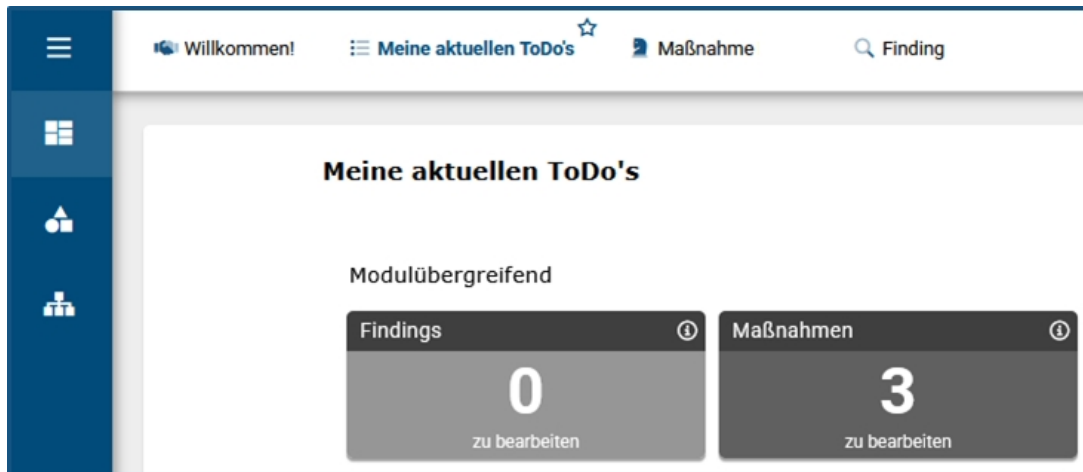
- 2 **Kontroll- Assessment:** Der Link zu einem spezifischem Assessment wird automatisch ausgefüllt von BIC GRC, wenn die *Maßnahme* aus einem passenden Assessment erstellt wurde. Sollte die *Maßnahme* schon vor dem Assessment bestehen kann das "Kontroll-Assesement" im Nachgang verlinkt werden.
- 3 **Statuswechsel:** 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.

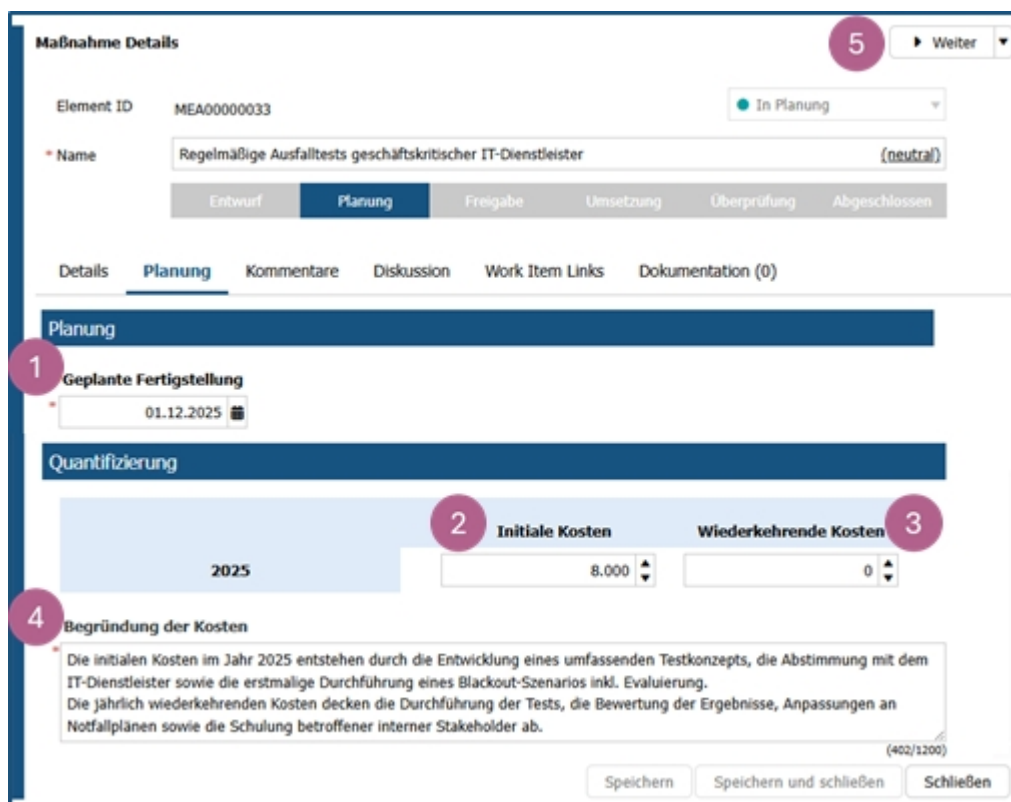
1.9.3 Maßnahme aufbauen & planen

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_ & freigegeben](#) 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.

1.9.4 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 freigeben und einen Statusübergang zu "Umsetzung" durchgeführt hat. Der Link zu der spezifischen *Maßnahme* befindet sich in der Notifikation.

Maßnahme wurde genehmigt

Werter User,

das Work Item "Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister" wurde genehmigt.

Element ID:	MEA00000033
Status:	In Umsetzung

Diese Nachricht dient nur zur Information und impliziert keinen Handlungsbedarf.

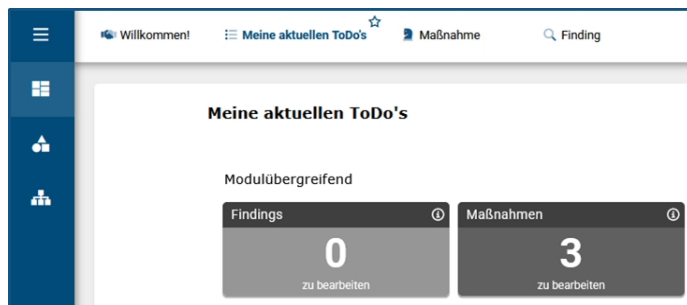
Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail.

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

Maßnahme Details

4 ▶ Überprüfung

Element ID

MEA00000077

Umsetzung

Name

Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Entwurf

Planung

Freigabe

Umsetzung

Überprüfung

Abgeschlossen

Details

Umsetzung

Kommentare

Diskussion

Work Item Links

Dokumentation (0)

Umsetzungsdetails

1 Umsetzungsgrad

0 %

25 %

50 %

75 %

100 %

☐ Umsetzungsgrad entspricht Wirksamkeit der Maßnahme

2 In Umsetzung seit

03.02.2026

Fertigstellung bei Verzögerung

TT.MM.JJJJ

3 Beschreibung der Umsetzungsschritte

-Erstellung eines detaillierten Testkonzepts einschließlich Zieldefinition und Bewertungskriterien
 -Erstberatung mit dem IT-Dienstleister hinsichtlich der Machbarkeit der geplanten Szenarien
 -Beauftragung externer Unterstützung für die Testdurchführung (technischer Dienstleister)
 -Planung des ersten Testlaufs für Q4/2025

Begründung bei Verzögerungen

Speichern

Schließen

- 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.

1.9.5 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

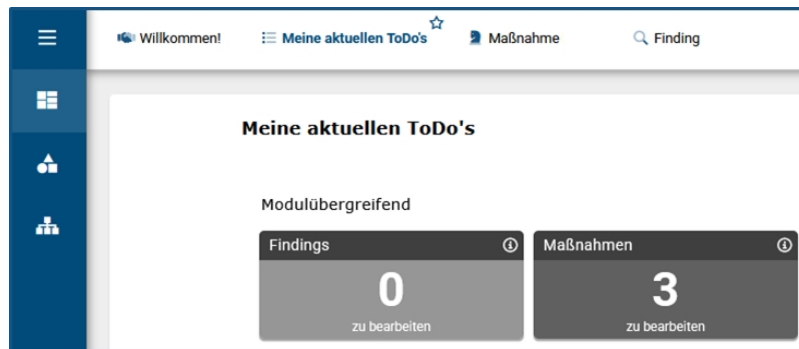
Der Bearbeiter Maßnahme hat zwei Möglichkeiten, eine *Maßnahme* zu bearbeiten/öffnen.

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.

Maßnahme Details

8

In Umsetzung

Abgeschlossen

Element ID

MEA00000033

In Überprüfung

Name

Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Entwurf

Planung

Freigabe

Umsetzung

Überprüfung

Abgeschlossen

Details

Umsetzung

Testing

Kommentare

Diskussion

Work Item Links

Dokumentation (0)

Testing-Details

1

Testing-Datum

31.07.2025

2

Testbeschreibung

Im Rahmen der Maßnahme wurden in Kooperation mit dem IT-Dienstleister geplante Ausfalltests durchgeführt. Die Tests umfassten:

- Blackout-Simulationen inkl. Serverabschaltung
- Wiederanlauf-Szenarien aus dem Notfallhandbuch

3

Angemessenheitsprüfung

bestanden

fehlgeschlagen

Details

Die Maßnahme ist geeignet, die geplanten Ziele zu erreichen. Die Tests decken typische Szenarien ab, sind standardisiert dokumentiert und technisch sowie organisatorisch angemessen dimensioniert.

4

Wirksamkeitsprüfung

bestanden

fehlgeschlagen

Details

Die Maßnahme hat den erwarteten Effekt erzielt. Die Tests wurden erfolgreich durchgeführt und belegten eine signifikante Reduktion der Wiederanlaufzeit sowie eine verbesserte Abstimmung mit dem IT-Dienstleister. Die Kommunikation im Krisenfall konnte nachweislich verbessert werden.

5

Nachweis

Dateien hierher ziehen zum Hochladen

Testbericht

Administrator Riem

31.07.2025 11:32

6

Findings

Name	Status	B...
Dokumentationslücke beim Notfalltestprotokoll 2025	Erfassung	

7

Bemerkungen

Speichern

Speichern und schließen

Schließen

- 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.

1.9.6 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.

Findings		
Name	Status	B...
 Dokumentationslücke beim Notfalltestprotokoll 2025	 Erfassung	 

Schritt 2: Finding dokumentieren

Finding Details 10 Weiter

1 **Name**
 * Dokumentationslücke beim Notfalltestprotokoll 2025 (neutral)

Details

2 **GRC Perspektive**
 Business Continuity Management

3 **Bearbeiter**
 * Editor

4 **Datum der Meldung**
 * 31.07.2025

5 **zu behandeln bis**
 31.08.2025

6 **Art des Findings**
 Beobachtung Empfehlung Verbesserungswunsch Unwesentliche Nichtkonformität Wesentliche Nichtkonformität

7 **Finding für diese Assets:**

Name	Asset-Typ	Besch...
Gruppe	Unternehmensorganisation	

8 **Beschreibung des Findings**
 * Beim Review der durchgeführten Notfalltests wurde festgestellt, dass das vollständige Testprotokoll für das Jahr 2025 noch nicht im zentralen Dokumentenmanagementsystem abgelegt wurde. Die Durchführung selbst ist dokumentiert, der Ablageprozess war jedoch unvollständig.

9 **Priorität des Findings**
 * Sehr Niedrig Niedrig Mittel Hoch Kritisch

Speichern Speichern und schließen Schließen

- 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 eine 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 Dashboards 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](#).

1.9.7 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

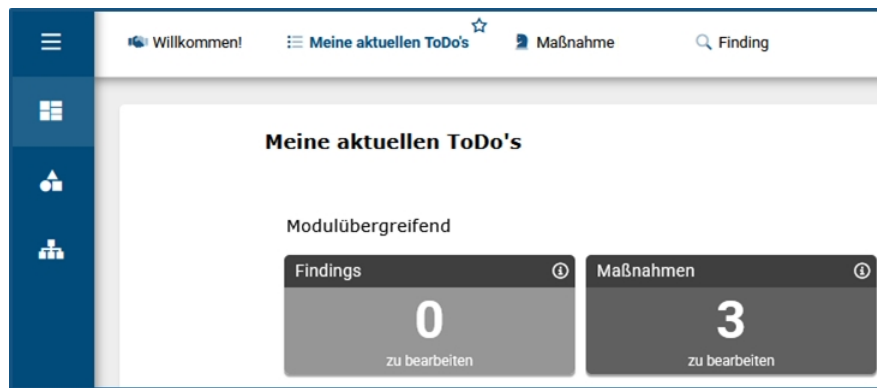
Der Bearbeiter hat zwei Möglichkeiten ein zu bearbeitendes *Finding* zu öffnen.

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

4

← Erfassung

► Abgeschlossen

Finding Details

Datum der Meldung

31.07.2025

zu behandeln bis

11.09.2025

1

Art des Findings

Beobachtung

Empfehlung

Verbesserungswunsch

Unwesentliche Nichtkonformität

Wesentliche Nichtkonformität

Finding für diese Assets:

Name	Asset-Typ	Besch...
Gruppe	Unternehmensorganisation	

Beschreibung des Findings

Beim Review der durchgeführten Notfalltests wurde festgestellt, dass das vollständige Testprotokoll für das Jahr 2025 noch nicht im zentralen Dokumentenmanagementsystem abgelegt wurde. Die Durchführung selbst ist dokumentiert, der Ablageprozess war jedoch unvollständig.

Priorität des Findings

Sehr Niedrig

Niedrig

Mittel

Hoch

Kritisch

Behandlung

2

Beschreibung der Behandlung

Das fehlende Testprotokoll wird umgehend im zentralen Dokumentenmanagementsystem abgelegt. Zusätzlich wird der Ablageprozess überprüft und angepasst, um sicherzustellen, dass zukünftig alle Protokolle zeitnah und vollständig erfasst werden.

3

Maßnahme

Keine Zuordnung vorhanden.

Speichern

Speichern und schließen

Schließen

- 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.
- 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.
- Maßnahme:** Das *Finding* wird durch eine *Maßnahme* behandelt. Mehr Informationen über die Erstellung einer Maßnahme unter [Bearbeiter_Maßnahme_-_Maßnahme_definieren_&_erstellen](#) Schritt 2.

GBTEC Austria GmbH

110/252

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.

1.10 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](#).

1.10.1 Maßnahme überprüfen & freigeben

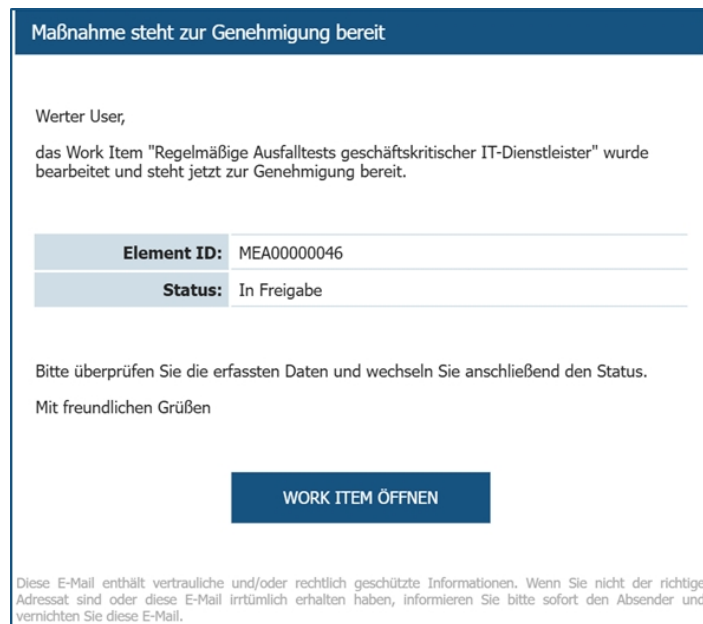
Nach der Erstellung und Planung einer *Maßnahme* durch einen Erfasser bzw. einen Bearbeiter, muss diese vor der Umsetzung einer Freigabe durch den Freigeber der Maßnahme überprüft werden.

Schritt 1: Navigation zur Maßnahme

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

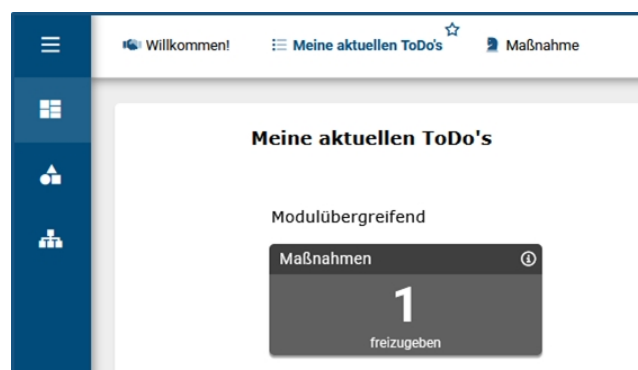
1. Öffnen über Notifikation

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.

Maßnahme Details

Planung

Weiter

Element ID

MEA00000068

Freigabe

Name

Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Entwurf

Planung

Freigabe

Umsetzung

Überprüfung

Abgeschlossen

Details

Planung

Kommentare

Diskussion

Work Item Links

Dokumentation (0)

Kommentare

Kommentar

Können wir das geplante Datum um eine Woche verschieben?

(56/1000)

Kommentar hinzufügen

Alle Kommentare

Sie haben ungespeicherte Änderungen.

Speichern

Schließen

Nach dem Statusübergang kann das Fenster geschlossen werden.

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

1.11 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 Benutzerprofil "Bearbeiter Maßnahme" verwiesen:

- [Maßnahme definieren & erstellen](#)

1.11.1 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.

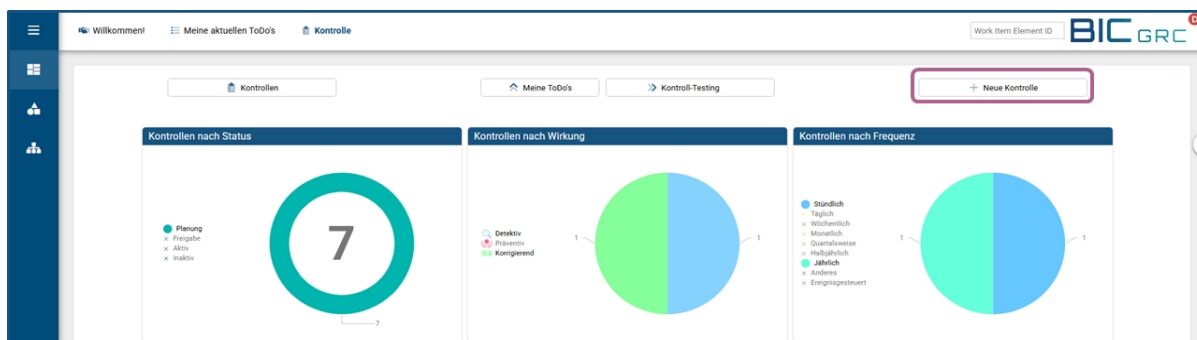
Schritt 1: Kontrolle erstellen

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.

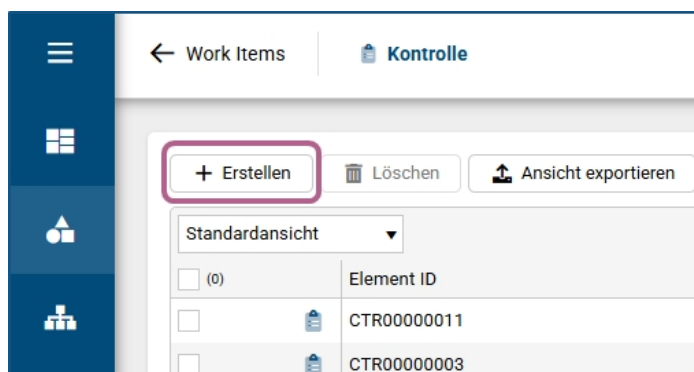


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung 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 freigeschalteten 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.

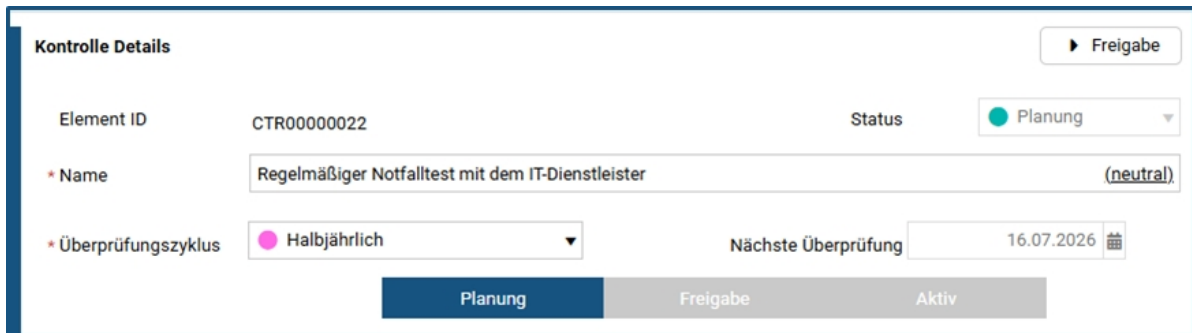
Ansonsten wird der hinterlegte Bearbeiter Kontrolle nach dem Speichervorgang mittels Notifikation über den Statusübergang benachrichtigt.

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" geschaltet und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.



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

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.

1.11.2 Kontrolle bearbeiten & prüfen

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

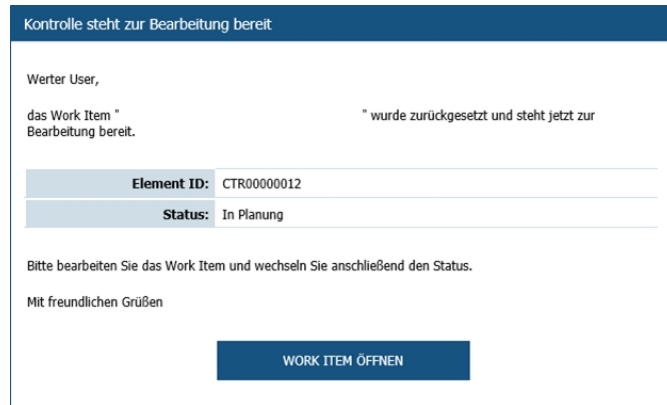
Wenn der Ersteller und der Bearbeiter unterschiedliche Benutzer sind, wird der Bearbeiter gesondert mittels Notifikation über die neue *Kontrolle* informiert. Die folgenden Schritte 1 & 2 beziehen sich auf die Schritte nach der Erstellung durch einen anderen Benutzer.

Optional Schritt 1: Navigation zu spezifischer Kontrolle nach Fremderstellung

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

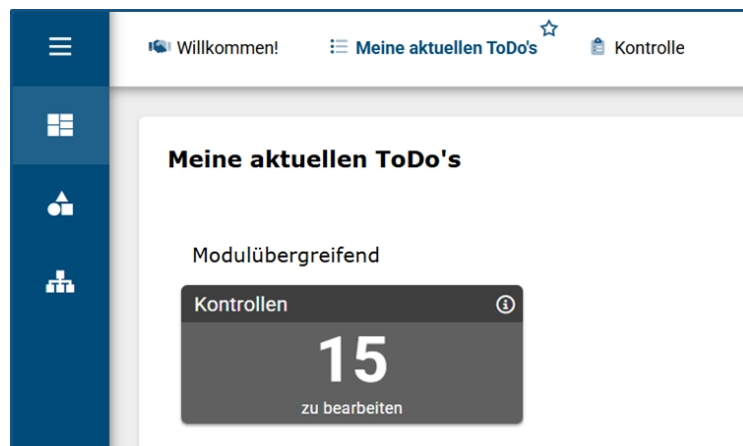
1. Öffnen über Notifikation

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 Details der Eingaben 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.

Kontrolle Details

Element ID

CTR00000019

In Planung

Name

Regelmäßiger Notfalltest mit dem IT-Dienstleister

(neutral)

In Planung

In Freigabe

Aktiv

Zuordnung

Kontrolldurchführung

Kontroll-Testing

Kommentare

Diskussion

Work Item Links

Dc

Diskussion

Teilnehmer (leseberechtigt)

Suchtext hier eingeben

Beiträge

Neuer Beitrag

Tragen Sie hier Ihren Beitrag ein.

(0/500)

Beitrag hinzufügen

Speichern

Speichern und schließen

Schließen

Schritt 3: Kontrolle ergänzen

Kontrolle Details

Element ID

CTR00000019

In Planung

Name

Regelmäßiger Notfalltest mit dem IT-Dienstleister

(neutral)

In Planung

In Freigabe

Aktiv

Zuordnung

Kontroll-Testing

Kommentare

Diskussion

Systeminformationen

Work Item Links

Dokumentation (0)

1

Kontrollziele

Name	Katalog	B...
Datensicherheit und Vertraulichkeit	Kontrollziele	
Risikomanagement und -überwachung	Kontrollziele	
Geschäftskontinuitäts- und Notfallplanung	Kontrollziele	
Compliance mit gesetzlichen und regulatorischen Anforderungen	Kontrollziele	

2

Kontroll Frequenz

Jährlich

3

Kontrollautomatisierung

Manuell

4

Kontroll-Testing Frequenz

Jährlich

5

Wirkung der Kontrolle

Präventiv

5

Auslagerung

ausgelagert innerhalb des Unternehmens

5

Kontrolle zugeordnet zu

Name	Asset-Typ	Beschrei...
Standort Australien	Unternehmensorganisation	

5

Ist die Kontrolle ausgelagert?

☒

- 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 berechnigte 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 Effektivität 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 Hierarchie 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:

- **Kontrollkatalog:** Der "Kontrollkatalog" führt nicht zu Work Items des Typen *Kontrolle*, sondern zu den Kontrollkatalog(en) von
 - BSI Anforderungen BCM
- **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.

- **Assessment:** Der Link zu einem spezifischem Assessment wird automatisch ausgefüllt von BIC GRC, wenn die *Kontrolle* aus einem passenden Assessment erstellt wurde. Sollte die *Kontrolle* schon vor dem Assessment bestehen kann das "Assesement" im Nachgang verlinkt werden.

6 Referenzen

Kontrollkataloge

Elementname	Name
ISO270022022.ISO27002_2022.05.29	5.29 Informationssicherheit bei Störungen
BSIRequirementsGrundschatz.BSI.SB.APP.04.03.A22_H	APP.4.3.A22 Notfallvorsorge (H)
BSIRequirementsGrundschatz.BSI.PB.DER.04.A10_H	DER.4.A10 Tests und Notfallübungen (H) [Institutionsleitung]

Dokumentierte Informationen

Keine Zuordnung vorhanden.

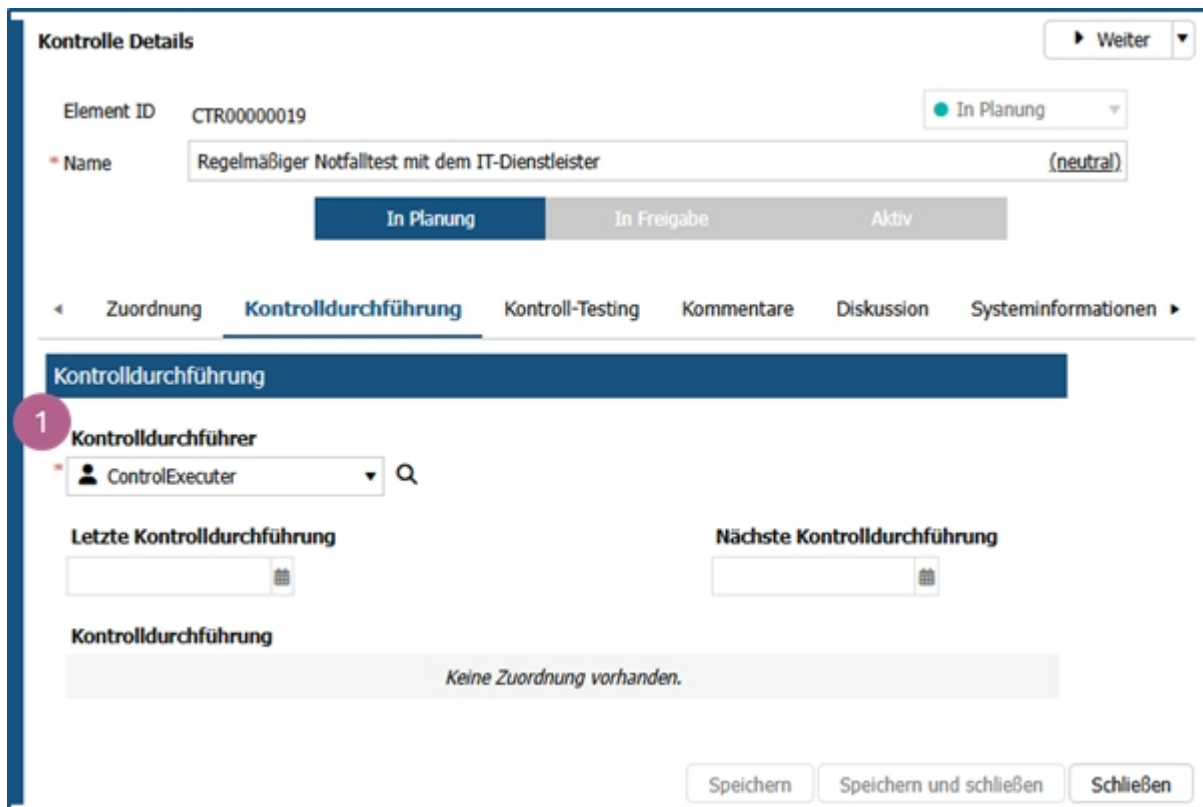
Assessment

Keine Zuordnung vorhanden.

Speichern Speichern und schließen Schließen

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:

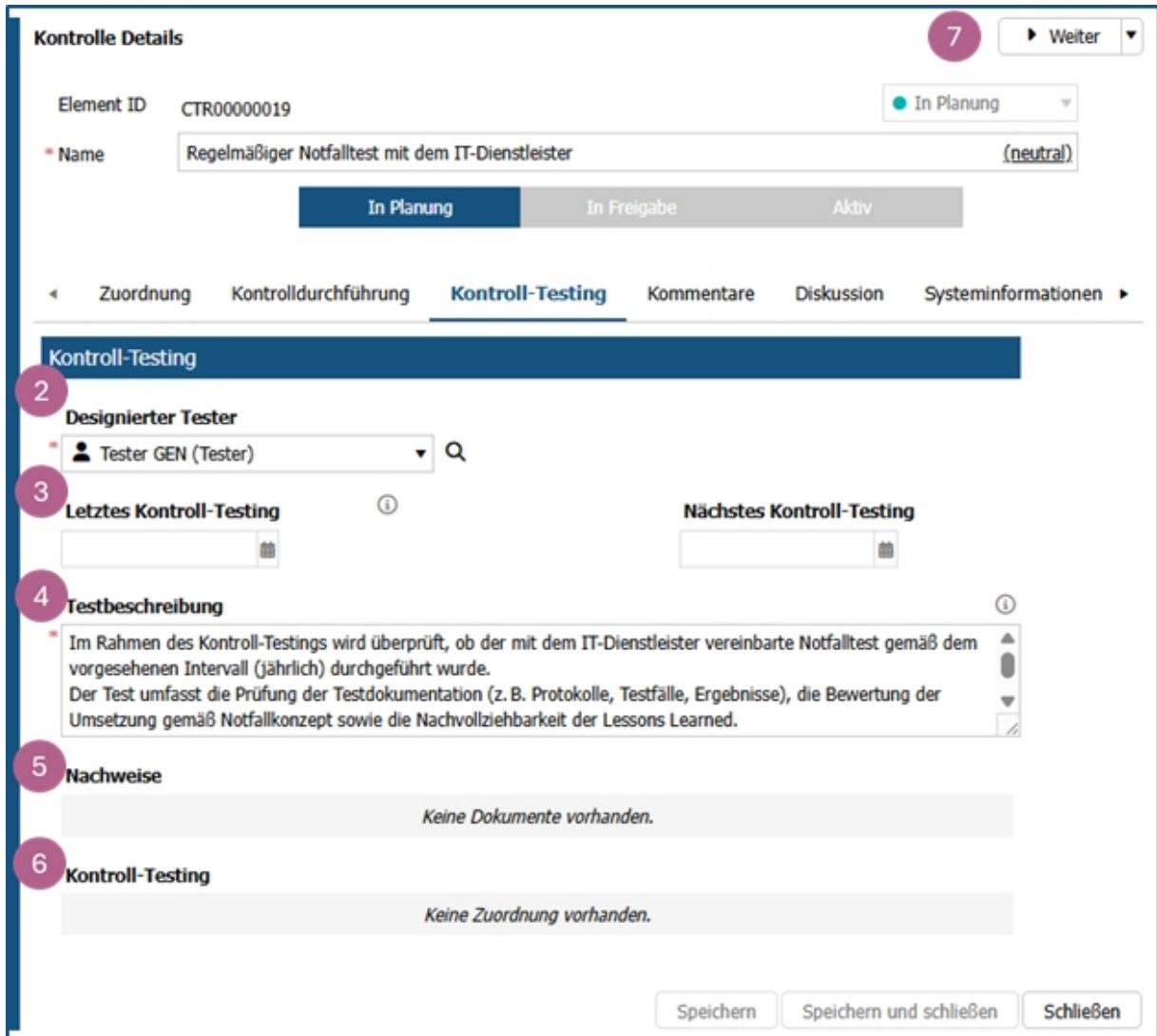
- **Letzte Kontrolldurchführung:** Setzt sich automatisch nach dem Statusübergang der *Kontrolldurchführung* von "Durchführung" zu "Abgeschlossen".

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 Designerter 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.

1.11.3 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.

Kontroll-Testing steht zum Testen bereit

Werter User,

das Work Item " " wurde bearbeitet und steht jetzt zum Testen bereit.

Element ID:	CTE00000001
Status:	Testdurchführung

Bitte führen Sie das Testing durch und wechseln Sie anschließend den Status.

Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

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.

Kontrolle Details

◀ In Planung

▶ Weiter ▼

📄

Element ID

CTR00000019

● Aktiv ▼

Name

Regelmäßiger Notfalltest mit dem IT-Dienstleister

(neutral)

In Planung

In Freigabe

Aktiv

◀ Zuordnung

Kontrolldurchführung

Kontroll-Testing

Kommentare

Diskussion

Systeminformationen ▶

Kontroll-Testing

Designierter Tester

👤

Tester GEN (Tester)

🔍

Letztes Kontroll-Testing

31.07.2025

📅

Nächstes Kontroll-Testing

31.07.2026

📅

Testbeschreibung

Im Rahmen des Kontroll-Testings wird überprüft, ob der mit dem IT-Dienstleister vereinbarte Notfalltest gemäß dem vorgesehenen Intervall (jährlich) durchgeführt wurde. Der Test umfasst die Prüfung der Testdokumentation (z. B. Protokolle, Testfälle, Ergebnisse), die Bewertung der Umsetzung gemäß Notfallkonzept sowie die Nachvollziehbarkeit der Lessons Learned.

Nachweise

Dateien hierher ziehen zum Hochladen

Keine Dokumente vorhanden.

Kontroll-Testing

Name	Status	B...	
📄 Regelmäßiger Notfalltest mit dem IT-Dienstleister - 2025-07-31	● Test be...		👁 +

Speichern

Speichern und schließen

Schließen

GBTEC Austria GmbH

124/252

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.

1.11.4 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

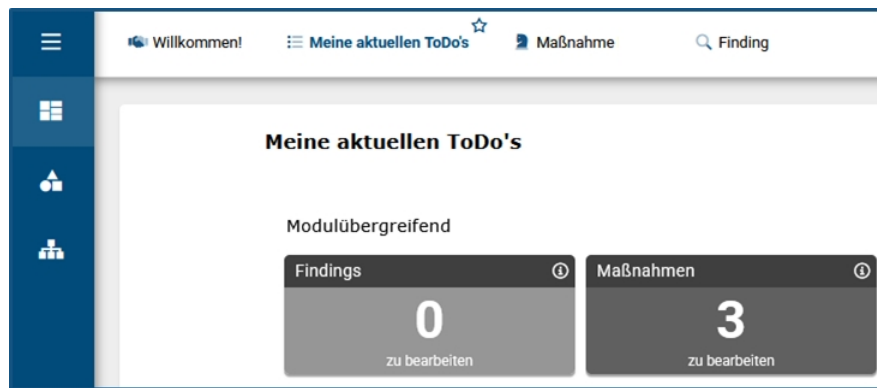
Der Bearbeiter hat zwei Möglichkeiten ein zu bearbeitendes *Finding* zu öffnen.

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

4

← Erfassung

► Abgeschlossen

Finding Details

Datum der Meldung

31.07.2025

zu behandeln bis

11.09.2025

1

Art des Findings

Beobachtung

Empfehlung

Verbesserungswunsch

Unwesentliche Nichtkonformität

Wesentliche Nichtkonformität

Finding für diese Assets:

Name	Asset-Typ	Besch...
Gruppe	Unternehmensorganisation	

Beschreibung des Findings

Beim Review der durchgeführten Notfalltests wurde festgestellt, dass das vollständige Testprotokoll für das Jahr 2025 noch nicht im zentralen Dokumentenmanagementsystem abgelegt wurde. Die Durchführung selbst ist dokumentiert, der Ablageprozess war jedoch unvollständig.

Priorität des Findings

Sehr Niedrig

Niedrig

Mittel

Hoch

Kritisch

Behandlung

2

Beschreibung der Behandlung

Das fehlende Testprotokoll wird umgehend im zentralen Dokumentenmanagementsystem abgelegt. Zusätzlich wird der Ablageprozess überprüft und angepasst, um sicherzustellen, dass zukünftig alle Protokolle zeitnah und vollständig erfasst werden.

3

Maßnahme

Keine Zuordnung vorhanden.

Speichern

Speichern und schließen

Schließen

- 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.
- 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.
- Maßnahme:** Das *Finding* wird durch eine *Maßnahme* behandelt. Mehr Informationen über die Erstellung einer Maßnahme unter [Bearbeiter_Maßnahme_-Maßnahme_definieren_&_erstellen](#) Schritt 2.

GBTEC Austria GmbH

127/252

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.

1.11.5 Kontroll-Testing überprüfen & freigeben

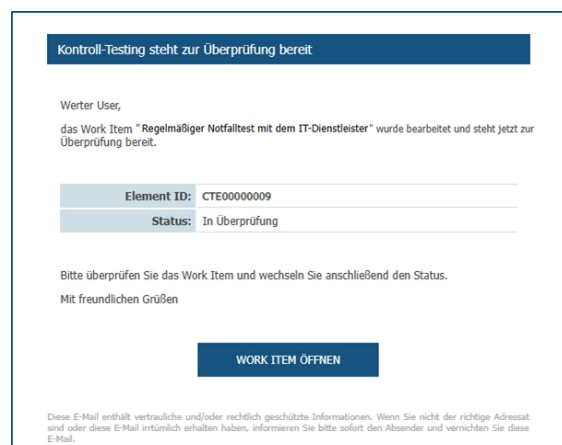
Ein *Kontroll-Testing* wird vom Bearbeiter Kontrolle erstellt und vom Tester dokumentiert. Sobald die Eingaben der Prüfungsergebnisse abgeschlossen sind, kann das *Kontroll-Testing* dem Bearbeiter Kontrolle weitergegeben werden mittels Statusübergang in "Überprüfung".

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".

Kontroll-Testing Details

Element ID: CTE00000007

Name: Regelmäßige Ausfalltests geschäftskritischer IT-Dienstleister (neutral)

Testdurchführung | **Überprüfung** | Abgeschlossen

Testdurchführung | **Kommentare** | Diskussion | Work Item Links | Dokumentation (0)

Kommentare

Kommentar

Tragen Sie hier Ihren Kommentar ein. (0/1000)

Alle Kommentare

2026-01-22, S02, EditorControl:
Das nächste Mal muss der Testingzeitraum kürzer sein.

Speichern Schließen

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.

1.12 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 Freigeber 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](#)

1.12.1 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.

Kontrolle steht zur Genehmigung bereit

Werter User,
 das Work Item "Regelmäßiger Notfalltest mit dem IT-Dienstleister" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	CTR00000019
Status:	In Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.
 Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

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

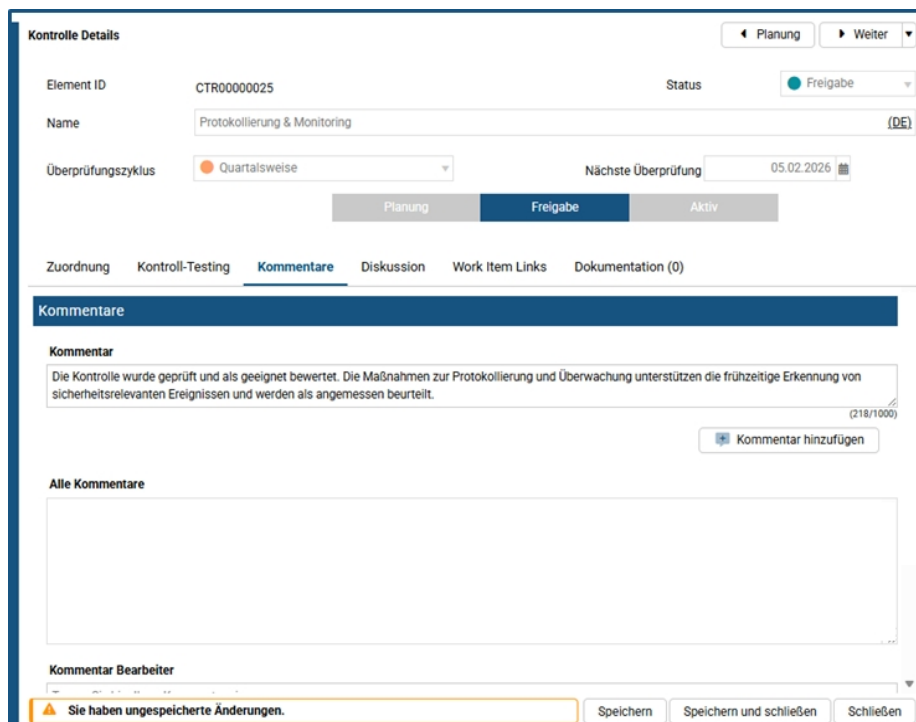
Im oberen Teil des Dashboards "Meine aktuellen ToDo's" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Freigeber Kontrolle noch eine Freigabe durchzuführen hat.



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.

1.13 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.

1.13.1 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

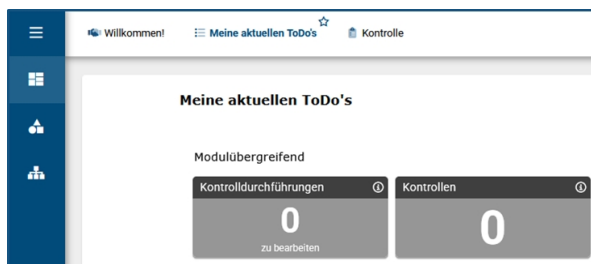
Der Kontrolldurchführer hat zwei Möglichkeiten, eine *Kontrolle* zu öffnen.

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.

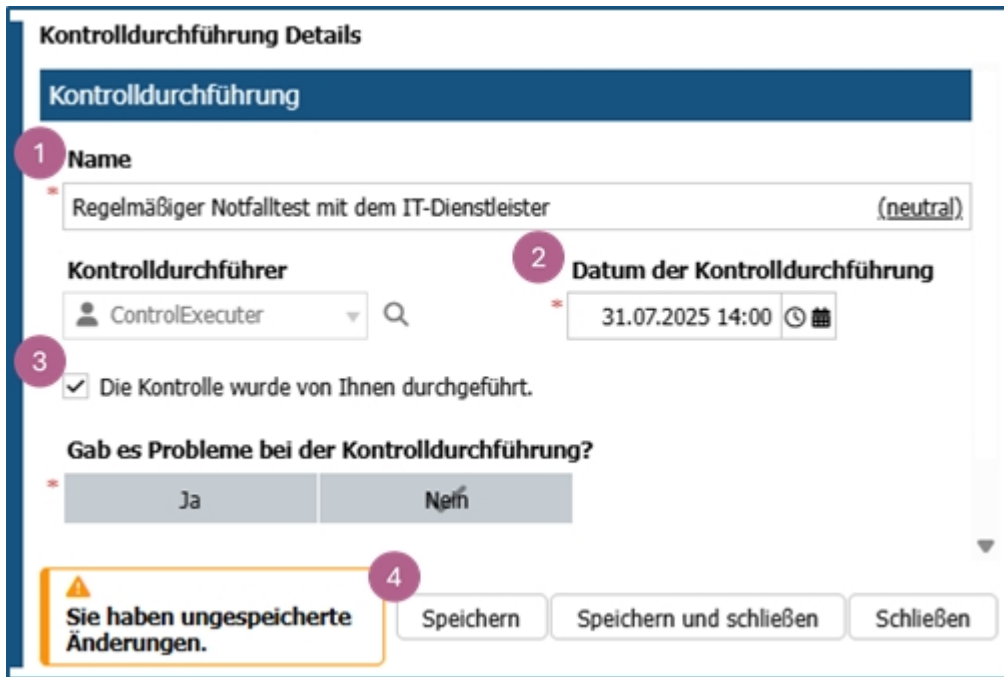


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontrolle* automatisch. Der Kontrolldurchführer steigt direkt in den Tab "*Kontrolldurchführung*" der *Kontrolle* ein.

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 durchgeführten 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 vorgesehen, dass es eine Überprüfung der *Kontrolldurchführung* in BIC GRC gibt. Jedoch wird der Bearbeiter Kontrolle mittels Notifikation darüber informiert, wenn eine *Kontrolldurchführung* abgeschlossen wurde.

Kontrolldurchführung Details
6
▶ Abgeschlossen

Kontrolldurchführung

Name

Regelmäßiger Notfalltest mit dem IT-Dienstleister
(neutral)

Kontrolldurchführer

ControlExecuter
🔍

Datum der Kontrolldurchführung

30.07.2025 14:00
🕒 📅

☑ Die Kontrolle wurde von Ihnen durchgeführt.

Gab es Probleme bei der Kontrolldurchführung?

Ja
Nein

Details der Kontrolldurchführung

Die Kontrolle wurde gemäß dem definierten Ablauf erfolgreich durchgeführt. Der IT-Dienstleister stellte die Nachweise der Blackout-Simulation pünktlich zur Verfügung. Das Testprotokoll war vollständig und nachvollziehbar dokumentiert. Alle kritischen Kommunikationskanäle sowie Wiederanlaufzeiten wurden wie vereinbart geprüft und erfüllt.

5 Geprüfte Dokumente

Dateien hierher ziehen zum Hochladen

	Name	B...	Ersteller	Letzte Änder...	
	Testprotokoll de...		ControlExecuter...	04.08.2025 1...	📎 +

Speichern
Speichern und schließen
Schließen

1.14 Tester

Der Tester hat die Aufgabe in BIC GRC *Kontrollen* in regelmäßigen Abständen auf deren Angemessenheit oder Wirksamkeit zu überprüfen. Tester können dabei alle qualifizierten Personen inner- und außerhalb des Unternehmens sein, wie z.B. interne Revisoren oder Wirtschaftsprüfer. Dabei kann nur ein Tester pro *Kontrolle* nominiert werden. Neben der Dokumentation des *Kontroll-Testings* hat der Tester auch *Findings* aufzuzeigen, um die *Kontrolle* zu verbessern.

Folgende Aufgaben hat ein Tester in BIC GRC:

- [Kontroll-Testing durchführen & bewerten](#)
- [Finding identifizieren & erstellen](#)

1.14.1 Kontroll-Testing durchführen & bewerten

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* vom Bearbeiter Kontrolle gestartet werden.

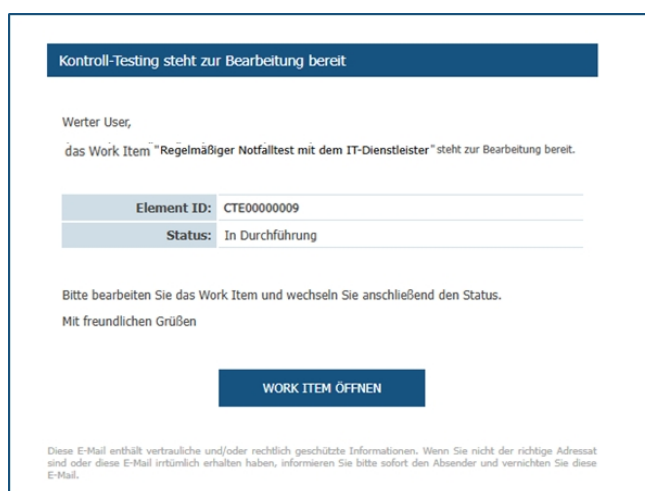
Das *Kontroll-Testing* wird vom Bearbeiter Kontrolle erstellt und nach dem ersten Speichervorgang an den Tester mittels Notifikationsnachweis übergeben.

Schritt 1: Navigation zu Kontrolle

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

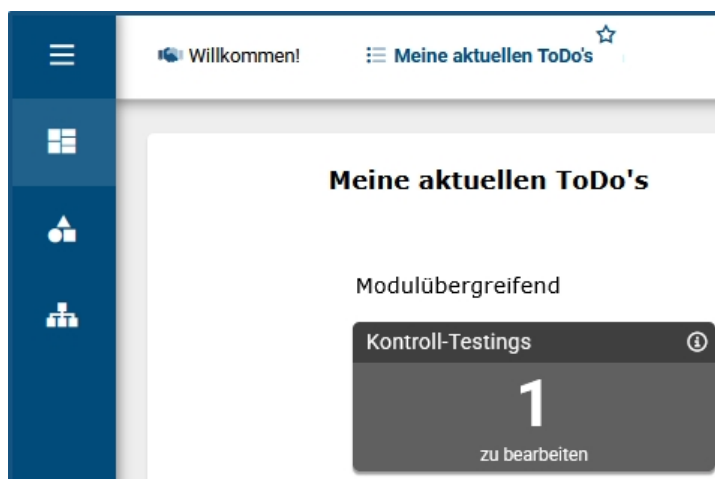
1. Öffnen über Notifikation

Der Tester bekommt eine E-Mail zugesendet, sobald der Bearbeiter Kontrolle ein *Kontroll-Testing* erstellt und erstmalig gespeichert hat. Der Link zu dem spezifischen *Kontroll-Testing* befindet sich in der Notifikation.



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

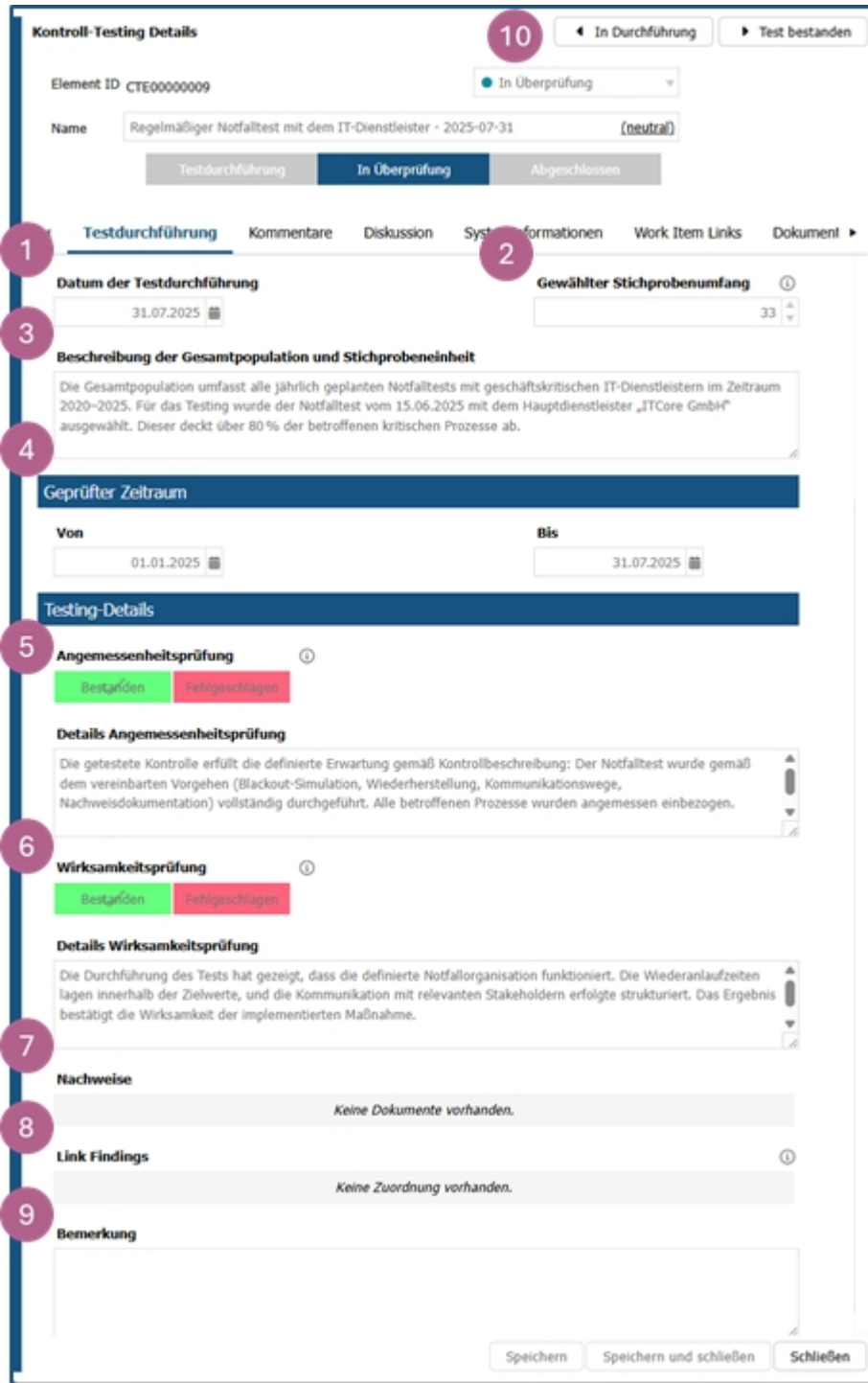
Im oberen Teil des Dashboards "Meine aktuellen ToDo's" sind Kacheln hinterlegt, die die Anzahl an Work Items im jeweiligen Status anzeigen. Bei Klick auf die Kachel wird eine Liste mit allen Work Items in diesem Status geöffnet, für die der Tester ein *Kontroll-Testing* durchzuführen hat.



Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für die *Kontrolle* automatisch. Der Tester steigt direkt in den Tab "*Kontroll-Testing*" der *Kontrolle* ein.

Schritt 2: Details hinterlegen

Durch die Erstellung des Bearbeiter Kontrolle wurden einige Informationen schon hinterlegt.



The screenshot shows the 'Kontroll-Testing Details' form. At the top, there are buttons for 'In Durchführung' (10) and 'Test bestanden'. Below this, the 'Element ID' is 'CTE00000009' and the status is 'In Überprüfung'. The 'Name' field contains 'Regelmäßiger Notfalltest mit dem IT-Dienstleister - 2025-07-31' with a '(neutral)' status. Below the name are three tabs: 'Testdurchführung', 'In Überprüfung', and 'Abgeschlossen'. The 'Testdurchführung' tab is active. It contains several sections: 'Datum der Testdurchführung' (1) with a date picker set to '31.07.2025'; 'Gewählter Stichprobenumfang' (2) with a value of '33'; 'Beschreibung der Gesamtpopulation und Stichprobeneinheit' (3) with a text area containing details about the test scope; 'Geprüfter Zeitraum' (4) with 'Von' and 'Bis' date pickers set to '01.01.2025' and '31.07.2025' respectively; 'Angemessenheitsprüfung' (5) with 'Bestanden' and 'Fehlgeschlagen' buttons and a text area for details; 'Wirksamkeitsprüfung' (6) with 'Bestanden' and 'Fehlgeschlagen' buttons and a text area for details; 'Nachweise' (7) with a message 'Keine Dokumente vorhanden.'; 'Link Findings' (8) with a message 'Keine Zuordnung vorhanden.'; and 'Bemerkung' (9) with a large text area. At the bottom right are buttons for 'Speichern', 'Speichern und schließen', and 'Schließen'.

- 1 **Datum der Testdurchführung:** Das aktuelle Datum, an dem das *Kontroll-Testing* durchgeführt wurde sollte an dieser Stelle angegeben werden. Wird kein Datum vor dem ersten Speichervorgang angegeben, wird das Datum automatisch mit dem tagesaktuellen Datum befüllt.

- 2 **Gewählter Stichprobenumfang:** Wie groß die Stichprobe tatsächlich vom Tester gewählt wurde, muss in diesem Attributsfeld eingetragen werden. Die Zahl kann dabei von dem Vorschlag des Bearbeiter Kontrolle abweichen und muss nicht übernommen werden.
- 3 **Beschreibung der Gesamtpopulation & Stichprobeneinheit:** An dieser Stelle kann der Tester eine Beschreibung angeben, wie er die Stichprobe gewählt hat.

So kann beispielsweise an dieser Stelle angegeben werden, wie die Stichproben ausgewählt wurden und ob es weitere Besonderheiten bei der Stichprobe zu beachten gibt

- 4 **Geprüfter Zeitraum:** Zuletzt muss ein Zeitraum angegeben werden, den der Tester im Rahmen seiner Testingtätigkeit prüfen wird.

Wird die Kontrolle bzw. deren Durchführung von November bis Dezember angesehen und geprüft, muss das Datum von 01.11. bis 31.12. angegeben werden.

- 5 **Angemessenheitsprüfung:** Der Tester kann im Rahmen des *Kontroll- Testings* die Angemessenheit der *Kontrolle* feststellen und mittels "Bestanden" oder "Fehlgeschlagen" einordnen.

Dabei ist beispielsweise zu hinterfragen, ob die *Kontrolle* angemessen ist, um ein spezifisches *Risiko* zu mitigieren oder nicht.

- 6 **Wirksamkeitsprüfung:** Neben der Angemessenheit muss der Tester überprüfen, ob die *Kontrolle* in ihrer Art und Beschaffenheit wirksam ist. Die Einordnung erfolgt hier mittels "Bestanden" oder "Fehlgeschlagen".

- 7 **Nachweise:** An dieser Stelle können Dokumente als Link, Memo oder eine Datei verlinkt werden. Es können 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 verlinkt sich anschließend in dem Attributsfeld.

- 8 **Link Findings:** Der Link, um ein *Finding* zu hinterlegen, ist immer sichtbar. Sollte allerdings die "Angemessenheitsprüfung" oder der "Wirksamkeitsnachweis" fehlgeschlagen sein, muss verpflichtend ein *Finding* angegeben werden. Hierfür kann der Tester über das Icon  ein neues *Finding* erstellen. Mehr dazu unter [Tester -Finding identifizieren & erstellen](#).

- 9 **Bemerkung:** An dieser Stelle kann noch eine ergänzende Bemerkung zum Testing hinterlassen werden. Dabei handelt es sich um Informationen, die an keiner anderen Stelle passend, aber für den Kontext des Testings relevant ist.

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

Nach dem Statuswechsel wird der eingetragene Bearbeiter Kontrolle mittels Notifikation benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.14.2 Finding identifizieren & erstellen

Sollte der Tester während eines *Kontroll-Testings* zu der Erkenntnis kommen, dass entweder die "Angemessenheitsprüfung" und/oder der "Wirksamkeitsnachweis" mit einem negativen Ergebnis abschließen werden, muss der Tester ein *Finding* erstellen.

Schritt 1: Finding aus Kontroll-Testing erstellen

Ein *Finding* kann aus einem *Kontroll-Testing* entstehen. Sollte das Ergebnis der "Angemessenheitsprüfung" oder der "Wirksamkeitsprüfung" im *Kontroll-Testing* als "Fehlgeschlagen" eingeordnet werden, muss verpflichtend ein Finding erstellt werden.

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

Findings 			
	Name	Status	B...
	Dokumentationslücke beim Notfalltestprotokoll 2025	 Erfassung 	

Das *Finding* geht automatisch in dem *Kontroll-Testing* 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 die *Finding* einzigartig.
- 2 GRC-Perspektive:** Die Perspektive wird automatisch aus dem *Kontroll-Testing* übernommen und gesetzt. Sie kann nach dem ersten Speichervorgang nicht mehr verändert werden.
- 3 Bearbeiter:** In das Attribut wird bei der Erstellung automatisch der "Bearbeiter Kontrolle" der *Kontrolle* gesetzt, für das das *Kontroll-Testing* durchgeführt wird.

Der Bearbeiter Kontrolle wird bei Statuswechsel über Notifikation benachrichtigt, sollte es ein Finding geben, sodass er passende *Maßnahmen* setzen kann. Sie auch Bearbeiter Kontrolle - Maßnahmen identifizieren & erstellen

- 4 Datum der Meldung:** Der Tester 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 eine 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 Tester kann im Rahmen von 5 Stufen einordnen, wie bedenklich das *Finding* im Kontext der Angemessenheit oder Wirksamkeit der *Kontrolle* 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 Dashboards verwendet werden kann.
- 10 **Statuswechsel:** Der Tester kann abschließend in den Status "Behandlung" schalten.

Nach dem Statuswechsel wird der eingetragene Bearbeiter Kontrolle mittels Notifikation benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

Anschließend kann der Tester in das *Kontroll- Testing* zurückkehren und mit der Dokumentation des *Kontroll- Testings* fortfahren. [Tester - Kontroll-Testing durchführen & bewerten](#)

1.15 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:

- [Vorfall bewerten & behandeln](#)
- [Business Impact Analyse feststellen & erstellen](#)
- [Business Impact Analyse bearbeiten & bewerten](#)
- [Essentiellen Prozess identifizieren & erstellen](#)
- [Kontinuitätsstrategie herleiten & erstellen](#)
- [Kontinuitätsstrategie bearbeiten & umsetzen](#)

- [Notfallplan herleiten & erstellen](#)
- [Ressource identifizieren & erstellen](#)
- [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](#)

1.15.1 Vorfall bewerten & behandeln

Wenn im Unternehmen ein *Vorfall* gemeldet wurde kann der Bearbeiter DS die Dokumentation, Einschätzung bzw. Bewertung und Behandlung vornehmen. Dabei werden für die Bewertung alle Bearbeiter DS am angegebenen Asset benachrichtigt. Der Bearbeiter DS der sich zuerst dem *Vorfall* annimmt ist offiziell für die Bewertung und Behandlung verantwortlich.

Schritt 1: Navigation zu spezifischem Vorfall

Der Bearbeiter DS hat zwei Möglichkeiten einen zu bewertenden *Vorfall* zu öffnen.

1. Öffnen über Notifikation

Der Bearbeiter DS bekommt eine E-Mail zugesendet, sobald der Ersteller die Meldung abgeschlossen und einen Statusübergang zu "Gemeldet" durchgeführt hat. Der Link zu dem spezifischen *Vorfall* befindet sich in der Notifikation.

Vorfall steht zur Bearbeitung bereit

Werter User,

das Work Item "Unberechtigter Zugriff auf personenbezogene Daten bei externem IT-Dienstleister" steht zur Bearbeitung bereit.

Element ID:	INC00000003
Status:	Gemeldet

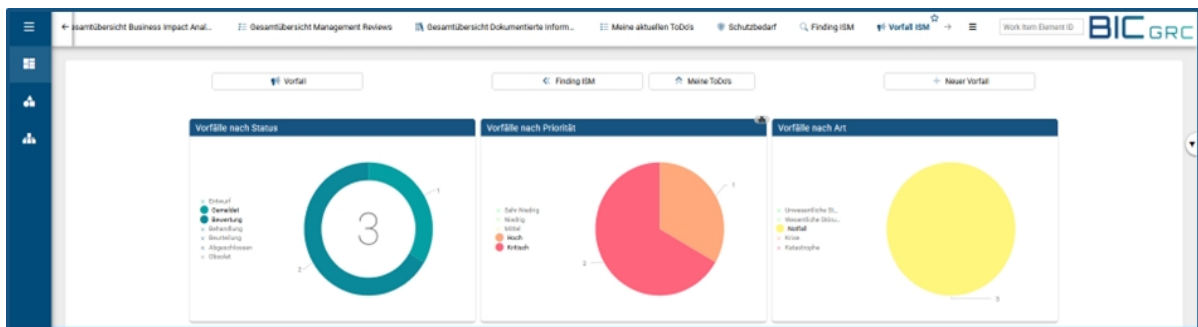
Bitte bearbeiten Sie das Work Item und wechseln Sie anschließend den Status.

Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

2. Öffnen über Dashboard "Vorfall"

Der Bearbeiter DS navigiert über **Dashboards >> Vorfall** zu einem gemeldeten *Vorfall*.

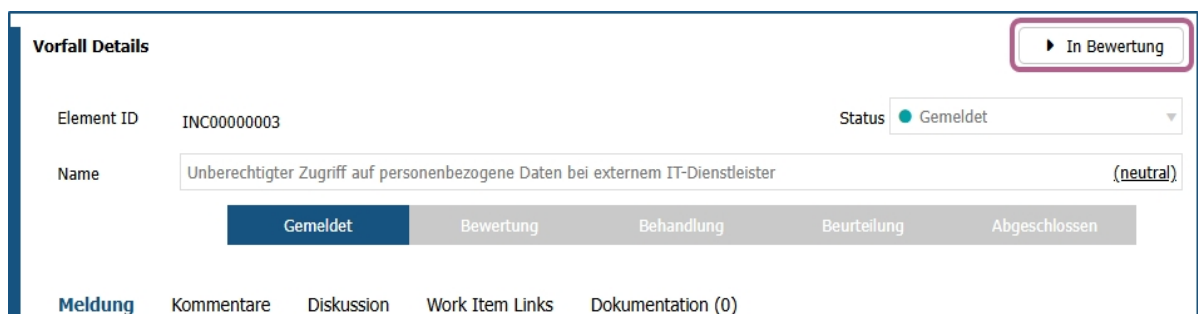


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für den *Vorfall* automatisch.

Schritt 2: Vorfall sichten

Als erstes sollte der Bearbeiter 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.

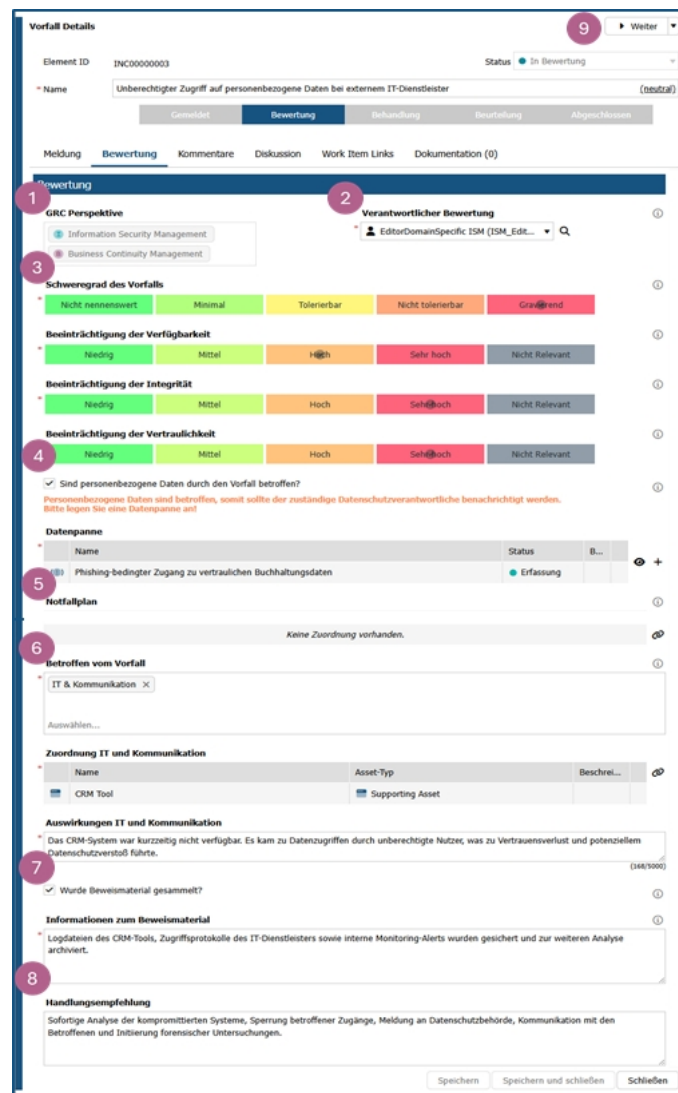
Der Erfasser wird mittels Notifikation über den Statuswechsel informiert.



The screenshot shows the 'Vorfall Details' form with the following fields and elements:

- Element ID:** INC00000003
- Status:** A dropdown menu currently set to 'Gemeldet'.
- Name:** Unberechtigter Zugriff auf personenbezogene Daten bei externem IT-Dienstleister (neutral)
- Process Flow:** A series of buttons: 'Gemeldet' (active), 'Bewertung', 'Behandlung', 'Beurteilung', and 'Abgeschlossen'.
- Navigation:** A row of tabs: 'Meldung' (selected), 'Kommentare', 'Diskussion', 'Work Item Links', and 'Dokumentation (0)'.
- Action:** A button labeled 'In Bewertung' is highlighted with a red box.

Schritt 3: Bewertung durchführen



- 1 **GRC Perspektive:** Es wird die Perspektive vom aktuellen Benutzer automatisch von BIC GRC eingetragen. Anders als in anderen Work Item Typen können hier nur die Perspektiven "Information Security" und/oder "Business Continuity" ausgewählt werden.

Durch die gleichzeitige Aktivierung der Module "Information Security" und "Business Continuity" können auch beide Perspektiven hinterlegt sein.

- 2 **Verantwortlicher Bewertung:** Der Bearbeiter DS der den Statusübergang in "Bewertung" durchführt wird automatisch als Verantwortlicher für die Bewertung hinterlegt.

Sollte er eine andere Person für die Bewertung für geeigneter halten (z.B. aufgrund Länge der Betriebszugehörigkeit oder Expertise) kann er diese eintragen. Der neue Verantwortliche für die Bewertung mittels Notifikation informiert.

- 3 **Schadenseinordnung:** Der Bearbeiter kann in vier Kategorien entscheiden, ob der *Vorfall* zu nachgelagerten Auswirkungen führen kann. Anhand einer Heatmap kann er zwischen vier bzw. fünf Schweregraden oder einer nicht-Relevanz entscheiden. Die vorgegebenen Kategorien sind hierbei immer:

- Schweregrad des Vorfalls
- Beeinträchtigung der Verfügbarkeit
- Beeinträchtigung der Integrität
- Beeinträchtigung der Vertraulichkeit

4 Optional - Personenbezogene Daten & Datenpanne: Sollte zusätzlich das Modul "Data Protection" aktiviert sein werden dem Bearbeiter zusätzlich noch eine Checkbox und ein Link zu der Erstellung eines Work Items *Datenpanne* angezeigt. Sollten personenbezogene Daten betroffen sein kann der Bearbeiter die Checkbox anklicken. Dann muss auch verpflichtend eine *Datenpanne* erstellt werden. Sollte die Checkbox nicht angeklickt sein kann der Bearbeiter trotzdem eine *Datenpanne* erstellen, falls sie im Kontext des *Vorfalls* notwendig ist.

Mehr zu der Erstellung einer Datenpanne unter Standard User - Datenpanne melden & erstellen im zugehörigen Data Protection User Manual.

5 Notfallplan: Ein Work Item *Notfallplan* muss verlinkt werden, wenn es sich im Rahmen der Perspektive "Business Continuity" bei dem *Vorfall* um einen Notfall, eine Krise oder eine Katastrophe handelt.

6 Betroffen vom Vorfall: Der Bearbeiter kann eine oder mehrere "Betroffene vom Vorfall" auswählen, die einen direkten Effekt von dem Vorfall haben oder haben werden.

Abhängig von der Auswahl der Betroffenen muss der Bearbeiter immer eine Zuordnung und Beschreibung

7 Beweismaterial: Falls zu dem *Vorfall* bereits "Beweismaterial" gesammelt worden ist kann diese Checkbox angeklickt werden. Anschließend können in dem Beschreibungsfeld, das nach dem Klicken auf die Checkbox erscheint, weitere "Informationen zu dem Beweismaterial" eingetragen werden.

8 Handlungsempfehlung: Final können noch Handlungsempfehlungen vom Bearbeiter DS angegeben werden.

9 Statuswechsel: Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu in "Behandlung" durchgeführt.

Der Bearbeiter DS wird automatisch in den nächsten Tab weitergeführt.

Schritt 4: Behandlung definieren

Vorfall Details ◀ Bewertung ▶ Beurteilung

Element ID: INC00000003 Status: ● Behandlung

Name: Unberechtigter Zugriff auf personenbezogene Daten bei externem IT-Dienstleister (neutral)

Gemeldet Bewertung **Behandlung** Beurteilung Abgeschlossen

Meldung ! Bewertung **Behandlung** Verlaufsprotokoll Kommentare Diskussion Work Item Links Dokumentation (0)

Behandlung

1 Beschreibung der Behandlung !

* Nach Bekanntwerden des Vorfalls wurde der betroffene Zugriff beim externen IT-Dienstleister umgehend überprüft und vorübergehend deaktiviert. Die relevanten Zugriffsprotokolle wurden analysiert, um Umfang und Zeitraum des möglichen Zugriffs festzustellen. Zusätzlich wurde der betroffene Dienstleister kontaktiert und zur Stellungnahme sowie zur Überprüfung der eigenen Zugriffskontrollen aufgefordert. Interne Fachbereiche (IT-Sicherheit und Datenschutz) wurden informiert und in die weitere Analyse eingebunden.

2 Maßnahme !

Name	Status	Be...
Schulungen	● Umsetzung	!

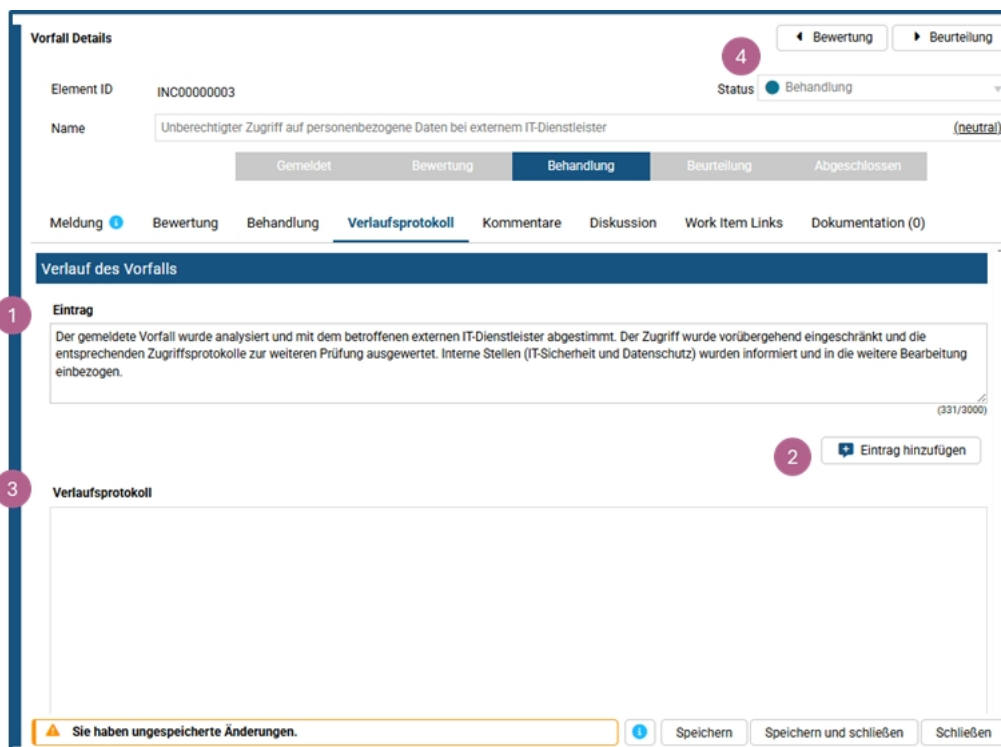
3

! Sie haben ungespeicherte Änderungen. ! Speichern Speichern und schließen Schließen

- 1 Beschreibung der Behandlung:** Nach der Bewertung des aktuellen Standes muss der Bearbeiter DS angeben, wie er vorhat den *Vorfall* zu behandeln. Dafür sollte er schriftlich eine "Beschreibung der Behandlung" hinterlegen.
- 2 Maßnahme:** Der Bearbeiter DS kann ein oder mehrere *Maßnahmen* mittels des Icons verlinken oder eine neue *Maßnahme* erstellen. Mehr zu der Erstellung einer Maßnahme unter [Bearbeiter Maßnahme - Maßnahme definieren & erstellen](#).
- 3 Speichervorgang:** Nach der Hinterlegung der notwendigen Informationen kann das Work Item gespeichert werden.

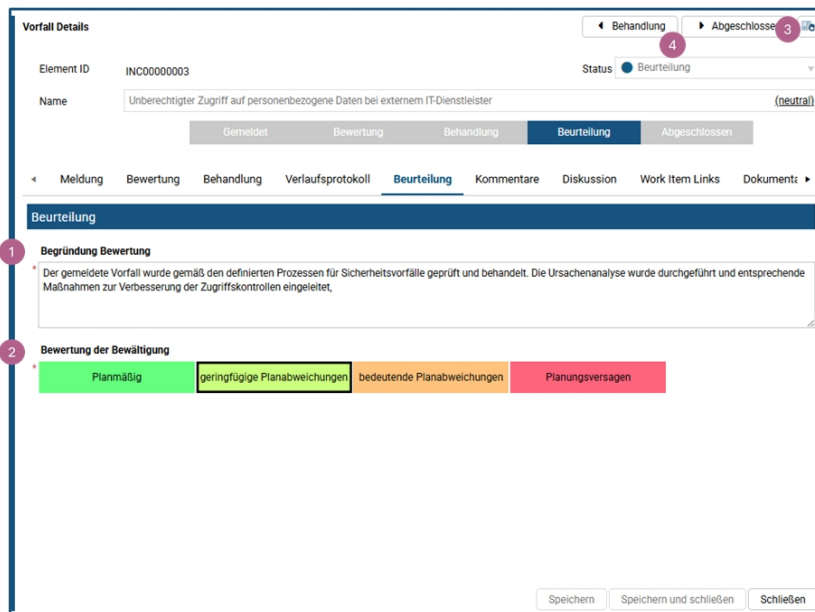
Schritt 5: Verlaufsprotokoll dokumentieren

Nach der Eingabe der Informationen im Tab "Behandlung" kann der Bearbeiter DS in den Tab "Verlaufsprotokoll" wechseln.



- 1 **Eintrag:** Der Bearbeiter DS sollte dokumentieren wie der Verlauf der Behandlung des *Vorfalles* war. Für die genaue Nachverfolgung kann er einzelne Einträge verfassen.
- 2 **Eintrag hinzufügen:** Sobald der Bearbeiter DS einen Eintrag verfasst hat kann er mittels des Buttons "Eintrag hinzufügen" den Eintrag posten.
- 3 **Verlaufsprotokoll:** Sobald der Button geklickt worden ist wird der Beitrag im Verlaufsprotokoll angezeigt. Der Eintrag ist Read Only und wird automatisch mit dem Bearbeiter und dem aktuellen Datum befüllt.
- 4 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu in "Behandlung" durchgeführt.
Der Bearbeiter DS wird automatisch in den nächsten Tab weitergeführt.

Schritt 6: Beurteilung durchführen



- 1 **Begründung Bewertung:** Der Bearbeiter DS sollte angeben zu welcher Gesamtbewertung er im Rahmen des *Vorfalles* gekommen ist.
- 2 **Bewertung der Bewältigung:** Neben einer schriftlichen Begründung der Bewertung muss der Bearbeiter eine Auswahl in der vorbereiteten Heatmap treffen. Mittels vier Stufen kann eingeordnet werden, wie kritisch der *Vorfall* schlussendlich war.
- 3 **Security- Risiko:** Wenn es zu einer "Bedeutenden Planabweichung" oder "Planungsversagen" durch den *Vorfall* gekommen ist, wird geraten ein *Security-Risiko* durch den Button in der oberen rechten Fensterseite zu erstellen. Mehr Informationen zu der Erstellung eines *Security-Risikos* unter [Bearbeiter_Risiko - Security-Risiko identifizieren & erstellen](#).
- 4 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Abgeschlossen" durchgeführt.

Nach dem Speichervorgang wird der Erfasser mittels Notifikation benachrichtigt.

Schritt 7: Report generieren

Nachdem der *Vorfall* in den Status "Abgeschlossen" geschaltet wurde können der Bearbeiter DS und der Freigeber DS einen Bericht generieren.

Vorfall Details

Behandlung

Report

Element ID

INC00000003

Status

Abgeschlossen

Name

Unberechtigter Zugriff auf personenbezogene Daten bei externem IT-Dienstleister

(neutral)

Gemeldet

Bewertung

Behandlung

Beurteilung

Abgeschlossen

Meldung

Bewertung

Behandlung

Verlaufsprotokoll

Beurteilung

Kommentare

Diskussion

Work Item Links

Dokumente

Beurteilung

Begründung Bewertung

Der gemeldete Vorfall wurde gemäß den definierten Prozessen für Sicherheitsvorfälle geprüft und behandelt. Die Ursachenanalyse wurde durchgeführt und entsprechende Maßnahmen zur Verbesserung der Zugriffskontrollen eingeleitet.

Bewertung der Bewältigung

Planmäßig

geringfügige Planabweichungen

bedeutende Planabweichungen

Planungsversagen

Speichern

Speichern und schließen

Schließen

Der Bericht ist eine Zusammenfassung des gesamten *Vorfall*.

Die Generierung des Berichts wird in der oberen rechten Fensterseite des Work Items durchgeführt. Bei der Ausgabedatei handelt es sich um ein PDF.

1.15.2 Business Impact Analyse feststellen & erstellen

Eine *Business Impact Analyse* kann in dem Modul Business Continuity Management nur aus einem *Essentiellen Prozess* von einem Bearbeiter DS erstellt werden. Mehr unter [Bearbeiter_DS_-_Essentiellen Prozess identifizieren & erstellen](#).

Schritt 1: Business Impact Analyse aus Essentiellen Prozess erstellen

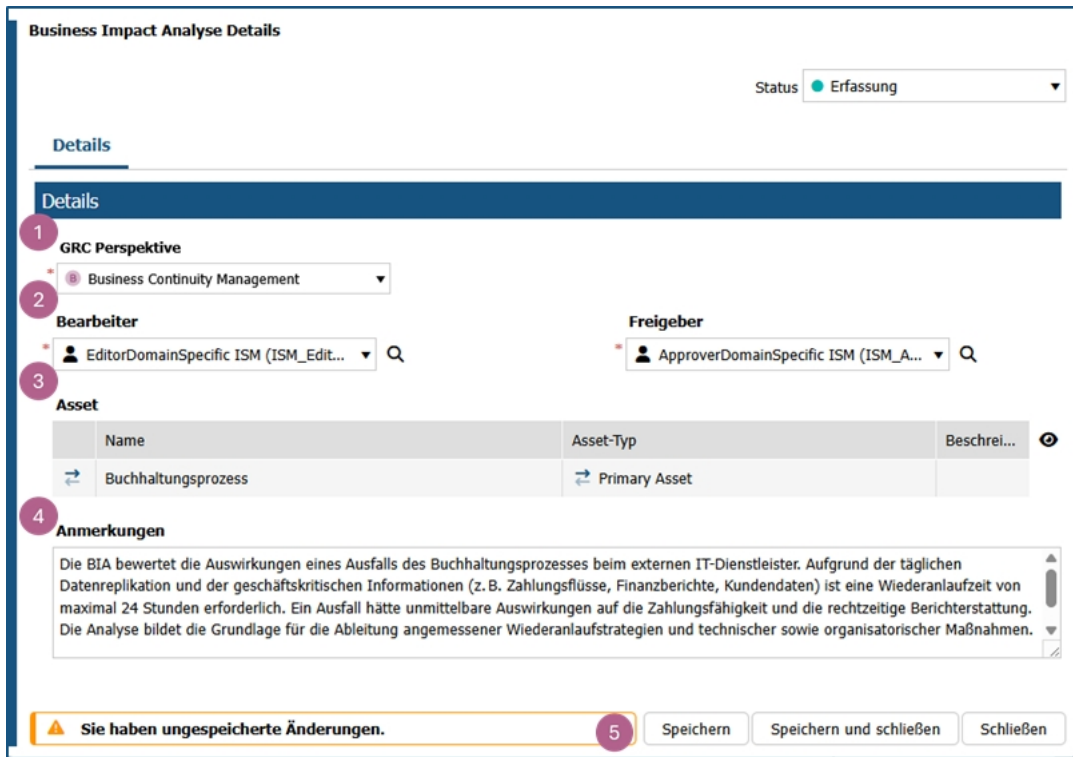
Der Bearbeiter DS kann die *Business Impact Analyse* direkt aus dem Work Item *Essentiellen Prozess* erstellen. Dafür erstellt er mittels des Icons  eine *Business Impact Analyse*.

Business Impact Analyse

Name	Status	A...
Controllingprozess	Erfassung	

+

Schritt 2: Details hinterlegen



- 1 **GRC- Perspektive:** Die Perspektive wird automatisch aus dem *Essentiellen Prozess* übernommen und gesetzt.
- 2 **Verantwortliche Personen:** Der Bearbeiter DS hat einen "Bearbeiter" zu hinterlegen, und zusätzlich einen "Freigeber DS", der für die Freigabe der *Business Impact Analyse* verantwortlich ist.

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

Der Bearbeiter DS wird nach der Erstellung aus dem *Essentiellen Prozess* automatisch als Bearbeiter vorgeschlagen und in das Attribut "Bearbeiter" übertragen.

Damit auf einen Blick erkennbar ist, von wem die *Business Impact Analyse* erstellt wurde, wird auch der Ersteller in diesem Abschnitt angezeigt.

- 3 **Asset:** Das Asset wird aus dem Work Item übernommen, aus dem die *Business Impact Analyse* erstellt wurde.

Auch hier gilt weiterhin der Filter des Assets auf den Typen "Primary Asset"

- 4 **Anmerkung:** Hier können zusätzliche Informationen hinterlegt werden, wenn es passende Anmerkungen geben sollte.
- 5 **Speichern:** Sobald alle Informationen eingetragen wurden kann die *Business Impact Analyse* gespeichert werden.

Wenn der Ersteller der *Business Impact Analyse* gleichzeitig der Bearbeiter DS ist, kann er mit dem nächsten Schritt [Bearbeiter DS - Business Impact Analyse bearbeiten & bewerten](#) fortfahren.

1.15.3 Business Impact Analyse bearbeiten & bewerten

Eine *Business Impact Analyse* kann in dem Modul Business Continuity Management nur aus einem *Essentiellen Prozess* von einem Bearbeiter DS erstellt werden. Mehr unter Bearbeiter DS - Essentiellen Prozess identifizieren & erstellen.

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

Optional Schritt 1: Navigation zu spezifischer Business Impact Analyse nach Fremderstellung

Der Bearbeiter hat zwei Möglichkeiten, eine zu bearbeitende *Business Impact Analyse* 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 *Business Impact Analyse* befindet sich in der Notifikation.

Business Impact Analyse wurde angelegt

Werter User,

das Work Item "Buchhaltungsprozess" wurde angelegt.

Element ID:	BIA00000001
Status:	Erfassung

Diese Nachricht dient nur zur Information und impliziert keinen Handlungsbedarf.

Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

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 Bewertung durchzuführen hat.

Meine aktuellen ToDo's

Information Security Management

Schutzbedarfe

1

Modulübergreifend

Security-Risiken

6

Business Impact Analysen

1

Maßnahmen

0

Management Reviews

1

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

Optional Schritt 2: Überprüfung der Eingaben des Erstellers

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.

Business Impact Analyse Details

Element ID: BIA00000003

Status: Erfassung

Name: Production of Electric Drive Axles

Überprüfungszyklus: --

Nächste Überprüfung: --

Erfassung Freigabe Abgeschlossen

Details Bewertung Wiederherstellung Kommentare Diskussion Work Item Links Dokumentation (0)

Diskussion

Teilnehmer (leseberechtigt)

Suchtext hier eingeben

Beiträge

Neuer Beitrag

Eingaben bitte nochmals überprüfen.

Sie haben ungespeicherte Änderungen.

Speichern Speichern und schließen Schließen

Schritt 3: Bewertung durchführen

Nach der Durchsicht kann der Bearbeiter DS in den Tab "Bewertung" wechseln.

Business Impact Analyse Details Weiter

Element ID: BIA00000003 Status: Erfassung

1 Name: Production of Electric Drive Axles (neutral)

2 Überprüfungszyklus: Jährlich Nächste Überprüfung: Erfassung Freigabe Abgeschlossen

Details **Bewertung** Wiederherstellung Kommentare Diskussion Work Item Links Dokumentation (0)

3 **Finanzielle Auswirkungen** keine

Gering 240,0 % 0,0 h

Mittel 240,0 % 0,0 h

Hoch 240,0 % 0,0 h

Sehr hoch 240,0 % 0,0 h

Begründung der Bewertung

3 **Beeinträchtigung der Aufgabenerfüllung** keine

Gering 240,0 % 0,0 h

Mittel 240,0 % 0,0 h

Hoch 240,0 % 0,0 h

Sehr hoch 240,0 % 0,0 h

⚠ Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

Business Impact Analyse Details Weiter

Element ID: BIA00000003 Status: Erfassung

Name: Production of Electric Drive Axles (neutral)

Überprüfungszyklus: Jährlich Nächste Überprüfung: Erfassung Freigabe Abgeschlossen

Details **Bewertung** Wiederherstellung Kommentare Diskussion Work Item Links Dokumentation (0)

3 **Negative innen- oder Außenwirkung** keine

Gering 240,0 % 0,0 h

Mittel 240,0 % 0,0 h

5 Hoch 240,0 % 0,0 h

Sehr hoch 240,0 % 0,0 h

6 Begründung der Bewertung

3 **Beeinträchtigung der persönlichen Unversehrtheit** keine

Gering 240,0 % 0,0 h

Mittel 240,0 % 0,0 h

5 Hoch 240,0 % 0,0 h

Sehr hoch 240,0 % 0,0 h

⚠ Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

- 1 **Name:** Der Name wird nach dem ersten Speichervorgang durch den Ersteller automatisch festgelegt.

Der Name ergibt sich aus dem "Neutral" gepflegten Namen des Assets.

- 2 **Überprüfungszyklus:** Der Bearbeiter muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft eine *Business Impact Analyse* zurück in den Status "Erfassung" geschaltet wird, um die *Business Impact Analyse* in regelmäßigen Zeitabständen zu evaluieren.

Das Attributsfeld "Nächste Überprüfung" wird automatisch von BIC GRC gesetzt.

3 Bewertungskategorien: Der Bearbeiter DS kann unter dem Gesichtspunkt unterschiedlicher Faktoren die *Business Impact Analyse* durchführen. Folgende Bewertungskategorien stehen ihm zu Verfügung:

- Finanzielle Auswirkung
- Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze, Vorschriften, Verträge
- Negative Innen- oder Außenwirkung
- Beeinträchtigung der persönlichen Unversehrtheit

Für die Bewertung der *Business Impact Analyse* können Bewertungen zu ein oder mehrere der genannten Kategorien hinterlegt werden.

4 Keine Bewertung: Soll keine Bewertung zu einer Kategorie durchgeführt werden, kann die Checkbox im blauen Label angeklickt werden.

Wird die Checkbox benutzt, wird der ganze Abschnitt zu der Bewertung der Kategorie ausgeblendet.

5 Bewertung: Die Bewertung jeder einzelnen Kategorie wird jeweils mittels vier Slidern eingeschätzt.

Beeinträchtigungsgrad	Farbcode	Beschreibung
Gering	Rot	Kein wesentlicher Einfluss
Mittel	Orange	Erste Beeinträchtigungen
Hoch	Gelbgrün	Relevante Betriebsstörungen
Sehr hoch	Dunkelgrün	Kritische Auswirkung

Der Benutzer kann standardmäßig zwischen 0 und 240 Stunden wählen.

Es gibt zwischen den Eingaben der Slidern eine Abhängigkeit. Diese äußert sich durch den Umstand dass beispielsweise eine Einschätzung von "Mittel" nie unter der Einschätzung "Gering" liegen kann.

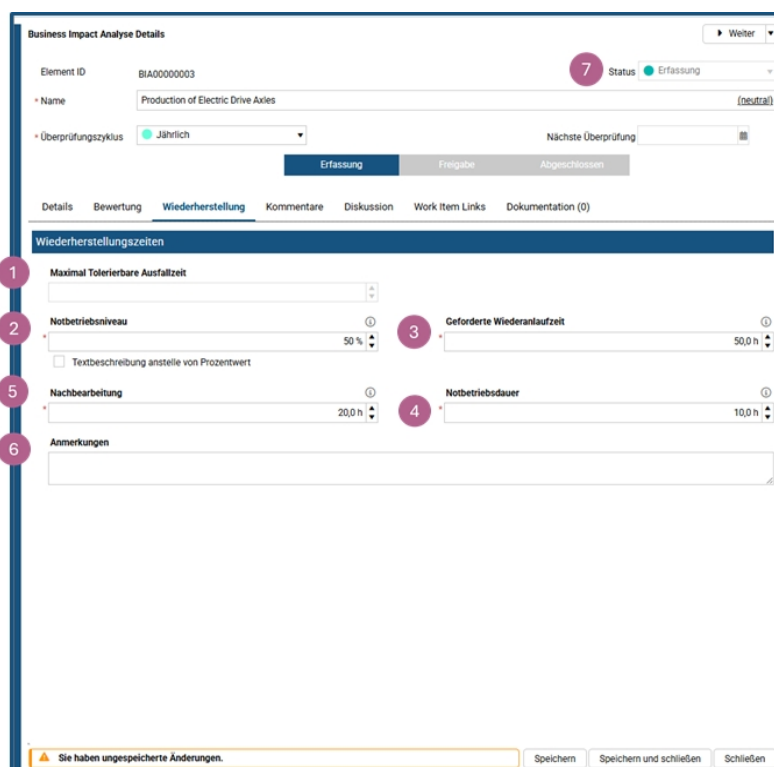
Warum ist "Gering" rot? Rot bedeutet in dem Kontext, dass keine große Ausfalltoleranz besteht, also schon kurze Ausfälle haben Folgen. Oder mit anderen Worten: Ein Prozess, der nach beispielsweise 36 h bereits eine mittlere Beeinträchtigung erfährt, ist kritischer. Fazit: Die Farbskala ist nicht auf die Höhe der Beeinträchtigung bezogen, sondern auf die Kritikalität des Prozesses in Bezug auf Zeit.

- 6 **Begründung der Bewertung:** Für jede einzelne Bewertung kann eine eigene Begründung der Bewertung eingegeben werden.

Für die Eingaben im Tab "Wiederherstellung" müssen alle Kategorien eine Bewertung und eine Beschreibung haben, wenn sie nicht alternativ die Checkbox "Keine" gesetzt haben.

Schritt 4: Wiederherstellung dokumentieren

Nach einem erneuten Speichervorgang kann der Bearbeiter DS in den Tab "Wiederherstellung" wechseln.



- 1 **Maximal Tolerierbare Ausfallzeit:** Dabei handelt es sich um ein Attribut, dass automatisch mittels einer Minimum-Formel von BIC GRC berechnet wird. Bei dem Minimum werden alle Bewertungskategorien analysiert und der minimalste Wert des Beeinträchtigungsgrades "Hoch" herangezogen.

Das Attribut ist Read Only und kann nicht vom Bearbeiter DS manuell angepasst werden.

- 2 **Notbetriebsniveau:** Der Bearbeiter DS hinterlegt den Mindestgrad an Leistungsfähigkeit, mit dem der Prozess im Notbetrieb fortgeführt werden kann, um wesentliche Geschäftsfunktionen aufrechtzuerhalten.

In Prozent zur Normalleistung oder alternativ in Textform (z. B. "manuelle

Bearbeitung mit reduzierter Kapazität").

- 3 **Geforderte Wiederanlaufzeit (RTO):** Dieses Attribut gibt die Zeitspanne an, innerhalb derer der Prozess nach Eintritt der Störung wieder in Betrieb genommen werden muss, um kritische Auswirkungen zu vermeiden.

Die "Geforderte Wiederanlaufzeit" sollte unterhalb der maximal tolerierbaren Ausfallzeit. Sollte dies nicht der Fall sein wird dies dem Bearbeiter DS mittels eigenem Label angezeigt.

- 4 **Notbetriebsdauer:** Zeitraum, über den der Prozess im Notbetrieb auf dem definierten Notbetriebsniveau aufrechterhalten werden muss, bis zur vollständigen Wiederherstellung der Normalfunktion.
- 5 **Nachbearbeitung:** Der Bearbeiter DS hinterlegt die Zeit, die nach Wiederanlauf zusätzlich benötigt wird, um aufgelaufene Rückstände abzarbeiten oder Qualitäts- und Compliance-Anforderungen zu erfüllen.
- 6 **Anmerkungen:** Hier können zusätzliche Informationen hinterlegt werden, wenn es passende Anmerkungen geben sollte.
- 7 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen aus Tab "Bewertung" (Schritt 3) und Tab "Wiederherstellung" (Schritt 4) ein Statusübergang zu in "Freigabe" durchgeführt.

Der Freigeber DS wird mittels Notifikation automatisch über den Statusübergang informiert.

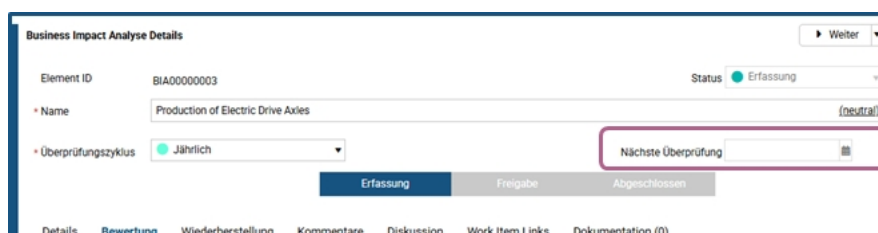
Nach der Eingabe aller notwendigen Informationen kann das Work Item gespeichert werden bevor das Fenster manuell geschlossen wird.

Schritt 5: Update durchführen

Der Bearbeiter sollte die *Business Impact Analyse* regelmäßig dahingehend überprüfen, ob die Angaben noch korrekt sind.

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 die *Business Impact Analyse* im Status "Aktiv" in den Status "Erfassung" geschaltet 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 *Business Impact Analyse* 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.

1.15.4 Essentiellen Prozess identifizieren & erstellen

Durch die Definition eines *Essentiellen Prozesses* unterstützt der Bearbeiter DS, um die Widerstandsfähigkeit einer Organisation sicherzustellen.

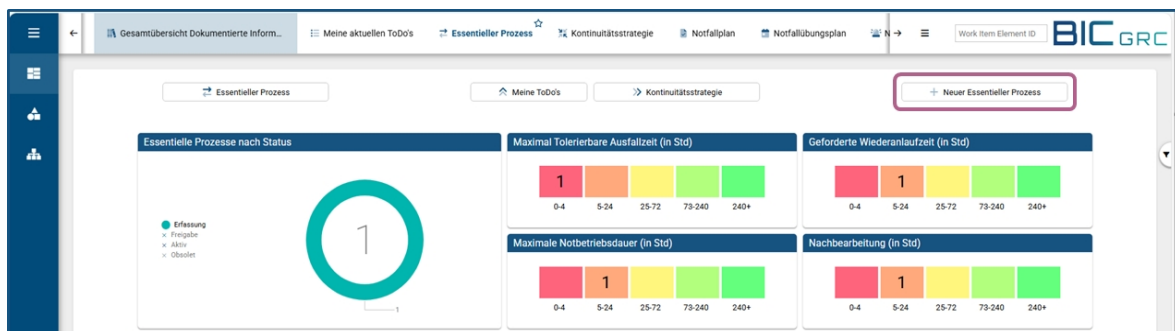
Der *Essentielle Prozess* kann nur an Assets des Typen "Primary Asset" erstellt werden, mit dem zusätzlichen Tag "Prozess".

Schritt 1: Essentiellen Prozess erstellen

Der Bearbeiter DS kann in BIC GRC an mehreren Stellen *Essentielle Prozesse* erstellen.

1. Erstellen über Dashboard "Essentieller Prozess"

Der Bearbeiter navigiert über die Menüleiste zu **Dashboards >> Essentieller Prozess >> "Neuer Essentieller Prozess"**. Die Erstellung eines neuen *Essentiellen Prozesses* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

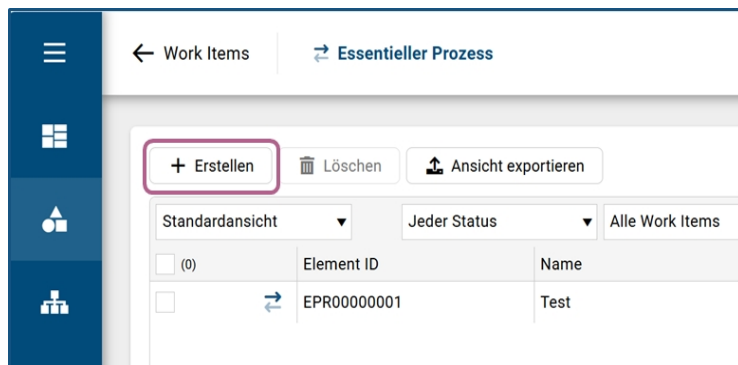


Ein neues Fenster öffnet sich anschließend automatisch.

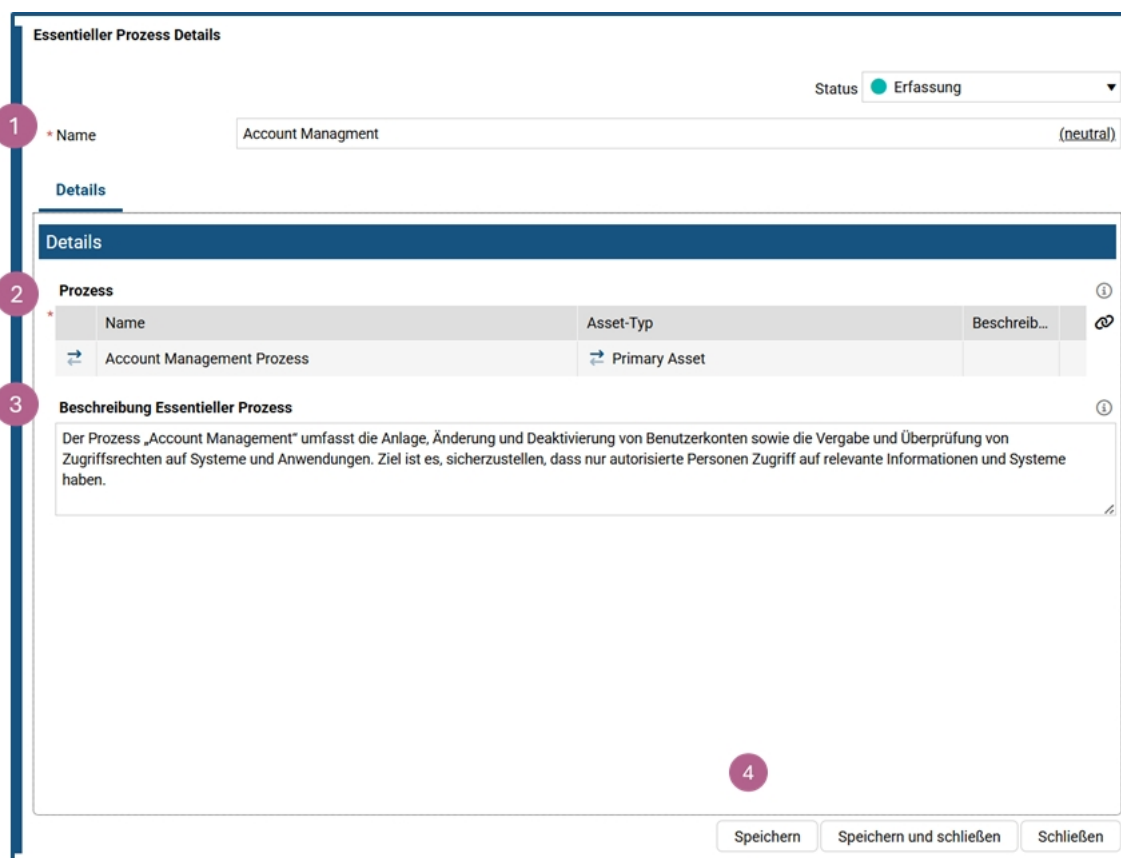
2. Erstellung über Work Item List

Der Bearbeiter navigiert über die Menüleiste zu **Work Items** >> **Essentieller Prozess** >> "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 *Essentiellen Prozess* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist der *Essentielle Prozess* einzigartig.

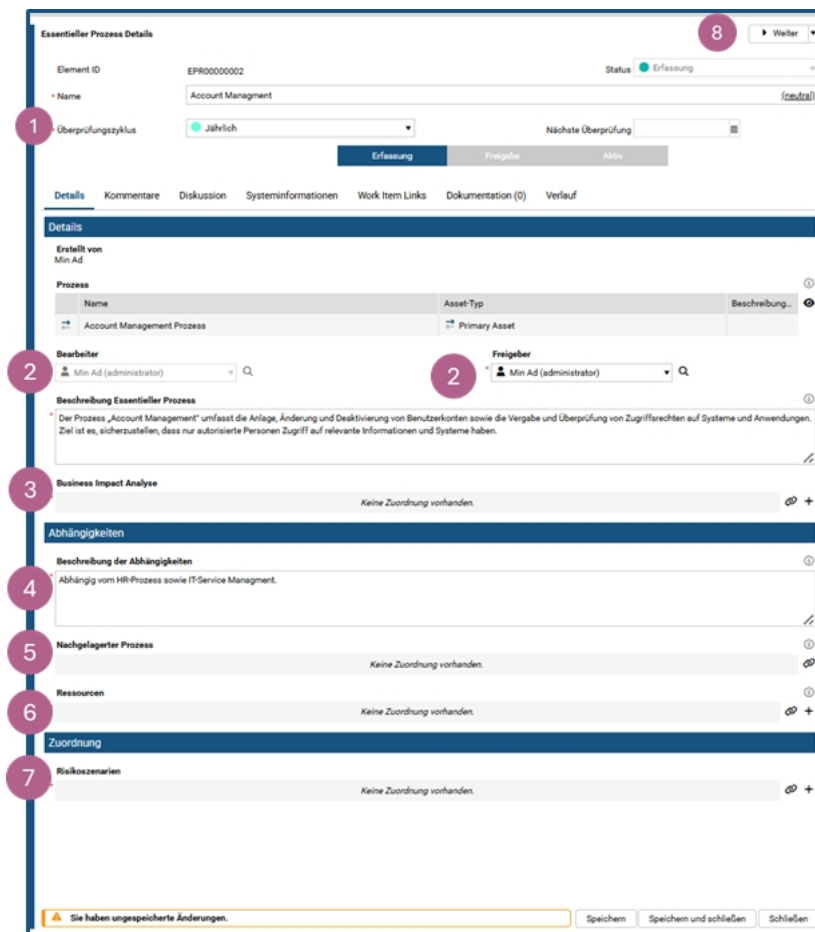
2 Prozess: Der Bearbeiter DS kann mittels des Icons  einen Prozess verlinken.

Der "Prozess"-Link wird automatisch befüllt, wenn die Erstellung über die Asset-Ansicht (2) erstellt worden ist.

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 **Beschreibung:** Anschließend ist eine Beschreibung des *Essentiellen Prozesses* zu hinterlegen. Alle User, die im Workflow des *Essentiellen Prozesses* nachgelagert sind, orientieren sich an dieser Beschreibung, daher sollte sie so viele notwendige Informationen und Daten wie möglich enthalten.
- 4 **Speichern:** Sobald die Informationen angegeben sind, kann der Bearbeiter DS speichern.

Schritt 3: Eingaben vervollständigen



The screenshot shows the 'Essentieller Prozess Details' form. The form is titled 'Essentieller Prozess Details' and has a status of 'Erfassung'. The form contains several sections and fields:

- Element ID:** EPR00000002
- Name:** Account Management
- Überprüfungszyklus:** Jährlich (annotated with 1)
- Nächste Überprüfung:** (empty field)
- Status:** Erfassung (annotated with 8)
- Details:** A section with tabs for Details, Kommentare, Diskussion, Systeminformationen, Work Item Links, Dokumentation (0), and Verlauf.
- Erstellt von:** Min Ad
- Prozess:** A table with columns Name, Asset-Typ, and Beschreibung. The first row is 'Account Management Prozess' with 'Primary Asset' (annotated with 2).
- Bearbeiter:** Min Ad (administrator) (annotated with 2)
- Freigeber:** Min Ad (administrator) (annotated with 2)
- Beschreibung Essentieller Prozess:** A text area with a description of the process (annotated with 3).
- Business Impact Analyse:** A section with a table (annotated with 4).
- Abhängigkeiten:** A section with a table (annotated with 5).
- Nachgelagerter Prozess:** A section with a table (annotated with 6).
- Ressourcen:** A section with a table (annotated with 7).
- Zuordnung:** A section with a table (annotated with 7).
- Risikozustand:** A section with a table (annotated with 7).

At the bottom of the form, there is a warning message: 'Sie haben ungespeicherte Änderungen.' and buttons for 'Speichern', 'Speichern und schließen', and 'Schließen'.

- 1 **Überprüfungszyklus:** Der Bearbeiter muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft ein *Essentieller Prozess* zurück in den Status "Überprüfung" geschaltet wird, um den *Essentieller Prozess* in regelmäßigen Zeitabständen zu evaluieren.

Das Attributsfeld "Nächste Überprüfung" wird automatisch von BIC GRC gesetzt.

- 2 **Verantwortliche Personen:** Der Bearbeiter wird automatisch in dem Feld "Bearbeiter" hinterlegt und kann nicht mehr geändert werden. Ein "Freigeber", der für die Freigabe des *Essentieller Prozess* 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.

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

- 3 **Business Impact Analyse:** Für jeden *Essentiellen Prozess* ist verpflichtend eine *Business Impact Analyse* zu erstellen, um die konkrete Auswirkung eines Prozessausfalls systemisch bewerten zu können.

Sobald eine *Business Impact Analyse* erstellt oder verlinkt wurde die sich im Status "Aktiv" befindet werden aus dem verlinkten Work Item Informationen übernommen bzw. automatisch von BIC GRC berechnet, wie Wiederherstellungsdaten, Schutzbedarf Verfügbarkeit und die Kritikalität des *Essentiellen Prozesses*.

Es werden dem Bearbeiter nur *Business Impact Analysen* angezeigt, die an seinem Prozess erstellt wurden. Sollte es keine passende *Business Impact Analyse* geben, muss der Bearbeiter eine erstellen.

Mehr Informationen unter [Bearbeiter DS - Business Impact Analyse feststellen & erstellen](#).

- 4 **Beschreibung der Abhängigkeiten:** In diesem Beschreibungsfeld kann der Bearbeiter DS erklären und dokumentieren, wie der Zusammenhang zu anderen Prozessen aussieht.

- 5 **Nachgelagerter Prozess:** Der Bearbeiter DS kann "Nachgelagerte Prozesse" angeben, um anderen Benutzern die Abhängigkeit zu anderen Prozessen besser anzeigen zu können.

Es werden dem Bearbeiter dabei nicht "Primary Assets" aus der Assethierarchie angezeigt, sondern andere Work Items des Typen *Essentieller Prozess*.

- 6 **Ressourcen:** An dieser Stelle kann der Bearbeiter Work Items des Typen *Ressource* erstellen oder verlinken, die benötigt werden, um den *Essentiellen Prozess* aufrecht zu erhalten.

Ressourcen mit der Ressourcenkategorie "Standardressource" werden dem Bearbeiter DS zur Auswahl vorgeschlagen.

Mehr Informationen unter [Bearbeiter DS - Ressource identifizieren & erstellen](#).

- 7 **Risikoszenarien:** Zuletzt kann der Bearbeiter DS ein oder mehrere Risikoszenarien zuordnen.

Dabei werden dem Bearbeiter DS nur Risikoszenarien vorgeschlagen bei denen beim

Attribut "Betroffene Schutzziele" der Listenwert "Verfügbarkeit" ausgewählt wurde.

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

Der Freigeber DS wird mittels Notifikation 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 Freigeber DS ein Kommentar in dem Tab "Kommentar" hinterlassen und den *Essentiellen Prozess* erneut in den Status "Erfassung" setzen. Der Bearbeiter DS wird über diesen Vorgang mittels Notifikation benachrichtigt.

Schritt 4: Update durchführen

Der Bearbeiter sollte den *Essentieller Prozess* regelmäßig dahingehend überprüfen, ob die Angaben noch korrekt sind.

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 der *Essentieller Prozess* im Status "Aktiv" in den Status "Erfassung" geschaltet 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 der *Essentieller Prozess* 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.

1.15.5 Kontinuitätsstrategie herleiten & erstellen

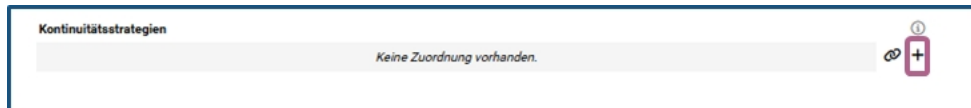
Eine Kontinuitätsstrategie kann nur aus einem Work Item des Typs *Risikoszenario* erstellt werden.

Daher ist wichtig für den Start des Moduls Business Continuity, dass von den zuständigen Bearbeitern Risiko alle *Risikoszenarien* die für den Bereich Business Continuity relevant sind weitgehend erstellt bzw. bei mehreren aktiven Modulen die richtigen Perspektiven hinterlegt wurden.

Schritt 1: Kontinuitätsstrategie aus Risikoszenario erstellen

Der Bearbeiter DS kann über die Menüleiste zu den **Dashboards >> Gesamtübersicht Risikoszenarien** gehen und dort zu "Risikoszenarien nach GRC Perspektiven >> "Business Continuity Management" auswählen, um eine Liste aller BCM getaggtten *Risikoszenarien* zu bekommen. Nach der Auswahl eines *Risikoszenarios* kann er am unteren Ende des Tabs "Übersicht" eine *Kontinuitätsstrategie* erstellen oder verlinken.

Der Bearbeiter DS kann die *Kontinuitätsstrategie* direkt aus dem Work Item *Risikoszenario* erstellen. Dafür erstellt er mittels des Icons  eine *Kontinuitätsstrategie*.



Schritt 2: Details hinterlegen

Kontinuitätsstrategie Details

Status Planung

1

Name

Sicherstellung der Betriebsfähigkeit durch redundante IT- und Kommunikationslösungen (neutral)

Details

Systeminformationen

Details

3

Ausfallszenario

Name	Katalog	Besc...	
Ausfall von IT & Kommunikationssystemen	Ausfallszenarien		

4

Beschreibung

Zur Aufrechterhaltung des Geschäftsbetriebs bei Ausfall von IT- und Kommunikationssystemen werden redundante Systemlandschaften sowie alternative Kommunikationswege eingesetzt. Kritische Anwendungen und Infrastrukturen sind in hochverfügbaren Umgebungen betrieben oder können auf Ersatzsysteme (z. B. Backup-Systeme oder Notfallarbeitsplätze) umgeschaltet werden.

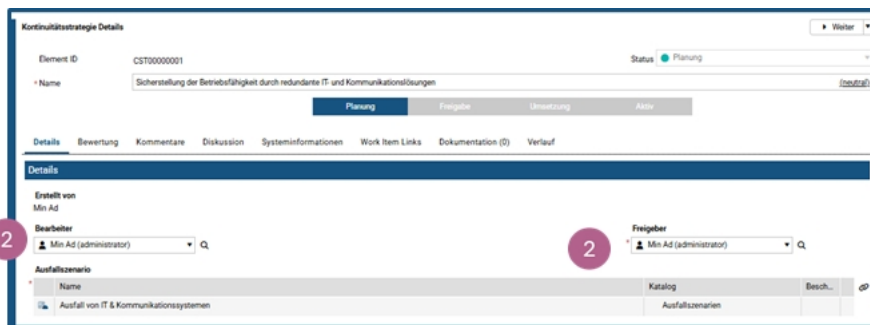
5

Sie haben ungespeicherte Änderungen.

Speichern

Speichern und schließen

Schließen



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

2 **Verantwortliche Personen:** Der Bearbeiter DS hat einen "Bearbeiter" zu hinterlegen, und zusätzlich einen "Freigeber DS", der für die Freigabe des *Kontinuitätsstrategie* verantwortlich ist.

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

Der Bearbeiter DS wird nach der Erstellung aus dem *Essentiellen Prozess* automatisch als Bearbeiter vorgeschlagen und in das Attribut "Bearbeiter" übertragen.

3 **Ausfallszenario:** Wie schon in der dem Risikoszenario muss ein "Ausfallsszenario" verlinkt werden.

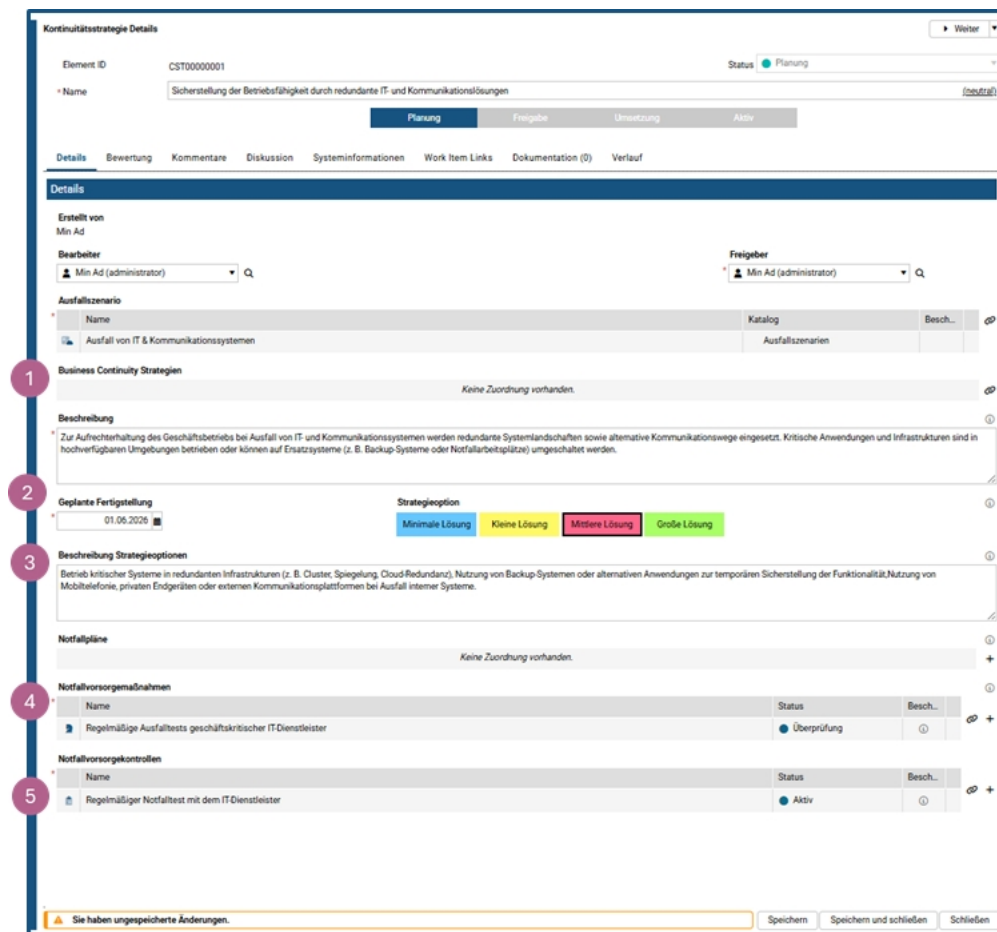
Im *Risikoszenario* waren potenziell mehrere "Ausfallsszenarien" zu verlinken, in der spezifischen *Kontinuitätsstrategie* ist der Schwerpunkt allerdings auf genau einem "Ausfallsszenario". Daher kann hier keine Übernahme der Werte aus dem *Risikoszenario* stattfinden.

Es werden dem Bearbeiter DS nur jene "Ausfallsszenarien" angezeigt, die auch im *Risikoszenario* ausgewählt wurden. Eine andere Auswahl wird technisch unterbunden.

4 **Beschreibung:** Anschließend ist eine Beschreibung der *Kontinuitätsstrategie* zu hinterlegen. Alle User, die im Workflow der *Kontinuitätsstrategie* nachgelagert sind, orientieren sich an dieser Beschreibung, daher sollte sie so viele notwendige Informationen und Daten wie möglich enthalten.

5 **Speichern:** Sobald alle Informationen eingetragen wurden kann die *Kontinuitätsstrategie* gespeichert werden.

Schritt 3: Eingaben vervollständigen



1 **Business Continuity Strategien** : Der Link führt zu einem GRC Framework der fachlich fundierte Strategien abbildet, die sich an gängigen Standards wie "BSI-Standard 200-4" und "ISO 22301:2019" orientieren. Dabei soll die Strategie angepasst an das "Ausfallszenario" ausgewählt werden.

2 **Geplante Fertigstellung**: Dieses Datum soll angeben, wann die Strategie ausgearbeitet und finanziert sein sollte.

Dieses Datum soll zu der zeitlichen Planung und Steuerung der Strategiedefinition beitragen.

Strategieoption: Der Bearbeiter hat den Umfang und Investitionsgrad der Strategie auszuwählen:

- Minimale Lösung – z. B. rein organisatorisch, keine Technik
- Kleine Lösung – z. B. einfache Backup-Option
- Mittlere Lösung – z. B. automatisierter Wiederanlauf im Haus
- Große Lösung – z. B. aktives Failover in externes Rechenzentrum

3 **Beschreibung Strategieoptionen**: In diesem Beschreibungsfeld kann der Bearbeiter DS erklären und dokumentieren, welche Strategieoptionen im Raum standen und warum er sich für die angegebene Option entschieden hat.

- 4 **Notfallvorsorgemaßnahmen:** Der Bearbeiter DS muss Work Item des Typs *Maßnahme* verlinken oder bei Bedarf erstellen.

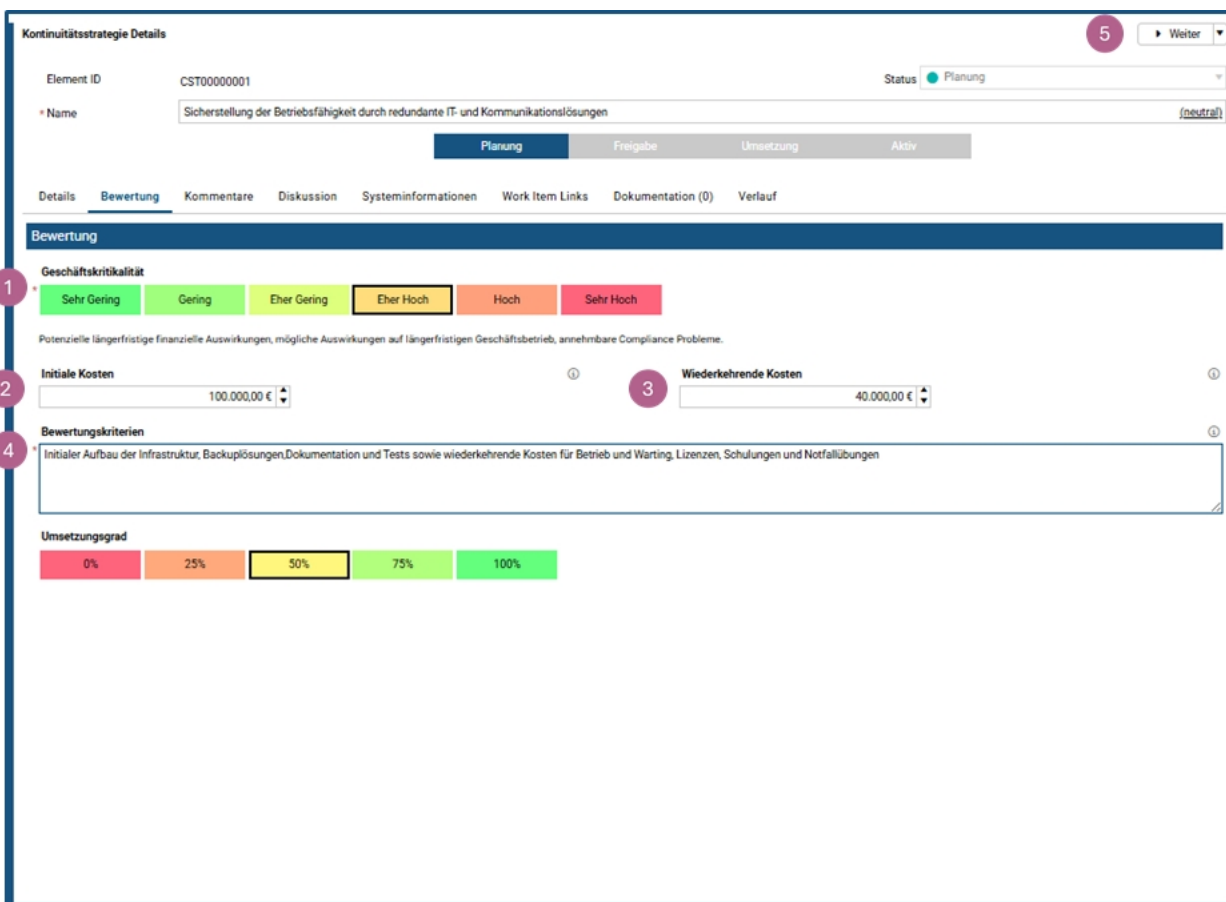
Mehr Informationen unter [Bearbeiter Kontrolle - Kontrolle ableiten & erstellen](#).

- 5 **Notfallvorsorgekontrollen:** An dieser Stelle muss der Bearbeiter Work Items des Typs *Kontrolle* erstellen oder verlinken.

Mehr Informationen unter [Bearbeiter Maßnahme - Maßnahme definieren & erstellen](#).

Schritt 4: Bewertung durchführen

Nachdem alle Angaben in dem Tab "Details" hinterlegt sind kann in dem Tab "Bewertung" fortgefahren werden.



- 1 **Geschäftskritikalität:** Der Bearbeiter DS hat anzugeben mit welcher Kritikalität die Strategie zu betrachten ist. Abhängig von der Wahl kann die Einschätzung zur Priorisierung von Maßnahmen überdacht, jeweilige Risikobewertungen ergänzt oder die Wahl als Grundlage für eine Kosten-Nutzen Entscheidung herangezogen werden.
- 2 **Initiale Kosten:** Der Bearbeiter hat anzugeben mit welchen einmaligen Kosten bei der Implementierung zu rechnen sind.
- 3 **Wiederkehrende Kosten:** Gegenüber den einmaligen Kosten sind die laufenden bzw. wiederkehrenden Kosten anzugeben.
- 4 **Bewertungskriterien:** Zuletzt hat der Bearbeiter anzugeben wie die Bewertung zustande kam und welche Annahmen den Kosten zu Grunde liegen.

5

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

Der Freigeber DS wird mittels Notifikation automatisch über den Statusübergang informiert.

1.15.6 Kontinuitätsstrategie bearbeiten & umsetzen

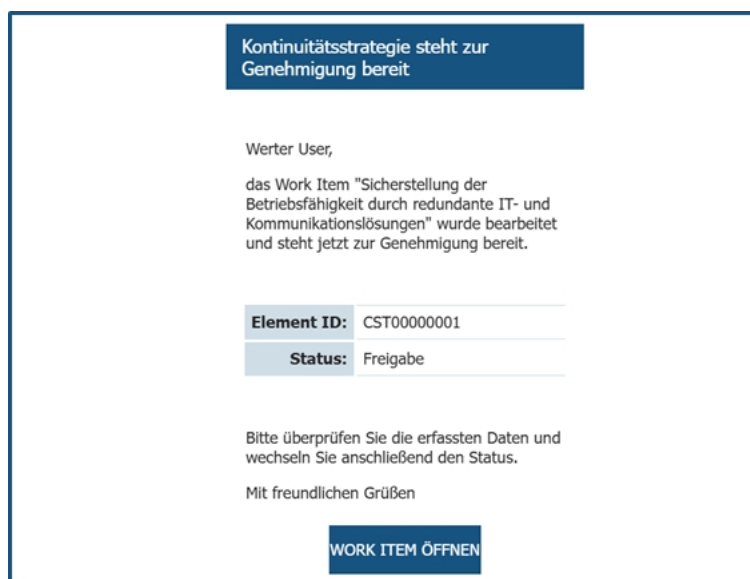
Nachdem eine *Kontinuitätsstrategie* erstellt, geplant und freigegeben wurde kann mit der Umsetzung begonnen werden.

Schritt 1: Navigation zu Kontinuitätsstrategie

Der Bearbeiter hat zwei Möglichkeiten eine zu bearbeitende *Kontinuitätsstrategie* zu öffnen.

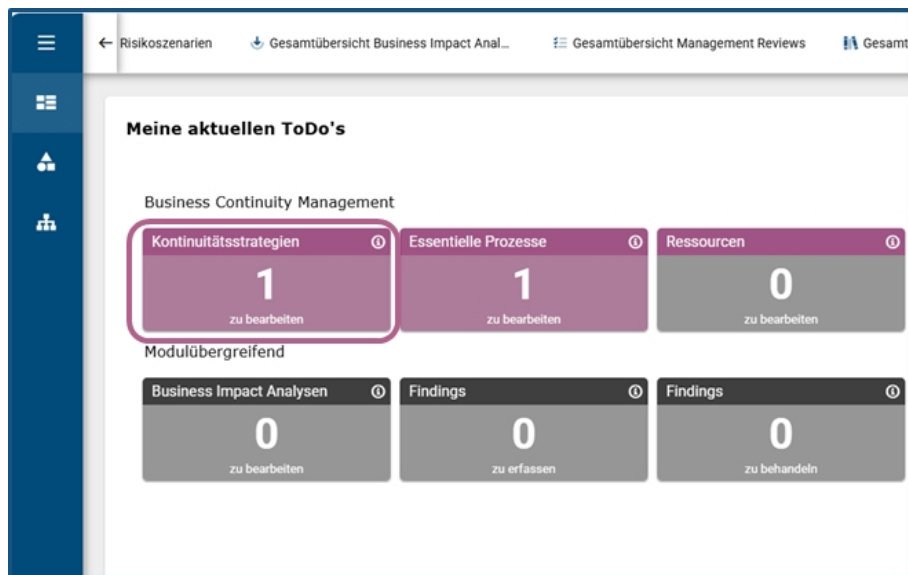
1. Öffnen über Notifikation

Der Bearbeiter bekommt eine E-Mail zugesendet, sobald der Freigeber in den Status "Umsetzung" weitergeschaltet hat. Der Link zu der spezifischen *Kontinuitätsstrategie* 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 Bewertung durchzuführen hat.



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

Schritt 2: Bewertung durchführen

Kontinuitätsstrategie Details

Element ID

CST00000001

Status

Umsetzung

Name

Sicherstellung der Betriebsfähigkeit durch redundante IT- und Kommunikationslösungen

(neutral)

Planung

Freigabe

Umsetzung

Aktiv

Details

Bewertung

Kommentare

Diskussion

Systeminformationen

Work Item Links

Dokumentation (0)

Verlauf

Unwahrscheinliche finanzielle Auswirkungen, vermutlich keine Auswirkungen auf längerfristigen Geschäftsbetrieb, mögliche Auswirkungen auf Compliance.

Initiale Kosten

100.000,00 €

Wiederkehrende Kosten

40.000,00 €

Bewertungskriterien

Initialer Aufbau der Infrastruktur, Backuplösungen, Dokumentation und Tests sowie wiederkehrende Kosten für Betrieb und Wartung, Lizenzen, Schulungen und Notfallübungen

Angemessenheitsprüfung

angemessen

nicht angemessen

Begründung Bewertung

Die implementierten Maßnahmen stehen in einem angemessenen Verhältnis zum identifizierten Risiko eines Ausfalls von IT- und Kommunikationssystemen. Die Investitionen in redundante Systeme, Backup-Lösungen und Notfallverfahren sind erforderlich, um geschäftskritische Prozesse aufrechtzuerhalten und potenzielle finanzielle sowie operative Schäden zu minimieren. Die Kosten sind im Vergleich zu den möglichen Auswirkungen eines Systemausfalls wirtschaftlich vertretbar.

Wirksamkeitsprüfung

wirksam

nicht wirksam

Begründung Bewertung

Die definierten Maßnahmen gewährleisten eine schnelle Wiederherstellung der IT-Services innerhalb der festgelegten Wiederanlaufzeiten (RTO ≤ 4 Stunden) und minimieren Datenverluste (RPO ≤ 1 Stunde). Durch redundante Systeme, getestete Wiederanlaufverfahren und alternative Kommunikationswege wird sichergestellt, dass kritische Geschäftsprozesse auch im Störfall fortgeführt werden können.

Umsetzungsgrad

0%

25%

50%

75%

100%

Sie haben ungespeicherte Änderungen.

Speichern

Speichern und schließen

Schließen

- 1 **Umsetzungsgrad:** Der Bearbeiter kann den Grad der Umsetzung in 5 -Stufen bewerten, abhängig vom Reifegrad der *Kontinuitätsstrategie*.
- 2 **Angemessenheitsprüfung:** Der Bearbeiter kann im Rahmen des *Kontinuitätsstrategie* die Angemessenheit feststellen und mittels "Angemessen" oder "Nicht angemessen" einordnen. Zudem muss eine Begründung für die Einschätzung erfolgen.
- 3 **Wirksamkeitsprüfung:** Neben der Angemessenheit muss der Bearbeiter überprüfen, ob die *Kontinuitätsstrategie* in ihrer Art und Beschaffenheit wirksam ist. Die Einordnung erfolgt hier mittels "Wirksam" oder "Nicht wirksam". Anschließend muss die Einschätzung begründet werden.
- 4 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.
Der Status wird dem Bearbeiter angezeigt, sobald die oben genannten Attribute ausgewählt wurden und der Umsetzungsgrad bei 100% liegt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

Schritt 3: Notfallpläne erstellen

Nachdem die *Kontinuitätsstrategie* in den Status "Aktiv" geschaltet wurde kann der Bearbeiter DS aus der *Kontinuitätsstrategie* Work Items des Typs *Notfallpläne* erstellen.

Für die Erstellung von *Notfallplänen* navigiert er in der *Kontinuitätsstrategie* in den Tab "Details" und erstellt mittels des Icons  eine neuen *Notfallplan*.



Mehr Informationen über die Erstellung eines Notfallplans unter [Bearbeiter_DS_-_Notfallplan_herleiten & erstellen](#).

Es ist nicht vorgesehen, dass ein bestehender *Notfallplan* verlinkt wird, sondern es muss pro *Kontinuitätsstrategie* mindestens ein *Notfallplan* erstellt werden.

1.15.7 Notfallplan herleiten & erstellen

Notfallpläne unterstützen Unternehmen dabei für den Fall der Fälle einen Plan zur Hand zu haben.

Notfallpläne sollen in BIC GRC dazu beitragen das Business Continuity Management im Unternehmenskontext strategisch einzubetten und "Papiertiger" zu vermeiden. Um sicherstellen zu können das *Notfallpläne* einen Bezug zur Realität haben und revisionssicher gewartet werden ist ein unmittelbarer Bezug zu einer *Kontinuitätsstrategie* notwendig.

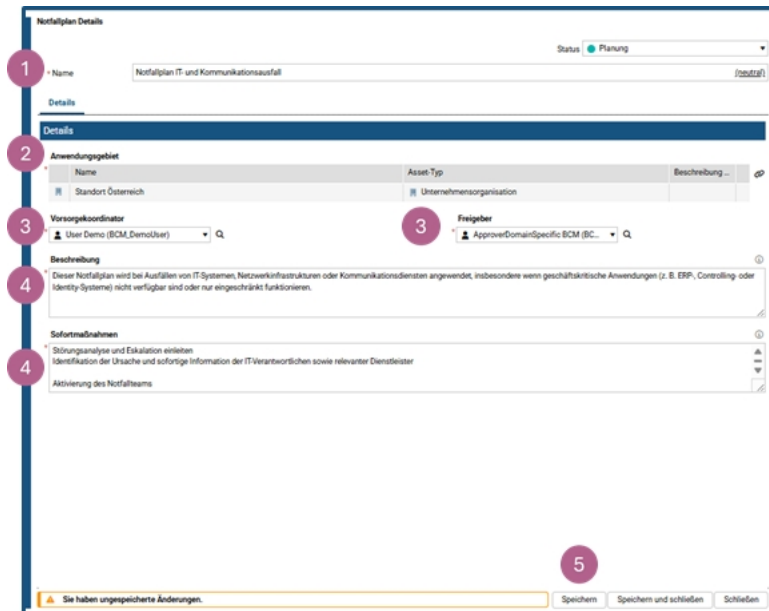
Schritt 1: Notfallplan erstellen

Der *Notfallplan* kann nur mittels Erstellung aus dem Work Item *Kontinuitätsstrategie* durch den verantwortlichen Bearbeiter erfolgen.

Für die Erstellung wird im Tab "Details" durch das Icon  ein neuer *Notfallplan* erstellt.



Schritt 2: Notfallplan beschreiben



The screenshot shows the 'Notfallplan Details' form. It includes a 'Name' field (1), a 'Details' section with a table for 'Anwendungsgebiet' (2), 'Vorsorgekoordinator' (3), and 'Freigeber' (3). There is a 'Beschreibung' field (4) and a 'Sofortmaßnahmen' section (4). At the bottom, there is a status bar (5) with a warning message and buttons for 'Speichern', 'Speichern und schließen', and 'Schließen'.

- 1 **Name:** Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für den *Notfallplan* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht den *Notfallplan* einzigartig.
- 2 **Anwendungsgebiet:** Der Bearbeiter hat ein Anwendungsgebiet für den *Notfallplan* anzugeben. Dabei werden dem Bearbeiter bei der Auswahl nur Assets des Typen "Organisationseinheit" angezeigt.

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](#).

Es werden dem Bearbeiter DS nur jene Anwendungsgebiete angezeigt denen ein Prozess zugewiesen ist, der über die Schritte *Essentieller Prozess* >> *Risikoszenario* >> *Kontinuitätsstrategie* mit einem *Notfallplan* verbunden ist.

- 3 **Verantwortliche Personen:** Der Bearbeiter hat einen eigenen "Vorsorgekoordinator" zu hinterlegen und zusätzlich einen "Freigeber", der für die Freigabe des *Notfallplans* verantwortlich ist. Sowohl der Vorsorgekoordinator als auch der Freigeber DS müssen dabei das passende Benutzerprofil am Asset/Scope haben.

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

- 4 **Beschreibung und Sofortmaßnahmen:** Anschließend kann der Bearbeiter eine Beschreibung hinterlegen, welchen Zweck dieser Notfallplan hat und weitere hilfreiche Details. Danach kann er in schriftlicher Form direkte Sofortmaßnahmen dokumentieren.

Es wird hier kein Link zu dem Work Item Maßnahme angezeigt, sondern es ist in einer schriftlichen Form die Maßnahme zu beschreiben.

- 5 **Speichern:** Sobald alle Informationen eingetragen wurden kann der *Notfallplan* gespeichert werden.

Nach dem Speichervorgang wird das hinterlegte Notfallschutzteammitglied mittels Notifikation benachrichtigt. Mehr Informationen unter [Vorsorgekoordinator - Notfallplan definieren & planen](#).

1.15.8 Ressource identifizieren & erstellen

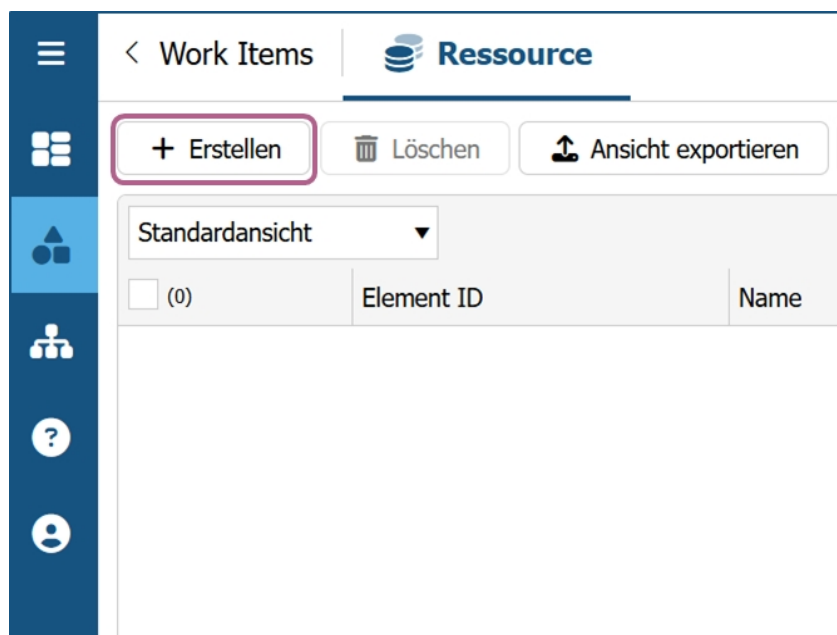
Jeder kritische Geschäftsprozess benötigt Ressourcen, um zu funktionieren. Daher ist es eine wichtige vorbereitende Tätigkeit, alle Ressourcen in BIC GRC zu erfassen, um sie später an anderen Stellen wieder verlinken zu können.

Ressourcen können nur an Assets der Typen "Primary Asset" oder "Supporting Assets" erstellt werden.

Schritt 1: Ressource erstellen

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

Ein neues Fenster öffnet sich anschließend automatisch.



Element ID	Name
(0)	

Schritt 2: Details hinterlegen

Ressource Details

Status: ● Erfassung

* Name Zentrale Hosting-Plattform des IT-Dienstleisters (neutral)

Details

Ressourcenkategorie

* Standardressource

Ressourcentyp ⓘ

* IT und Kommunikation

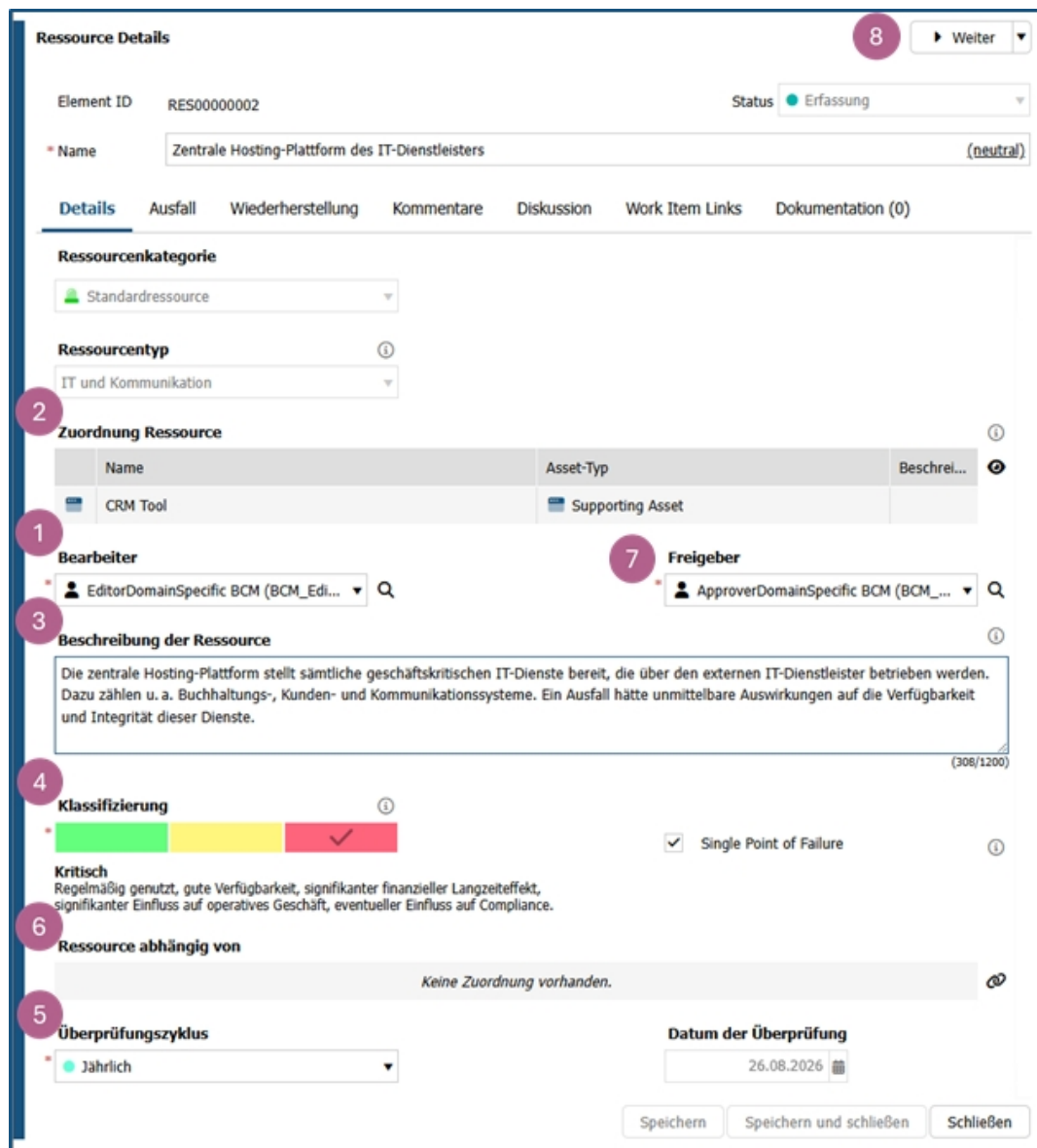
⚠ Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

- 1 **Name:** Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Ressource* erfolgen. Unter dem "Namen" in Kombination mit der "Element ID" ist die *Ressource* einzigartig.
- 2 **Ressourcenkategorie:** Sollte die erfasste *Ressource* eine Standardressource sein, dann ist sie Teil des regulären Tagesgeschäfts. Bei der Auswahl "Notfallressource" wird die *Ressource* benötigt im Notfall bzw. während des Wiederanlaufs.
- 3 **Ressourcentyp:** Ein "Ressourcentyp" ist Teil einer Gruppe, unter der *Ressourcen* mit ähnlicher Funktion oder Eigenschaften von Bearbeitern DS zusammengefasst werden können.

Sollte der Typ "Sonstige" ausgewählt werden, wird dem Bearbeiter DS ein zusätzliches Textfeld angezeigt.

- 4 **Speichern:** Sobald die Informationen angegeben sind kann der Bearbeiter DS speichern.

Schritt 3: Details ergänzen



- 1 **Überprüfungszyklus:** Der Bearbeiter muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft eine *Ressource* zurück in den Status "Erfassung" geschaltet wird, um die *Ressource* in regelmäßigen Zeitabständen zu evaluieren.

Das Attributsfeld "Nächste Überprüfung" wird automatisch von BIC GRC gesetzt.

- 2 **Zuordnung Ressource:** Der Link kann
 - zu der Assethierarchie führen, wo der Bearbeiter ein "Primary Asset" oder ein "Supporting Asset" auswählen kann oder
 - zu den passenden Frameworks von "Kunden", "Lieferanten" oder "Partner & Behörden" oder
 - es wird ein Textfeld angezeigt, wo der Name der *Ressource* angegeben werden muss.

Die Anzeige ist abhängig von der Auswahl des "Ressourcentypen".

- 3 **Verantwortliche Personen:** Der Bearbeiter wird automatisch in dem Feld "Bearbeiter" hinterlegt. Ein "Freigeber", der für die Freigabe der *Ressource* verantwortlich ist, muss vom Bearbeiter hinterlegt werden. Sowohl der Bearbeiter als auch der Freigeber DS müssen dabei das passende Benutzerprofil am Asset/Scope haben.
Dieser Benutzer wird durch das  Icon gesucht sowie verlinkt oder mittels der Eingabe des Namens des Benutzers im Attribut vorgeschlagen.
- 4 **Beschreibung der Ressource:** In diesem Beschreibungsfeld kann der Bearbeiter DS erklären und dokumentieren, warum die *Ressource* relevant ist und wie die Beziehung zu anderen *Ressourcen* aussieht.
- 5 **Optional - Klassifizierung:** Die Klassifizierung kann in drei Stufen - von "Unkritisch" bis "Kritisch" - angegeben werden, wenn es sich um eine "Standardressource" handelt.
- 6 **Optional - Single Point of Failure:** Der Bearbeiter kann mittels der Checkbox manuell festlegen, ob es sich bei der *Ressource* um einen "Single Point of Failure" handelt, wenn es sich um eine "Standardressource" handelt.

Die Checkbox kann auch von BIC GRC automatisch gesetzt werden, sobald die *Ressource* zu drei zeitkritischen *Essenziellen Prozessen* verlinkt ist.

Ein Single Point of Failure (SPOF) ist eine einzelne Komponente, Ressource oder Abhängigkeit, deren Ausfall zum Stillstand eines gesamten Systems, Prozesses oder Dienstes führt – weil es keine Redundanz oder Ausweichmöglichkeit gibt.

- 7 **Ressource abhängig von:** An dieser Stelle kann der Bearbeiter Work Items des Typs *Ressource* verlinken, die einen besonderen Bezug zu der aktuellen *Ressource* haben.

Nur *Ressourcen* mit der Ressourcenkategorie "Standardressource" werden dem Bearbeiter DS zur Auswahl vorgeschlagen.

- 8 **Speichervorgang oder Statuswechsel:** Nach der Hinterlegung der notwendigen Informationen kann die *Ressource* gespeichert werden.

Sollte es sich um eine Ressource der Kategorie "Notfallressource" handeln, dann kann der Bearbeiter direkt einen Statusübergang in den Status "Freigabe" vornehmen. Handelt es sich um eine "Standardressource" sollte er mit den Schritten 4 & 5 fortfahren.

Schritt 4: Ausfallszenario dokumentieren

Nach dem Speichervorgang sollte der Bearbeiter DS in den Tab "*Ausfall*" wechseln, um mit der Erfassung einer "Standardressource" fortzufahren.

Ressource Details Weiter

Element ID: RES00000002 Status: Erfassung

Name: Zentrale Hosting-Plattform des IT-Dienstleisters (neutral)

Details **Ausfall** Wiederherstellung Kommentare Diskussion Work Item Links Dokumentation (0)

Ausfall

1 **Ausfallszenarien** ⓘ

Elementname	Name
FailureScenario.ITCommunicationSystem	Ausfall von IT & Kommunikationssystemen

2 **Auswirkung Ausfall** ⓘ

Der Ausfall der Hosting-Plattform führt zur Unterbrechung aller geschäftskritischen IT-Services (z. B. ERP, Buchhaltung, Kundenkommunikation). Dies hat unmittelbare Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs, die Einhaltung regulatorischer Fristen sowie auf die Kundenbeziehung.

3 **Verantwortlich intern** ⓘ

Mag. Laura Berger, BCM-Verantwortliche

4 **Ansprechpartner extern** ⓘ

Maximilian Hofer, Account Manager ABC-IT GmbH
Tel.: +43 123 456789
E-Mail: maximilian.hofer@abc-it.at

5 **Zuordnung Notfallressource** ⓘ

Keine Zuordnung vorhanden. ⓘ

6 **Sie haben ungespeicherte Änderungen.** Speichern Speichern und schließen Schließen

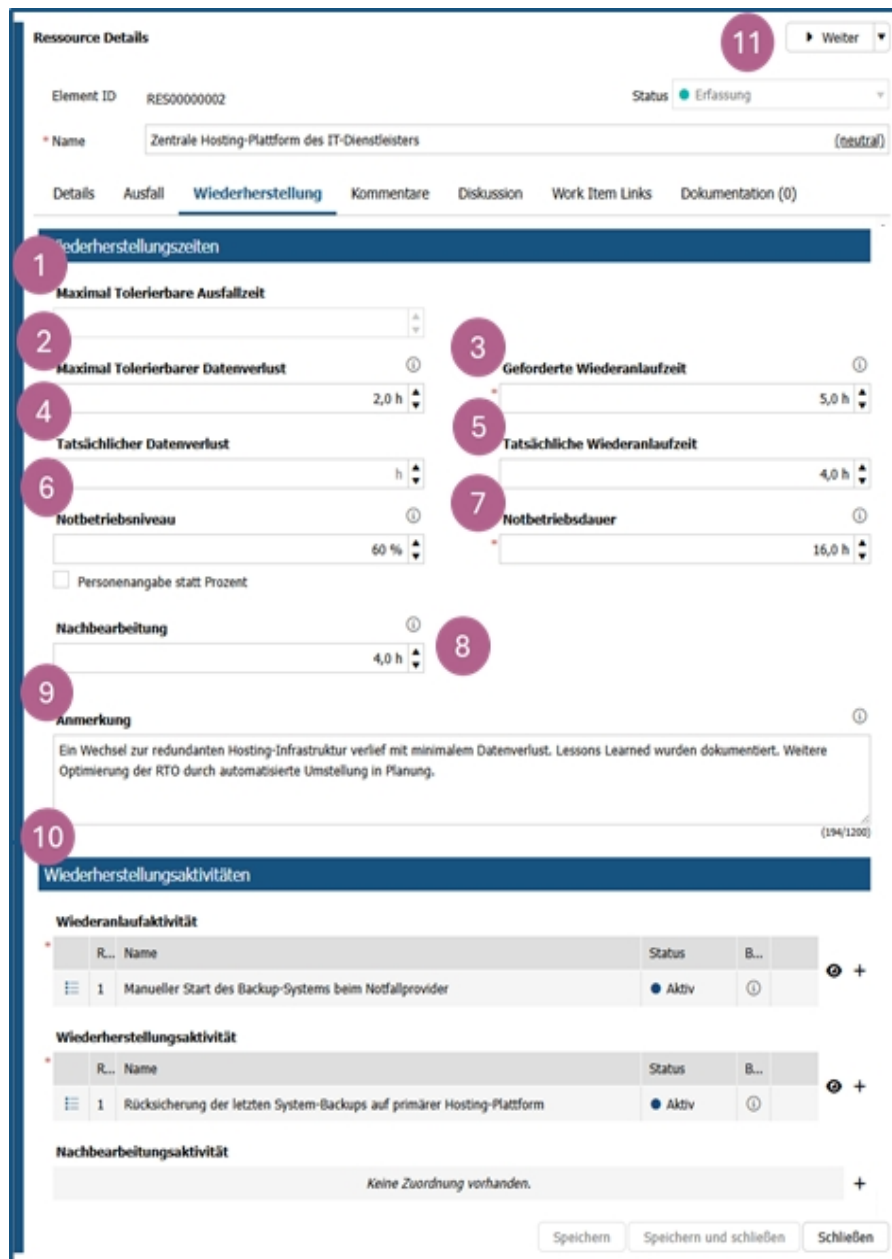
- 1 **Ausfallsszenarien:** Der Bearbeiter DS hat ein oder mehrere passende "Ausfallsszenarien" mittels des Icons ⓘ zu verlinken. Dabei wird ihm ein GRC Framework angezeigt.
- 2 **Auswirkung Ausfall:** Danach hat der Bearbeiter schriftlich anzugeben, mit welchen Auswirkungen zu rechnen ist oder wie sich die Geschäftsprozesse bei einem Ausfall verhalten würden.
- 3 **Verantwortliche intern:** Anschließend kann die interne Verantwortung intern notiert werden.
- 4 **Ansprechpartner extern:** Sollten auch externe Ansprechpartner beteiligt sein, können diese zusätzlich angegeben werden.
- 5 **Zuordnung Notfallressource:** An dieser Stelle kann der Bearbeiter Work Items des Typs *Ressource* verlinken, die einen besonderen Bezug zu der aktuellen *Ressource* haben.

Nur *Ressourcen* mit der Ressourcenkategorie "Notfallressource" werden dem Bearbeiter DS zur Auswahl vorgeschlagen.

- 6 **Speichervorgang:** Nach der Hinterlegung der notwendigen Informationen, kann die *Ressource* gespeichert werden

Schritt 5: Wiederherstellung dokumentieren

Nach dem Speichervorgang sollte der Bearbeiter DS in den Tab "*Wiederherstellung*" wechseln, um mit der Erfassung fortzufahren.



- 1 **Maximal Tolerierbare Ausfallzeit:** Die "Maximal Tolerierbare Ausfallzeit" ist die maximal zulässige Zeit, in der eine *Ressource* ausfallen darf, bevor es zu untragbaren Auswirkungen auf kritische Geschäftsprozesse kommt.

Dieser Wert kann nicht manuell gesetzt werden, sondern wird von BIC GRC automatisch gesetzt. Dabei ist der Wert das übernommene Minimum aller "Maximal Tolerierbare Ausfallzeit" der *Essentiellen Prozesse*, wo die *Ressource* zugelinkt wurde.

- 2 **Maximal Tolerierbarer Datenverlust:** Der Bearbeiter hat anzugeben, wie lang der größte akzeptable Datenverlust im Falle eines Ausfalls sein darf, gemessen ab dem letzten erfolgreichen Datenabzug (z. B. Backup).

Beispiel: Bei 4 Stunden bedeutet das: „Es dürfen maximal Daten der letzten 4

Stunden verloren gehen.“

- 3 **Geforderte Wiederanlaufzeit:** Gibt die vom Geschäftsbereich oder Management festgelegte Zielzeit an, innerhalb der die *Ressource* nach einem Ausfall spätestens wieder betriebsbereit sein muss.

Dieser Wert sollte unter der „Maximal tolerierbaren Ausfallzeit“ liegen.

- 4 **Tatsächlicher Datenverlust:** Der Bearbeiter sollte den real beobachtete Datenverlust bei einem Störungsszenario oder Test angeben. Dabei kann möglicherweise auf Erfahrungswerte zurückgegriffen werden.

- 5 **Tatsächliche Wiederanlaufzeit:** Gibt die im realen Fall oder Test gemessene Dauer an, bis die *Ressource* wieder zur Verfügung stand.

- 6 **Notbetriebsniveau:** Die Mindestressourcenkapazität (%) oder Mindestpersonalkapazität (pers), mit der der Prozess mit dieser Ressource noch funktionsfähig gehalten werden kann.

Mittels der Checkbox kann der Bearbeiter zwischen den beiden Einheiten % und pers wechseln.

- 7 **Notbetriebsdauer:** Zeitraum, in dem der Prozess mit reduzierter Kapazität (z. B. unter Notfallbedingungen) aufrechterhalten werden kann, bevor er vollständig wiederhergestellt sein muss.

Beispiel: „Der Prozess kann mit Notfallbesetzung 48 Stunden weitergeführt werden.“

- 8 **Nachbearbeitung:** Zeitaufwand, der nach einem Ausfall anfällt, um Rückstände aufzuarbeiten, z. B. manuell dokumentierte Vorgänge nachzupflegen.

Diese Angabe hilft bei der Ressourcen- und Personalplanung für die Wiederherstellungsphase.

- 9 **Anmerkung:** Sollten noch weitere schriftlichen Ergänzungen hinterlegt werden, um auf Sonderfälle oder Einschränkungen einzugehen, kann dies in diesem Textfeld dokumentiert werden.

- 10 **Wiederherstellungsaktivitäten:** Zuletzt hat der Bearbeiter anzugeben welche Aktivitäten gesetzt werden müssen. In BIC GRC wird unterschieden in:

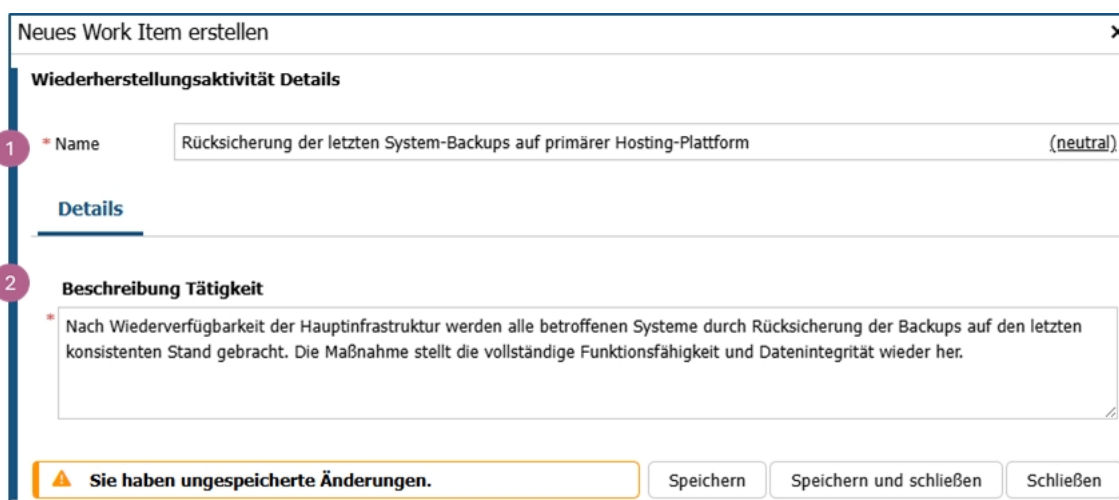
- **Wiederanlaufaktivität:** Beschreibt alle Aktivitäten, die unmittelbar nach dem Ausfall notwendig sind, um die betroffene *Ressource* grundlegend wieder in Betrieb zu nehmen, auch wenn nur auf Notbetriebsniveau.
- **Wiederherstellungsaktivität:** Bezeichnet die Aktivitäten zur vollständigen Wiederherstellung der normalen Betriebsfähigkeit nach dem ersten Wiederanlauf. Hier geht es um das Zurückführen auf den Soll-Zustand im Regelbetrieb.
- **Nachbearbeitungsaktivität:** Dient der Aufarbeitung und Nachdokumentation des Ereignisses bzw. der Übergangsphase. Sie umfasst organisatorische, technische und betriebliche „Aufräumarbeiten“ nach der Wiederherstellung.

Mehr Informationen zu der Erstellung des Work Items *Wiederherstellungsaktivitäten* im Schritt 6.

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

Der Freigeber DS wird mittels Notifikation über den Statuswechsel informiert.

Schritt 6: Wiederherstellungsaktivität erstellen



The screenshot shows a dialog box titled "Neues Work Item erstellen". Inside, there's a section "Wiederherstellungsaktivität Details". Step 1 points to the "Name" field, which contains "Rücksicherung der letzten System-Backups auf primärer Hosting-Plattform" and a "(neutral)" status indicator. Step 2 points to the "Beschreibung Tätigkeit" field, which contains a detailed description of the backup recovery process. At the bottom, there's a warning bar "Sie haben ungespeicherte Änderungen." and three buttons: "Speichern", "Speichern und schließen", and "Schließen".

Der Bearbeiter kann ein Work Item des Typs *Wiederherstellungsaktivität* mittels des Icons  nur aus einer *Ressource* erstellen. Dabei hat er einen "Namen" für die *Wiederherstellungsaktivität* anzugeben¹ und eine "Beschreibung der Tätigkeit"². Sobald er die *Wiederherstellungsaktivität* speichert muss er einen Rang eingeben. Dieser Rang bestimmt die Reihenfolge in der die *Wiederherstellungsaktivität* organisiert werden sollte. Nach der Eingabe des Rangs kann erneut gespeichert werden. Die *Wiederherstellungsaktivität* wechselt automatisch in den Status "Aktiv".

Schritt 7: Update durchführen

Der Bearbeiter sollte die *Ressource* regelmäßig dahingehend überprüfen, ob die Angaben noch korrekt sind.

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 die *Ressource* im Status "Aktiv" in den Status "Erfassung" geschaltet 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 *Ressource* 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.

1.15.9 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.

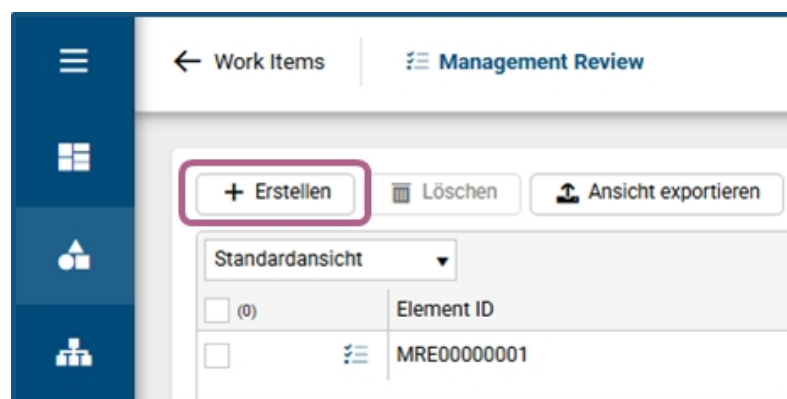


Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung 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

Management Review Details

Status
In Planung

Name
Integrierte Managementbewertung – Standort Deutschland
(neutral)

Planung

Anwendungsbereich

Name	Asset-Typ	Beschreib...
Standort Deutschland	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

Information Security Management
Business Continuity Management
Privacy Management
Enterprise Risk Management
Internal Control
Corporate Sustainability

Auswählen...

Gesprächsthemen

Information Security Management

Name	Be...
Welche Trends, Abweichungen oder Erkenntnisse wurden durch Überwachung, Messung, Audits oder Leistungsbewertungen identifiziert?	
Welche Risiken oder Probleme aus früheren Bewertungen sind noch nicht ausreichend mitigiert oder gelöst?	
Müssen bestehende Verfahren oder Kontrollen aufgrund interner Erkenntnisse oder neuer externer Anforderungen angepasst werden?	

Business Continuity Management

Name	Be...
Welche Ergebnisse liegen aus relevanten Bewertungen oder Analysen vor (z. B. Risikoanalysen, Business Impact Analysen etc.)?	

Sie haben ungespeicherte Änderungen.
Speichern
Speichern und schließen
Schließen

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 freigeschalteten Modulen.

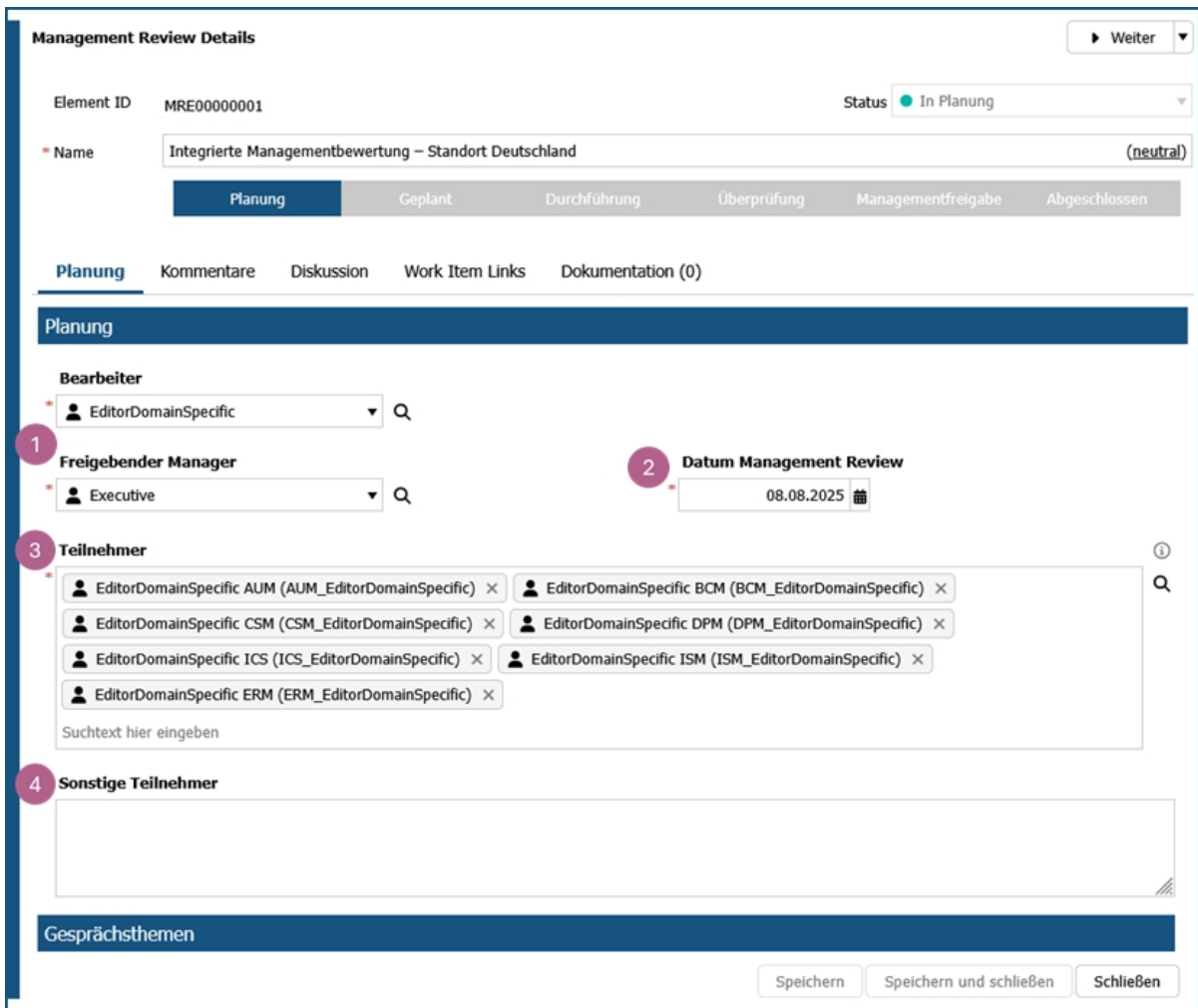
- 5 **Management Review Fragen** : Nachdem der Bearbeiter DS GRC Perspektiven ausgewählt hat werden im darunter je nach gewählter Perspektive Links angezeigt. Diese Links führen jeweils zu einem GRC Framework "Fragen Management Review".

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.

- 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.

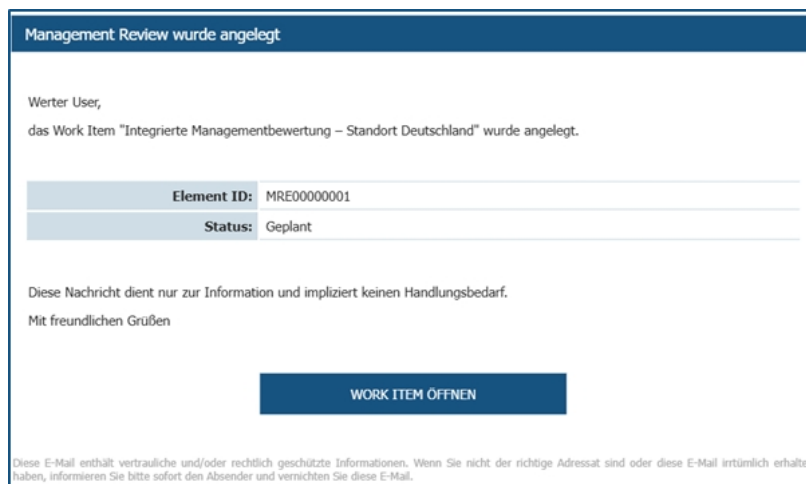
Nach der Eingabe aller notwendigen Informationen kann das Work Item gespeichert und ein Statusübergang durchgeführt werden, bevor das Fenster manuell geschlossen wird.

1.15.10 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.



Management Review wurde angelegt

Werter User,

das Work Item "Integrierte Managementbewertung – Standort Deutschland" wurde angelegt.

Element ID:	MRE00000001
Status:	Geplant

Diese Nachricht dient nur zur Information und impliziert keinen Handlungsbedarf.
Mit freundlichen Grüßen

[WORK ITEM ÖFFNEN](#)

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail.

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.

Management Review Details

In Planung
Weiter

In Durchführung
Obsolet

Element ID: MRE00000001
Status: Geplant

Name: Integrierte Managementbewertung – Standort Deutschland (neutral)

Planung
Geplant
Durchführung
Überprüfung
Managementfreigabe
Abgeschlossen

Planung
Kommentare
Diskussion
Work Item Links
Dokumentation (0)

Planung

Bearbeiter
EditorDomainSpecific

Freigebender Manager
Executive

Datum Management Review
08.08.2025

Anwendungsbereich

Name	Asset-Typ	Beschreib...
Standort Deutschland	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

Information Security Management
Business Continuity Management
Privacy Management
Enterprise Risk Management
Internal Control
Corporate Sustainability

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](#).

Management Review Details

► In Überprüfung

Element ID

MRE00000001

Status

In Durchführung

Name

Integrierte Managementbewertung – Standort Deutschland

(neutral)

Planung

Geplant

Durchführung

Überprüfung

Managementfreigabe

Abgeschlossen

Planung

Ergebnisse

Kommentare

Diskussion

Work Item Links

Dokumentation (0)

Ergebnisse

Getroffene Entscheidungen

- Einführung eines einheitlichen Monitorings für geschäftskritische Prozesse unter Berücksichtigung von Security-, BCM- und Datenschutzaspekten.
- Entscheidung zur Integration datenschutzrelevanter Prüfungen in interne Kontrollmechanismen (IKS).
- Aktualisierung der Zielsetzungen im Bereich Corporate Sustainability zur stärkeren Verzahnung mit ESG-Berichtspflichten gemäß CSRD.
- Start eines bereichsübergreifenden Projekts zur Überarbeitung des Business Continuity Plans mit Fokus auf Lieferkettenrisiken.

Finding

Name	Status	B...
Fehlende zentrale Verknüpfung regulatorischer Anforderungen mit operativen	Erfassung	1

Ergebnisse aus Besprechungen von Zielen

- Die strategischen Zielsetzungen wurden grundsätzlich als weiterhin gültig und zielführend eingestuft.
- Es besteht jedoch Optimierungsbedarf bei der Operationalisierung von Zielen im Bereich Nachhaltigkeit und Risikotransparenz.
- Eine Zielüberprüfung wird künftig in engerer Abstimmung mit Audit-Ergebnissen und Lessons Learned erfolgen.

Ergebnisse aus Besprechungen interner/externer Themen

Ein Vorschlag zur Einführung eines kontinuierlichen externen Anforderungsmonitorings wurde positiv aufgenommen und wird weiterverfolgt.

Speichern

Speichern und schließen

Schließen

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.

Management Review Details

In Durchführung
Managementfreigabe

Element ID: MRE00000001
Status: In Überprüfung

Name: Integrierte Managementbewertung – Standort Deutschland (neutral)

Planung Geplant Durchführung Überprüfung Managementfreigabe Abgeschlossen

Planung Ergebnisse **Kommentare** Diskussion Work Item Links Dokumentation (0)

Kommentare

Kommentar

Tragen Sie hier Ihren Kommentar ein.

(0/1000)

+ Kommentar hinzufügen

Alle Kommentare

1.15.11 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

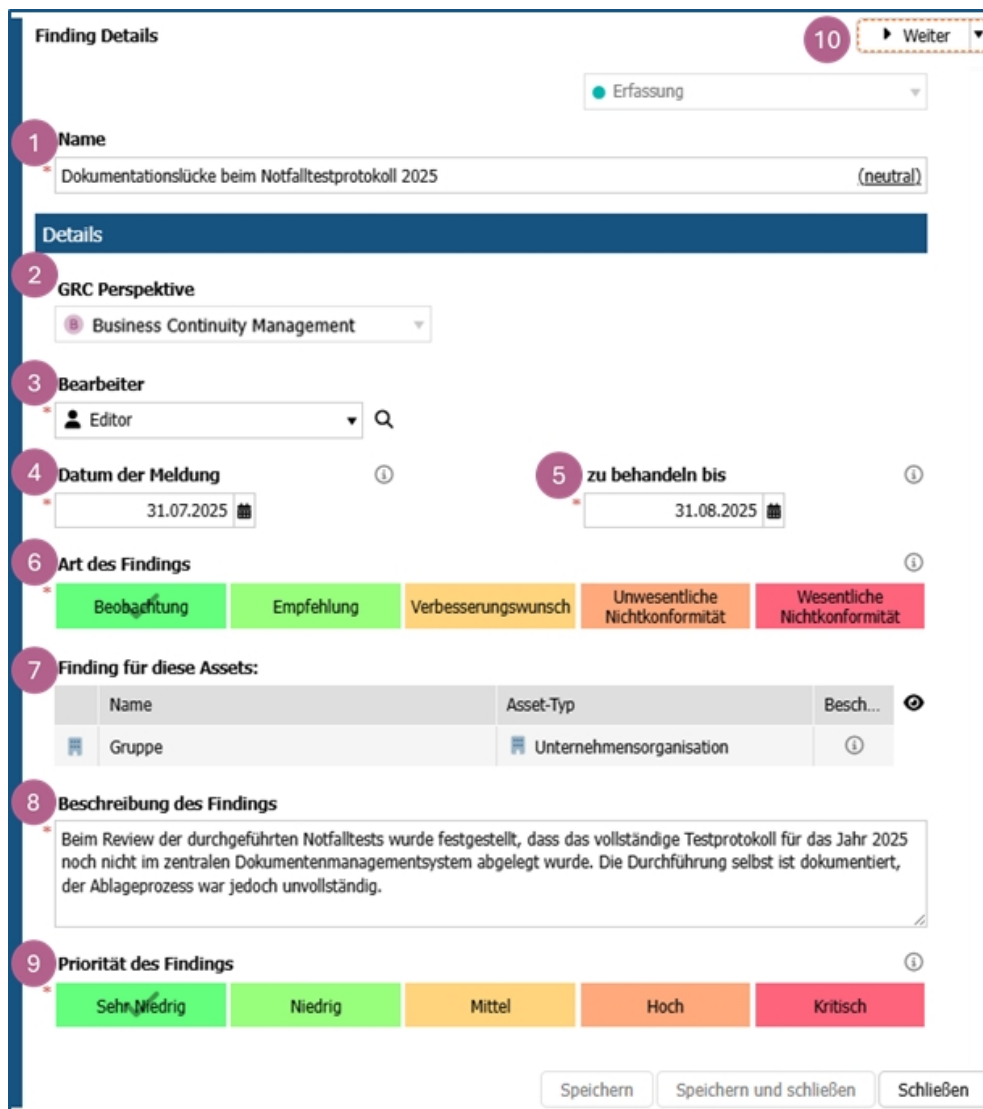
Ein *Finding* kann aus einem *Management Review* entstehen.

Die Erstellung erfolgt durch das Icon **+** nach einer schriftlichen Stellungnahme unter "Getroffene Entscheidungen".

Findings				
	Name	Status	B...	
	Dokumentationslücke beim Notfalltestprotokoll 2025	Erfassung		+

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 eine 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 Dashboards 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](#).

1.16 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](#))

Folgende laufende Aufgaben hat ein Freigeber DS in BIC GRC:

- [Business Impact Analyse überprüfen & freigeben](#)
- [Ressource überprüfen & freigeben](#)
- [Essentiellen Prozess überprüfen & freigeben](#)
- [Kontinuitätsstrategie überprüfen & freigeben](#)
- [Notfallplan überprüfen & freigeben](#)
- [Notfallübung überprüfen & freigeben](#)

- [Bericht\(e\) öffnen & generieren](#)

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:

- [Vorfall bewerten & behandeln](#)
- [Kontinuitätsstrategie herleiten & erstellen](#)
- [Essentieller Prozess identifizieren & erstellen](#)
- [Ressource identifizieren & erstellen](#)
- [Management Review definieren & erstellen](#)
- [Maßnahmen identifizieren & erstellen](#)
- [Kontrolle ableiten & erstellen](#)

1.16.1 Business Impact Analyse überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung und Bewertung einer *Business Impact Analyse* durch den Bearbeiter DS mittels Notifikation informiert.

Schritt 1: Navigation zu Business Impact Analyse

Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Business Impact Analyse* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu der spezifischen *Business Impact Analyse* befindet sich in der Notifikation.

Business Impact Analyse steht zur Genehmigung bereit

Werter User,

das Work Item "Controllingprozess" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	BIA00000002
Status:	Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.

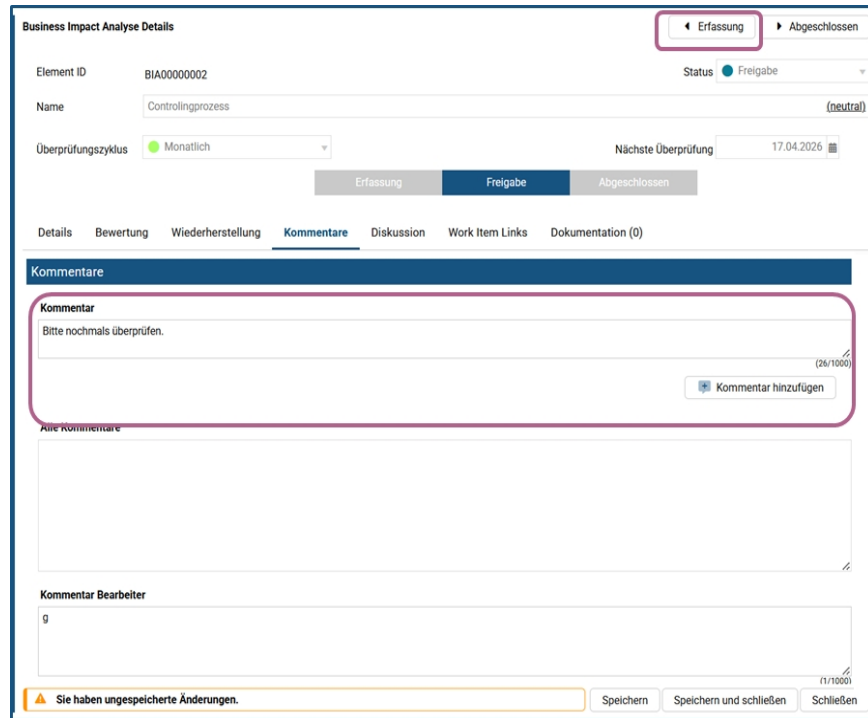
Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

Schritt 2: Business Impact Analyse überprüfen

Der Freigeber DS hat in der bewerteten *Business Impact Analyse* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Business Impact Analyse* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss die *Business Impact Analyse* aus Sicht des Freigeber DS erneut bewertet oder überprüft werden, kann der Freigeber DS einen Kommentar im Tab "Kommentar" hinterlassen und einen Statuswechsel in den Status "Erfassung" durchführen.



Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Aktiv" schalten. Der verantwortliche Bearbeiter DS wird mittels Notifikation über den Statuswechsel benachrichtigt.

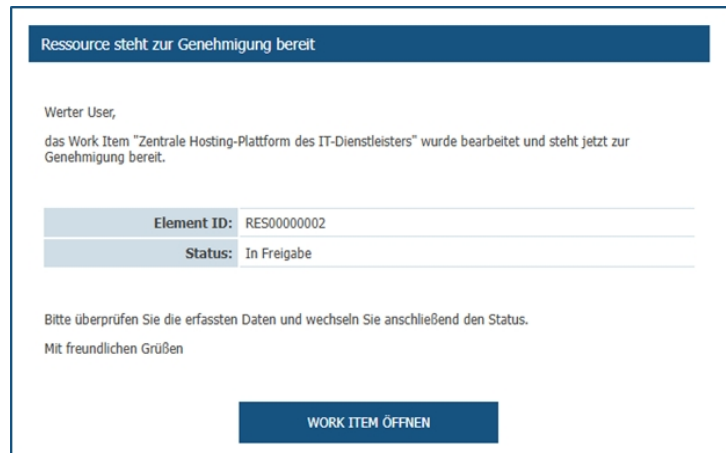
Nach dem Statusübergang kann das Fenster geschlossen werden.

1.16.2 Ressource überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung eines *Ressource* des Bearbeiter DS mittels Notifikation informiert.

Schritt 1: Navigation zu Ressource

Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Ressource* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu der spezifischen *Ressource* befindet sich in der Notifikation.



Ressource steht zur Genehmigung bereit

Werter User,

das Work Item "Zentrale Hosting-Plattform des IT-Dienstleisters" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	RES00000002
Status:	In Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.

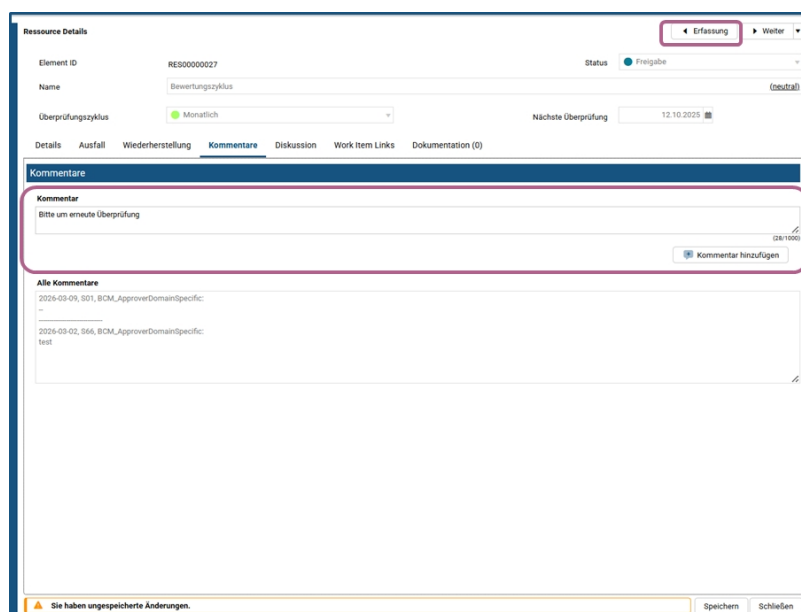
Mit freundlichen Grüßen

[WORK ITEM ÖFFNEN](#)

Schritt 2: Ressource überprüfen

Der Freigeber DS hat in der bewerteten *Ressource* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Ressource* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss die *Ressource* aus Sicht des Freigeber DS erneut bewertet oder überprüft werden, kann der Freigeber DS einen Kommentar im Tab "Kommentar" hinterlassen und einen Statuswechsel in den Status "Erfassung" durchführen.



Ressource Details

Element ID: RES00000027 Status: ● Freigabe

Name: Bewertungszyklus (neutral)

Überprüfungszyklus: ● Monatlich Nächste Überprüfung: 12.10.2025

Details Ausfall Wiederherstellung **Kommentare** Diskussion Work Item Links Dokumentation (0)

Kommentare

Kommentar: Bitte um erneute Überprüfung (28.10.2025)

[Kommentar hinzufügen](#)

Alle Kommentare

2024-09-09, 501, BCM_ApproverDomainSpecific: "

2024-09-02, 566, BCM_ApproverDomainSpecific: test

Sie haben ungespeicherte Änderungen. [Speichern](#) [Schließen](#)

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Aktiv" schalten. Der verantwortliche Bearbeiter DS wird mittels Notifikation über den Statuswechsel benachrichtigt.

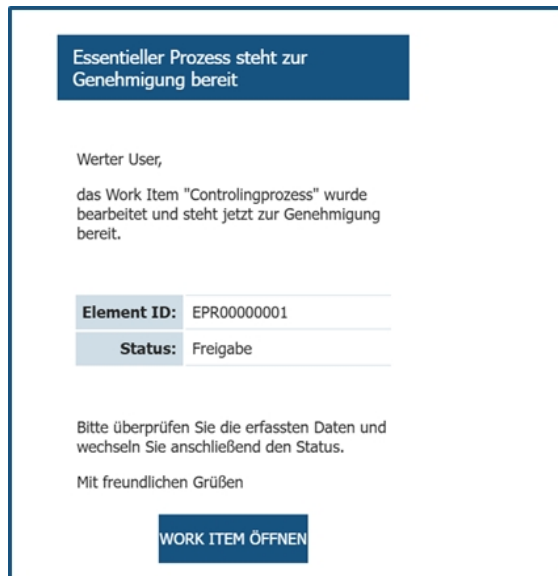
Nach dem Statusübergang kann das Fenster geschlossen werden.

1.16.3 Essentiellen Prozess überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung eines *Essentiellen Prozess* des Bearbeiter DS mittels Notifikation informiert.

Schritt 1: Navigation zu Essentiellen Prozess

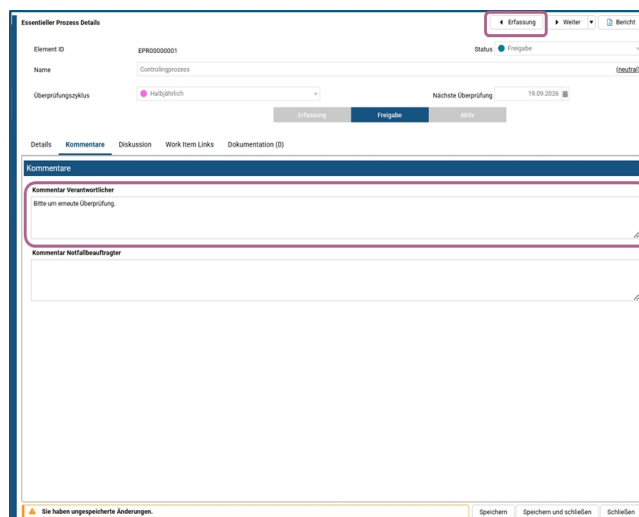
Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald ein *Essentieller Prozesserstellt* und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu dem spezifischen *Essentiellen Prozess* befindet sich in der Notifikation.



Schritt 2: Essentiellen Prozess überprüfen

Der Freigeber DS hat in dem bewerteten *Essentiellen Prozess* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob der *Essentielle Prozess* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss der *Essentielle Prozess* aus Sicht des Freigeber DS erneut bewertet oder überprüft werden, kann der Freigeber DS einen Kommentar im Tab "Kommentar" hinterlassen und einen Statuswechsel in den Status "Erfassung" durchführen.



Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Aktiv" schalten. Der verantwortliche Bearbeiter DS wird mittels Notifikation über den Statuswechsel benachrichtigt.

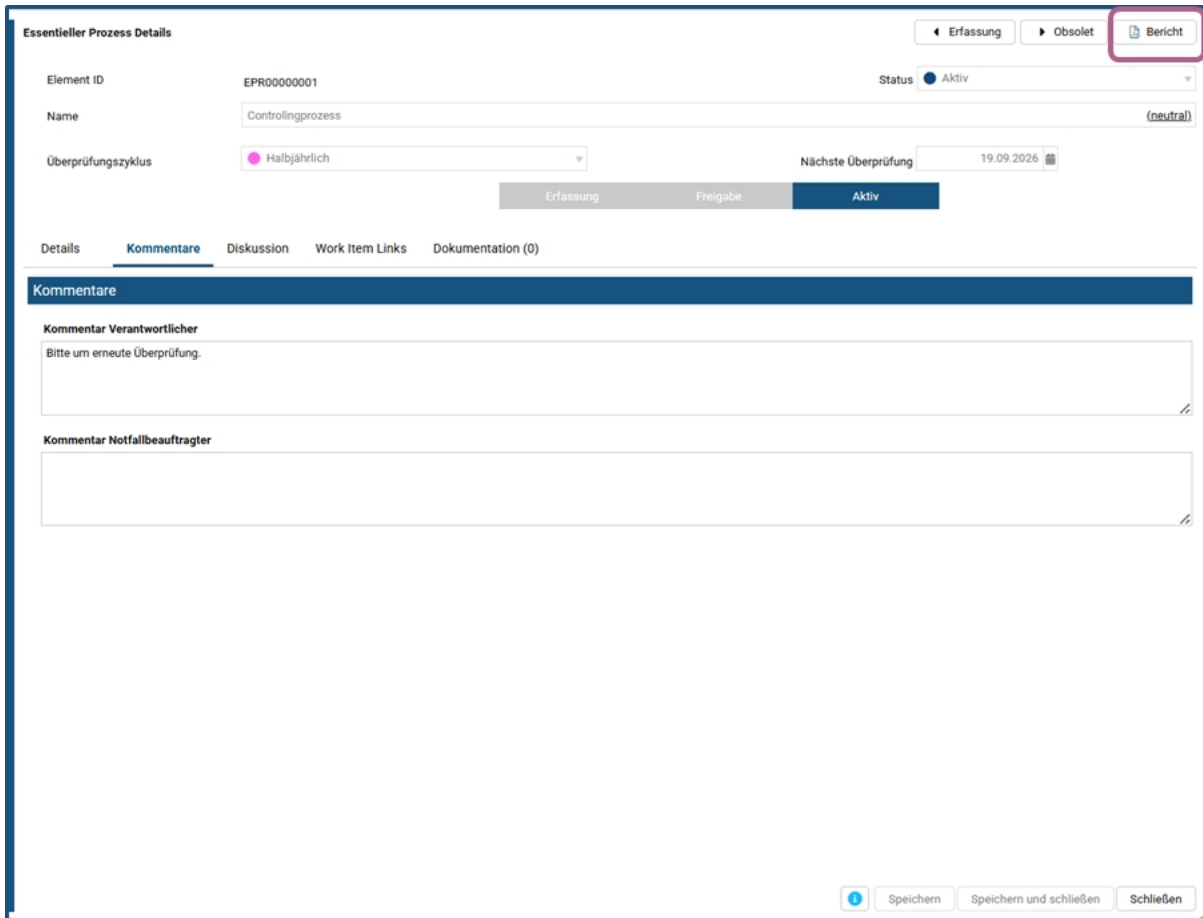
Nach dem Statusübergang kann das Fenster geschlossen werden.

Schritt 4: Bericht generieren

Nachdem der *Essentielle Prozess* in den Status "Aktiv" geschaltet wurde können der Bearbeiter DS und der Freigeber DS einen Bericht generieren.

Der Bericht ist eine Zusammenfassung des gesamten *Essentiellen Prozesses*.

Die Generierung des Berichts wird in der oberen rechten Fensterseite des Work Items durchgeführt. Bei der Ausgabedatei handelt es sich um ein Word.

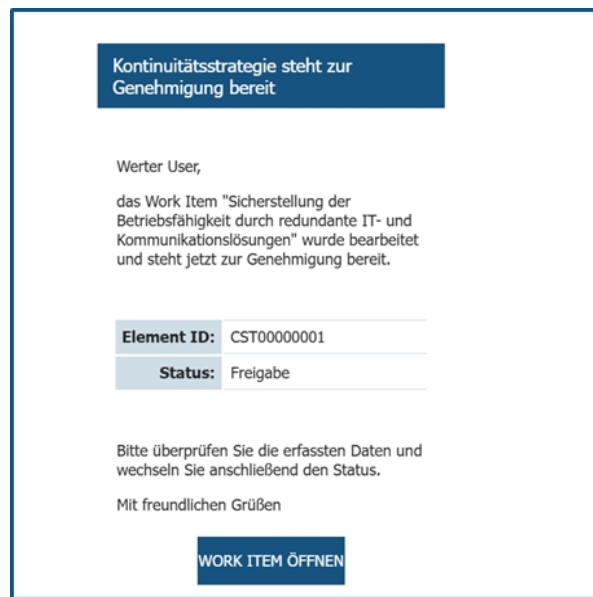


1.16.4 Kontinuitätsstrategie überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung einer *Kontinuitätsstrategie* des Bearbeiter DS mittels Notifikation informiert.

Schritt 1: Navigation zu Kontinuitätsstrategie

Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Kontinuitätsstrategie* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu dem spezifischen *Kontinuitätsstrategie* befindet sich in der Notifikation.



Kontinuitätsstrategie steht zur Genehmigung bereit

Werter User,

das Work Item "Sicherstellung der Betriebsfähigkeit durch redundante IT- und Kommunikationslösungen" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	CST00000001
Status:	Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.

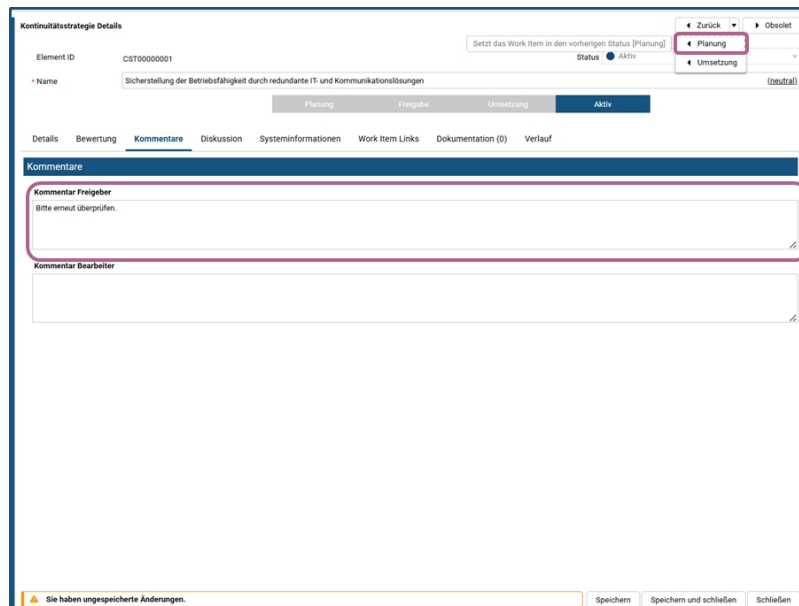
Mit freundlichen Grüßen

[WORK ITEM ÖFFNEN](#)

Schritt 2: Kontinuitätsstrategie überprüfen

Der Freigeber DS hat in der bewerteten *Kontinuitätsstrategie* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Kontinuitätsstrategie* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

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



Kontinuitätsstrategie Details

Element ID: CST00000001

Name: Sicherstellung der Betriebsfähigkeit durch redundante IT und Kommunikationslösungen

Status: Aktiv

Planung Freigabe Umsetzung Aktiv

Details Bewertung **Kommentare** Diskussion Systeminformationen Work Item Links Dokumentation (0) Verlauf

Kommentare

Kommentar Freigeber
Bitte erneut überprüfen.

Kommentar Bearbeiter

Sie haben ungespeicherte Änderungen.

Speichern Speichern und schließen Schließen

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Umsetzung" schalten. Der verantwortliche Bearbeiter DS wird mittels Notifikation über den Statuswechsel benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.16.5 Notfallplan überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung und Planung eines *Notfallplans* mittels Notifikation informiert.

Schritt 1: Navigation zu Notfallplan

Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald ein *Notfallplan* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu dem spezifischen *Notfallplan* befindet sich in der Notifikation.

Notfallplan steht zur Bearbeitung bereit

Werter User,

das Work Item "Notfallplan IT- und Kommunikationsausfall" steht zur Bearbeitung bereit.

Element ID:	EPL00000001
Status:	Freigabe

Bitte bearbeiten Sie das Work Item und wechseln Sie anschließend den Status.

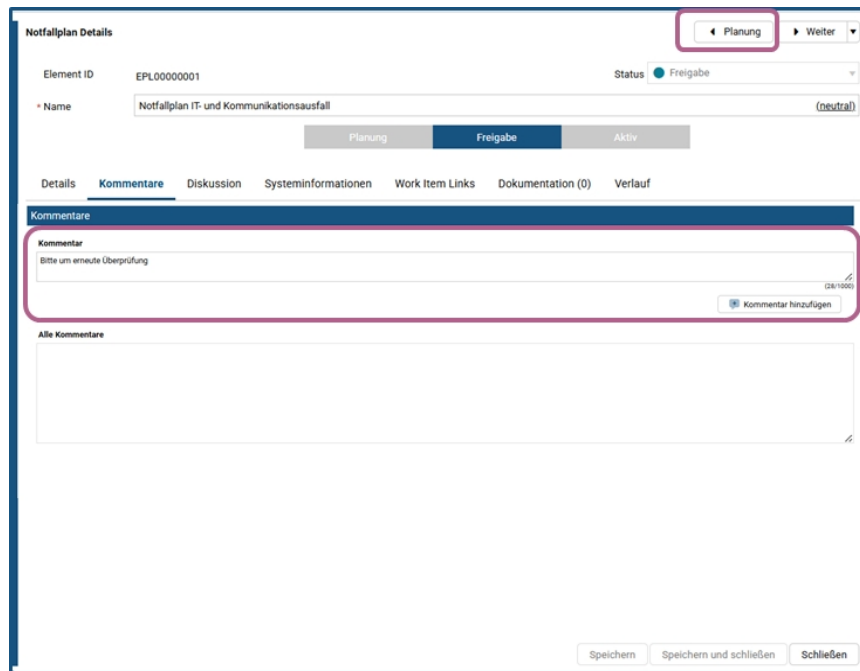
Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

Schritt 2: Notfallplan überprüfen

Der Freigeber DS hat in dem bewerteten *Notfallplan* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob der *Notfallplan* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

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



Schritt 3: Statusübergang durchführen

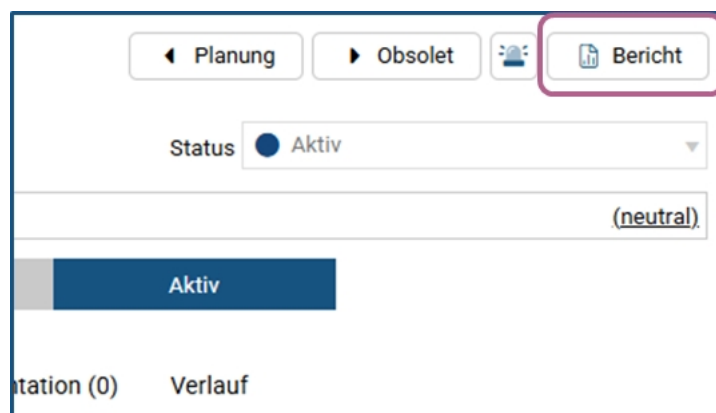
Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Aktiv" schalten. Der verantwortliche Vorsorgekoordinator wird mittels Notifikation über den Statuswechsel benachrichtigt.

Schritt 4: Bericht generieren

Nachdem der *Notfallplan* in den Status "Aktiv" geschaltet wurde können der Bearbeiter DS und der Freigeber DS einen Bericht generieren.

Der Bericht ist eine Zusammenfassung des gesamten *Notfallplans*.

Die Generierung des Berichts wird in der oberen rechten Fensterseite des Work Items durchgeführt. Bei der Ausgabedatei handelt es sich um ein PDF.



1.16.6 Notfallübung überprüfen & freigeben

Der Freigeber DS wird nach der Erstellung und Planung einer *Notfallübung* mittels Notifikation informiert.

Schritt 1: Navigation zu Notfallübung

Der Freigeber DS bekommt automatisch von BIC GRC eine E-Mail zugesendet, sobald eine *Notfallübung* erstellt und bearbeitet wurde sowie ein Statusübergang erfolgt ist. Der Link zu der spezifischen *Notfallübung* befindet sich in der Notifikation.



Notfallübung steht zur Genehmigung bereit

Werter User,

das Work Item "Simulation eines Ausfalls von IT- und Kommunikationssystemen" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	EDR00000001
Status:	Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.

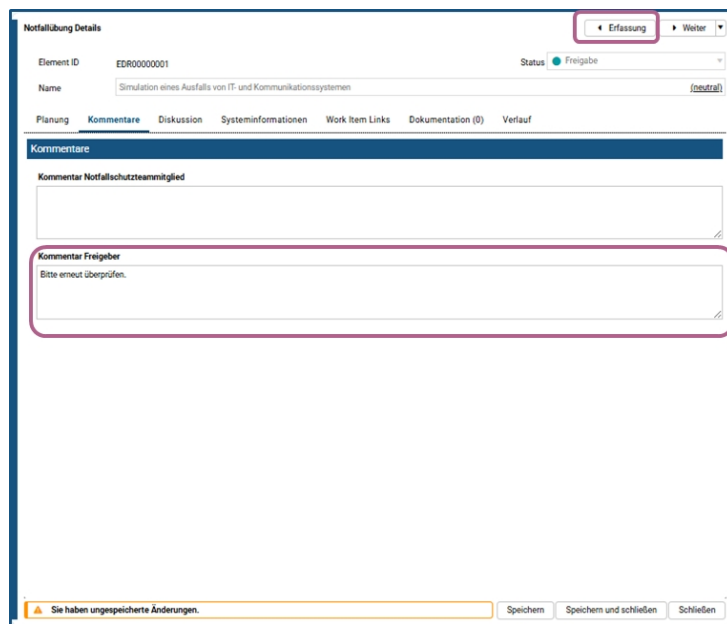
Mit freundlichen Grüßen

[WORK ITEM ÖFFNEN](#)

Schritt 2: Notfallplan überprüfen

Der Freigeber DS hat in der geplanten *Notfallübung* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob die *Notfallübung* richtig eingeordnet und die richtigen Rückschlüsse getroffen wurden.

Sollte dies nicht der Fall sein und muss die *Notfallübung* aus Sicht des Freigeber DS erneut überprüft werden, kann der Freigeber DS einen Kommentar im Tab "Kommentar" hinterlassen und einen Statuswechsel in den Status "Erfassung" durchführen.



Notfallübung Details

Element ID: EDR00000001 Status: Freigabe

Name: Simulation eines Ausfalls von IT- und Kommunikationssystemen (neutral)

Planung Kommentare Diskussion Systeminformationen Work Item Links Dokumentation (0) Verlauf

Kommentare

Kommentar Notfallschutzteammitglied

Kommentar Freigeber
Bitte erneut überprüfen.

Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

Schritt 3: Statusübergang durchführen

Sollten die Eingaben der vorgelagerten Benutzer passen, kann der Freigeber DS weiter in den Status "Geplant" schalten. Der verantwortliche Vorsorgekoordinator wird mittels Notifikation über den Statuswechsel benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.16.7 Bericht(e) öffnen & generieren

Der Freigeber DS und Manager können jederzeit einen vorbereiteten Bericht erstellen lassen. Der Bericht wird im Format PDF aufbereitet.

Vor der Berichtserstellung wird dem Freigeber DS oder Manager geraten eine Archivierung der Daten mittels Rollforward vorzunehmen.

1.17 Vorsorgekoordinator

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

Folgende Aufgaben hat ein Vorsorgekoordinator in BIC GRC:

- [Notfallplan definieren & planen](#)
- [Notfallaktivität definieren & erstellen](#)
- [Notfallübungen ableiten & erstellen](#)
- [Notfallübung einleiten & durchführen](#)
- [Finding identifizieren & erstellen](#)

Der Vorsorgekoordinator 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:

- [Security-Risiken identifizieren & erstellen](#)
- [Maßnahmen identifizieren & erstellen](#)

1.17.1 Notfallplan definieren & planen

Eine *Notfallplan* kann von einem Bearbeiter DS aus einer *Kontinuitätsstrategie* abgeleitet werden und muss von einem hinterlegten Vorsorgekoordinator geplant werden.

Schritt 1: Navigation zu spezifischer Notfallplan nach Fremderstellung

Der Vorsorgekoordinator hat zwei Möglichkeiten einen zu bearbeitenden *Notfallplan* zu öffnen.

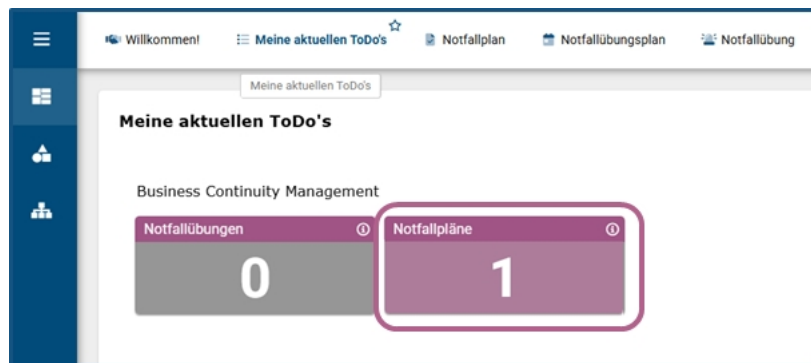
1. Öffnen über Notifikation

Der Vorsorgekoordinator bekommt eine E-Mail zugesendet, sobald der Ersteller alle Eingaben im Status "NEW" abgeschlossen hat. Der Link zu der spezifischen *Notfallplan* 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 das Vorsorgekoordinator noch eine Aufgabe zu erledigen hat.

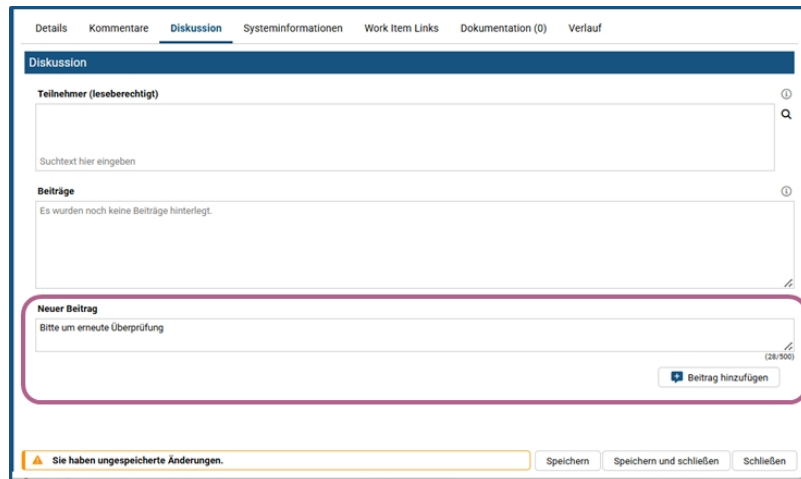


Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich ein neues Fenster für den *Notfallplan* automatisch.

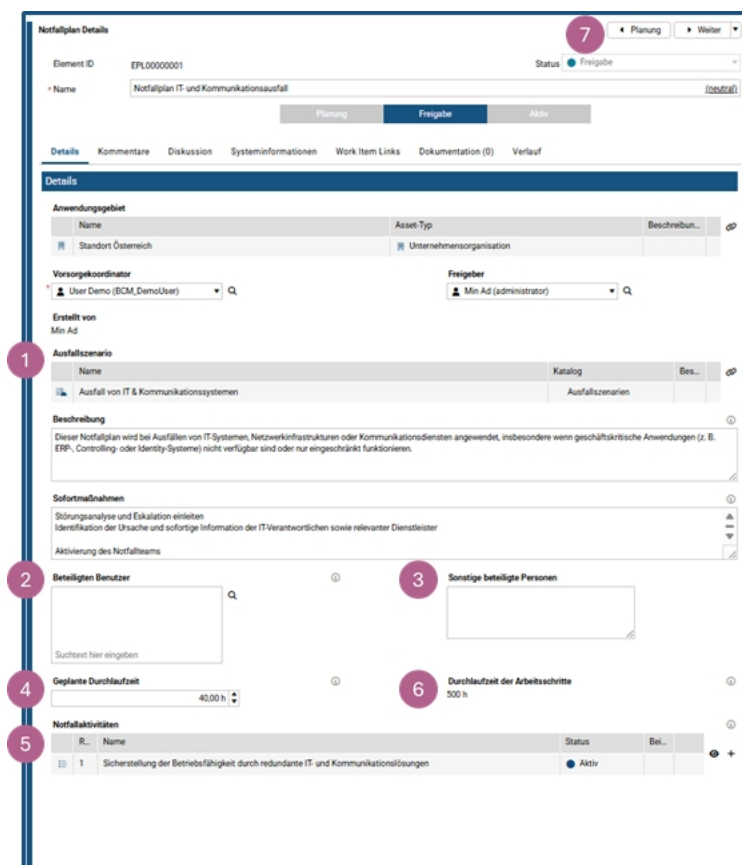
Optional Schritt 2: Überprüfung der Eingaben des Erstellers

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

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



Schritt 3: Eingaben ergänzen



- 1 **Ausfallsszenario:** Das Ausfallsszenario wird automatisch von der *Kontinuitätsstrategie* übernommen und kann nicht mehr verändert werden.
- 2 **Beteiligte Benutzer:** Mittels des Icons  kann das Vorsorgekoordinator "Beteiligte Benutzer" aus GRC hinterlegen. Dabei werden ihm alle aktiven Benutzer aus BIC GRC angezeigt.
- 3 **Sonstige beteiligte Personen:** Sollten noch weitere Personen beteiligt sein die an diesem *Notfallplan* mitwirken, die allerdings keinen Benutzer in BIC GRC haben, können diese mittels des Textfeldes schriftlich hinterlegt werden.
- 4 **Geplante Durchlaufzeit:** Anschließend muss das Vorsorgekoordinator eine Durchlaufzeit angeben. Dabei handelt es sich um die perspektivische Informationen wie lange der der *Notfallplan* braucht um durchlaufen zu werden.
- 5 **Notfallaktivitäten:** Nach den Angaben kann das Vorsorgekoordinator anfangen die einzelnen *Notfallaktivitäten* zu dokumentieren. Mehr Informationen über die Erstellung einer *Notfallaktivität* unter [Vorsorgekoordinator - Notfallaktivität definieren & erstellen](#).
- 6 **Durchlaufzeit der Arbeitsschritte:** Aus der Angabe der Notfallaktivitäten wird automatisch berechnet, wie lange die Summe der Arbeitsschritte aller *Notfallaktivitäten* insgesamt braucht.
- 7 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu in "Freigabe" durchgeführt.

Nach dem Statuswechsel wird der eingetragene Freigeber DS mittels Notifikation benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.17.2 Notfallaktivität definieren & erstellen

Notfallaktivitäten sollen dabei unterstützen einen *Notfallplan* zu strukturieren und organisieren.

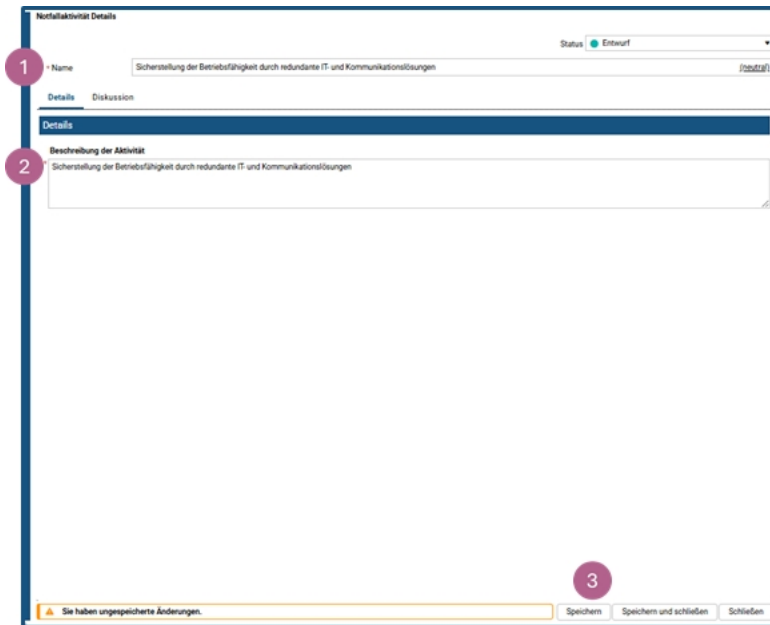
Schritt 1: Notfallaktivität erstellen

Notfallaktivitäten können nur aus Work Items des Typs *Notfallplan* erstellt werden.

Für die Erstellung wird im Tab "*Details*" durch das Icon  eine neue *Notfallaktivität* erstellt.



Schritt 2: Notfallaktivität beschreiben

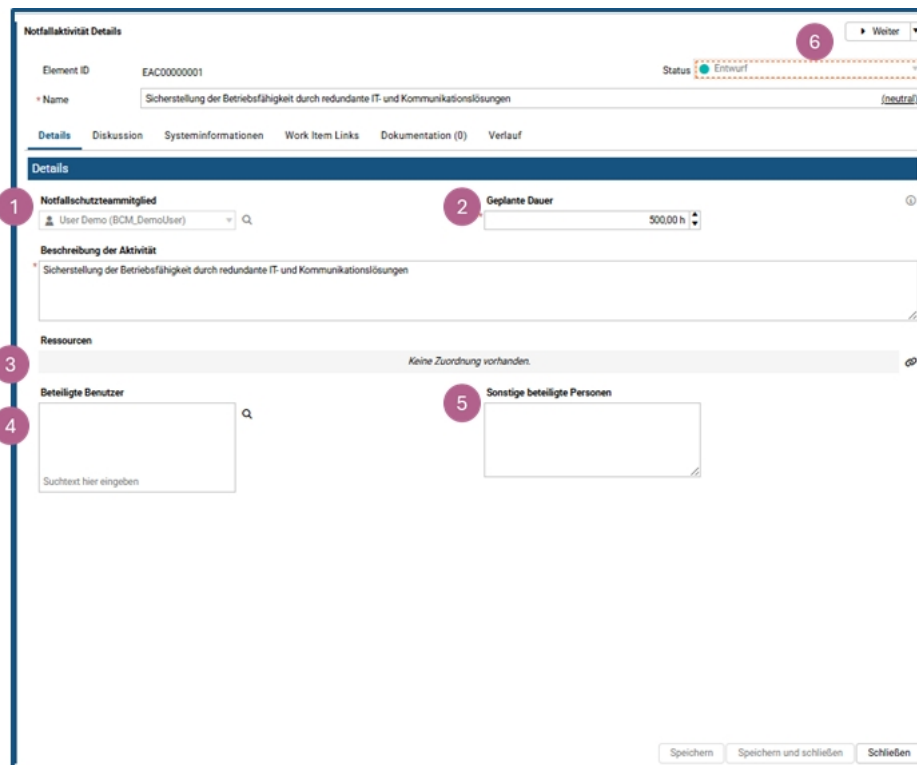


- 1 **Name:** Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Notfallaktivität* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht die *Notfallaktivität* einzigartig.
- 2 **Beschreibung:** Der Vorsorgekoordinator sollte eine ausführliche Angabe machen was die *Notfallaktivität* bezweckt und weitere wichtige und relevante Informationen angeben.
- 3 **Speichern:** Sobald alle Informationen eingetragen wurden kann die *Notfallaktivität* gespeichert werden.

Nach dem Klick auf den Button "Speichern" muss das Vorsorgekoordinator einen Rang angeben. Dieser Rang bestimmt in welcher Reihenfolge die einzelnen *Notfallaktivität* im Ablauf abgearbeitet werden sollen, sodass sich einzelne Schritte nicht zuvorkommen.

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

Schritt 3: Notfallaktivität ergänzen



- 1 **Vorsorgekoordinator** : Nach dem Speichervorgang wird das Vorsorgekoordinator automatisch in diesem Attribut hinterlegt und kann nicht mehr geändert werden.
- 2 **Geplante Dauer**: Für die einzelne Aktivität muss das Vorsorgekoordinator auch eine "Geplante Dauer" hinterlegen. Dies sollte erneut ein Schätzwert sein, wie lange die gesamte Aktivität dauern wird.
- 3 **Ressourcen**: Falls für die *Notfallaktivität* Ressourcen benötigt werden kann das Vorsorgekoordinator diese hier verlinken mittels des Icons .

Eine Erstellung einer *Ressource* ist nicht vorgesehen, sondern nur das verlinken einer bestehenden *Ressource*.

Nur *Ressourcen*, die zu einem Supporting Asset gehören, das einem Prozess zugewiesen ist, welcher über die Verknüpfungskette *Essentieller Prozess >> Risikoszenario >> Kontinuitätsstrategie >> Notfallplan* mit einer *Notfallaktivität* verbunden ist, können zugeordnet werden.

Mehr über die Erstellung von Ressourcen unter [Bearbeiter DS - Ressource identifizieren & erstellen](#).

- 4 **Beteiligte Benutzer**: Mittels des Icons  kann das Vorsorgekoordinator "Beteiligte Benutzer" aus GRC hinterlegen. Dabei werden ihm alle aktiven Benutzer aus BIC GRC angezeigt.

- 5 **Sonstige beteiligte Personen:** Sollten noch weitere Personen beteiligt sein die an dieser *Notfallaktivität* mitwirken, die allerdings keinen Benutzer in BIC GRC haben, können diese mittels des Textfeldes schriftlich hinterlegt werden.
- 6 **Statuswechsel:** Im oberen rechten Fenster wird nach Angabe aller Informationen ein Statusübergang zu "Aktiv" durchgeführt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

Es wird niemand über den Statuswechsel informiert.

Zurück zu dem Schritt [Vorsorgekoordinator - Notfallplan definieren & planen](#).

1.17.3 Notfallübungen ableiten & erstellen

Notfallübungen sollen dabei unterstützen einen *Notfallplan* einem realen Test zu unterziehen und Optimierungen festzustellen und vorzunehmen.

Schritt 1: Notfallübungen erstellen

1. Erstellen über Dashboard "Notfallübung"

Der Vorsorgekoordinator navigiert über die Menüleiste zu **Dashboards >> Notfallübung >> "Neue Notfallübung"**

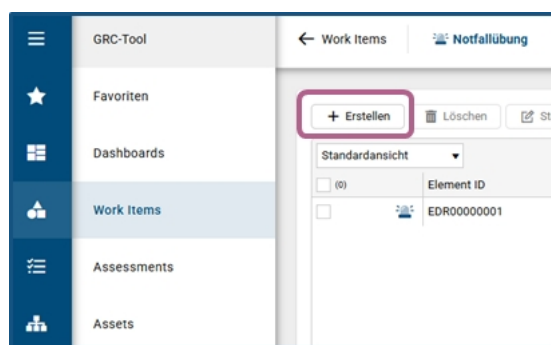
Die Erstellung einer neuen *Notfallübung* wird durch einen Button in der rechten oberen Fensterseite durchgeführt.

Ein neues Fenster öffnet sich anschließend automatisch.

2. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.



3. Erstellen über Work Item Notfallplan

Notfallübungen können aus Work Items des Typs *Notfallplan* in dem Status "Aktiv" erstellt werden.

Für die Erstellung wird mittels des Buttons in der rechten oberen Fensterseite eine neue *Notfallübung* erstellt.

Neben dem Button zur Erstellung von *Notfallübungen* findet der Vorsorgekoordinator einen Button "Bericht". Hinter diesem befindet sich eine Aufzählung aller Informationen aus dem *Notfallplan* und zugehörigen *Notfallaktivitäten*. Dieser Bericht ist für die spätere Ausführung der *Notfallübung* essentiell.

Schritt 2: Notfallübung beschreiben

Notfallübung steht zur Genehmigung bereit

Werter User,

das Work Item "Simulation eines Ausfalls von IT- und Kommunikationssystemen" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	EDR00000001
Status:	Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.

Mit freundlichen Grüßen

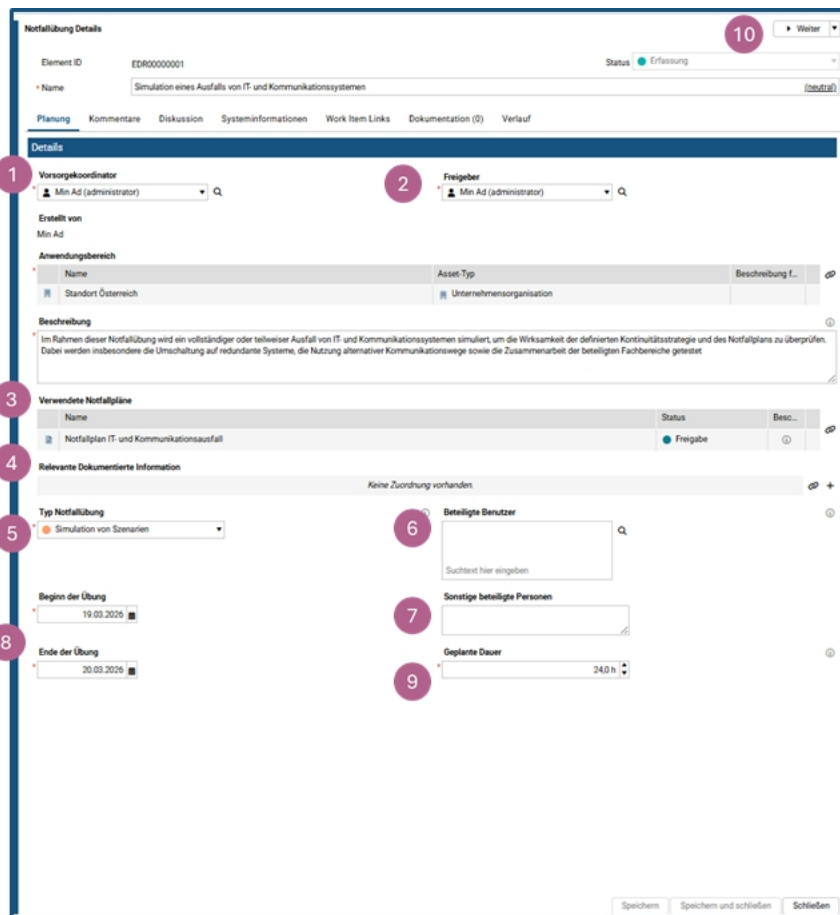
WORK ITEM ÖFFNEN

- 1 **Name:** Als erster Schritt sollte die Eingabe eines kurzen, aber aussagekräftigen Namens für die *Notfallübung* erfolgen. Dieser "Name" in Kombination mit der "Element ID" macht die *Notfallübung* einzigartig.
- 2 **Anwendungsgebiet:** Der Vorsorgekoordinator hat ein Anwendungsgebiet für den *Notfallplan* anzugeben. Dabei werden dem Vorsorgekoordinator bei der Auswahl nur Assets des Typen "Organisationseinheit" angezeigt.

Anders als beim *Notfallplan* ist die Filterung des Assets nicht nur auf den Asset Typen "Organisationseinheit", sondern spezifisch auf den Tag "Unternehmen" (Company) eingeschränkt.

- 3 **Beschreibung:** Der Vorsorgekoordinator sollte wichtige und relevante Informationen zu der *Notfallübung* angeben.
- 4 **Speichern:** Sobald alle Informationen eingetragen wurden kann die *Notfallübung* gespeichert werden.

Schritt 3: Notfallübung ergänzen



- 1 **Vorsorgekoordinator:** Nach dem Speichervorgang wird der Vorsorgekoordinator automatisch in diesem Attribut hinterlegt.
- 2 **Freigeber:** Der Freigeber kann mittels des Icons  gesucht werden. Er ist nach der Planung für die Freigabe der *Notfallübung* verantwortlich.
- 3 **Verwendete Notfallpläne:** Der spezifischen *Notfallübung* können ein oder mehrere *Notfallpläne* als Basis für die Übung dienen.

Wenn die *Notfallübung* direkt aus dem *Notfallplan* erstellt wird, wird der Link nach dem ersten Speichervorgang automatisch mit dem *Notfallplan* befüllt.

Es ist nicht vorgesehen, dass *Notfallpläne* aus einer *Notfallübung* erstellt werden. Die *Notfallpläne* müssen feststehen

- 4 **Relevante Dokumentierte Informationen:** Neben den *Notfallplänen* kann es Sinn machen auch *Dokumentierte Informationen* zu verlinken.

Sollten beispielsweise für die *Notfallübung* Genehmigungen eingeholt worden sein können diese hier verlinkt werden.

- 5 **Typ Notfallübung:** Eine Notfallübung hat ein bestimmtes Übungsziel (z. B. Test der Alarmierungskette). Für die genauere Einordnung hat der Vorsorgekoordinator einen Typen zu definieren, wie dieses Ziel erreicht werden soll.

So kann eine Simulation (z. B. IT-Ausfall, Cyberangriff) oder ein Live-Test (mit echter Umschaltung oder Wiederanlauf) als eigener Typ hinterlegt werden.

- 6 **Beteiligte Benutzer:** Mittels des Icons  kann der Vorsorgekoordinator "Beteiligte Benutzer" aus GRC hinterlegen. Dabei werden ihm alle aktiven Benutzer aus BIC GRC angezeigt.

- 7 **Sonstige beteiligte Personen:** Sollten noch weitere Personen beteiligt sein die an dieser *Notfallübung* mitwirken, die allerdings keinen Benutzer in BIC GRC haben, können diese mittels des Textfeldes schriftlich hinterlegt werden.

- 8 **Zeitraum der Übung:** Der Vorsorgekoordinator hat sowohl ein Datum für den Beginn der *Übung*, als auch eins für das geplante Ende anzugeben. In diesem Zeitraum soll die *Notfallübung* stattfinden.

- 9 **Geplante Dauer:** Neben dem Zeitraum ist die "Geplante Dauer" der *Notfallübung* in der Einheit Stunden (h) anzugeben.

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

Der Freigeber DS wird nach dem Statuswechsel mittels Notifikation benachrichtigt.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.17.4 Notfallübung einleiten & durchführen

Der Bearbeiter wird im Rahmen eines Schedulers mittels einer Notifikation erinnert, dass die *Notfallübung* durchzuführen ist. Dabei bezieht sich die Erinnerung auf das hinterlegte Datum, wann die *Notfallübung* beginnen wird.

Einen guten Überblick über die anstehenden *Notfallübungen* bekommt der Vorsorgekoordinator weiters unter dem Menüpunkt **Dashboards >> Notfallüberungsplan**.

Schritt 1: Navigation zu Notfallübung

Der Vorsorgekoordinator hat zwei Möglichkeiten eine durchzuführende *Notfallübungen* zu öffnen.

1. Öffnen über Notifikation

Der Vorsorgekoordinator bekommt eine E-Mail zugesendet, sobald das Datum wann die *Notfallübung* durchgeführt werden soll erreicht ist. Der Link zu der spezifischen *Notfallübung* befindet sich in der Notifikation.

The screenshot shows an email notification with a blue header bar that reads "Notfallübung steht zur Genehmigung bereit". The body of the email addresses "Werter User," and states that the work item "Simulation eines Ausfalls von IT- und Kommunikationssystemen" has been processed and is now ready for approval. Below this, there is a table with two rows: "Element ID:" with the value "EDR00000001" and "Status:" with the value "Freigabe". Further down, the email asks the user to check the entered data and change the status, followed by a friendly greeting. At the bottom right, there is a blue button labeled "WORK ITEM ÖFFNEN".

Element ID:	EDR00000001
Status:	Freigabe

2. Öffnen über Dashboard "Notfallübung"

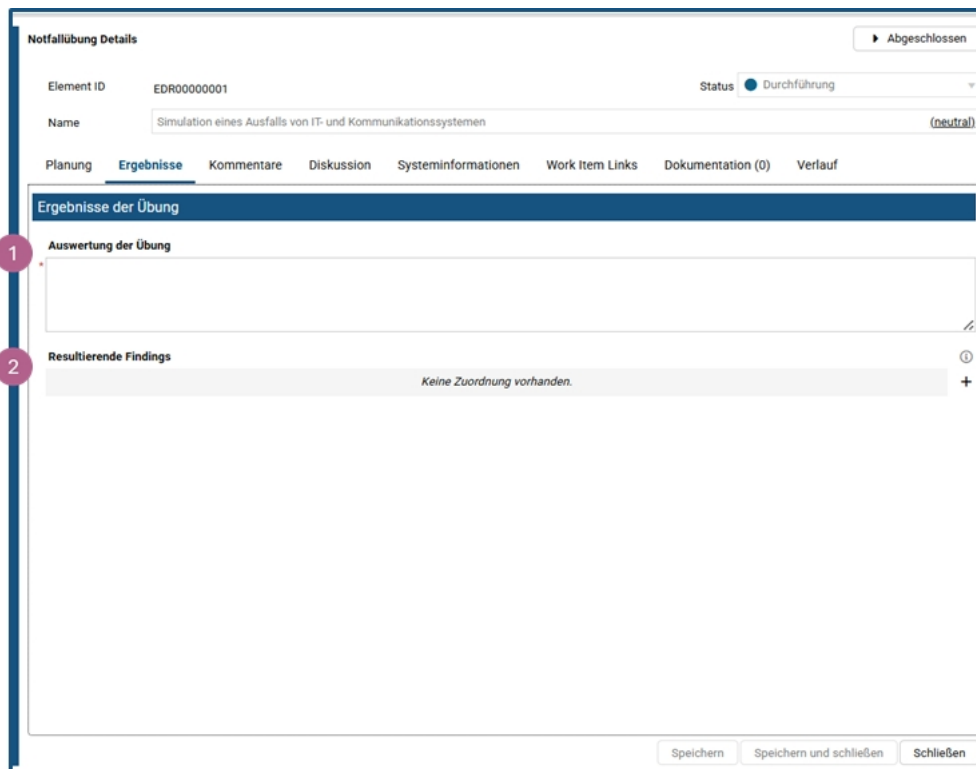
Der Bearbeiter kann in dem Dashboard nach seinen *Notfallübungen* filtern.

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

Schritt 2: Notfallübung starten

Der Vorsorgekoordinator hat als ersten Schritt den Statuswechsel von "Geplant" zu in "Durchführung" in der oberen rechten Fensterseite vorzunehmen. Nach dem Statuswechsel wird er automatisch in den Tab "*Ergebnisse*" weitergeleitet.

In diesem kann er schriftlich eine "Auswertung der Übung" ¹ dokumentieren und zudem aus der durchgeführten *Notfallübung* "Resultierende Findings" ² ableiten. Mehr zu der Erstellung von einem *Finding* unter [Vorsorgekoordinator - Finding identifizieren & erstellen](#).



Schritt 3: Statuswechsel durchführen

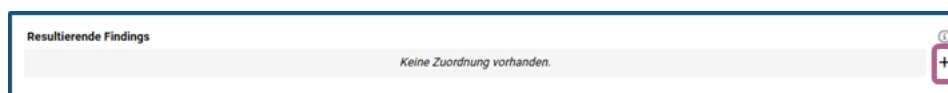
Nachdem eine Auswertung erfolgt und alle *Findings* erfasst worden sind kann der Vorsorgekoordinator in den Status "Abgeschlossen" weiterschalten.

Nach dem Statusübergang kann das Fenster geschlossen werden.

1.17.5 Finding identifizieren & erstellen

Sollte der Vorsorgekoordinator während der Durchführung einer *Notfallübung* zu der Erkenntnis kommen, dass es Verbesserungspotenzial gibt, das im Rahmen der *Notfallübung* aufgekommen ist, muss der Vorsorgekoordinator ein *Finding* erstellen.

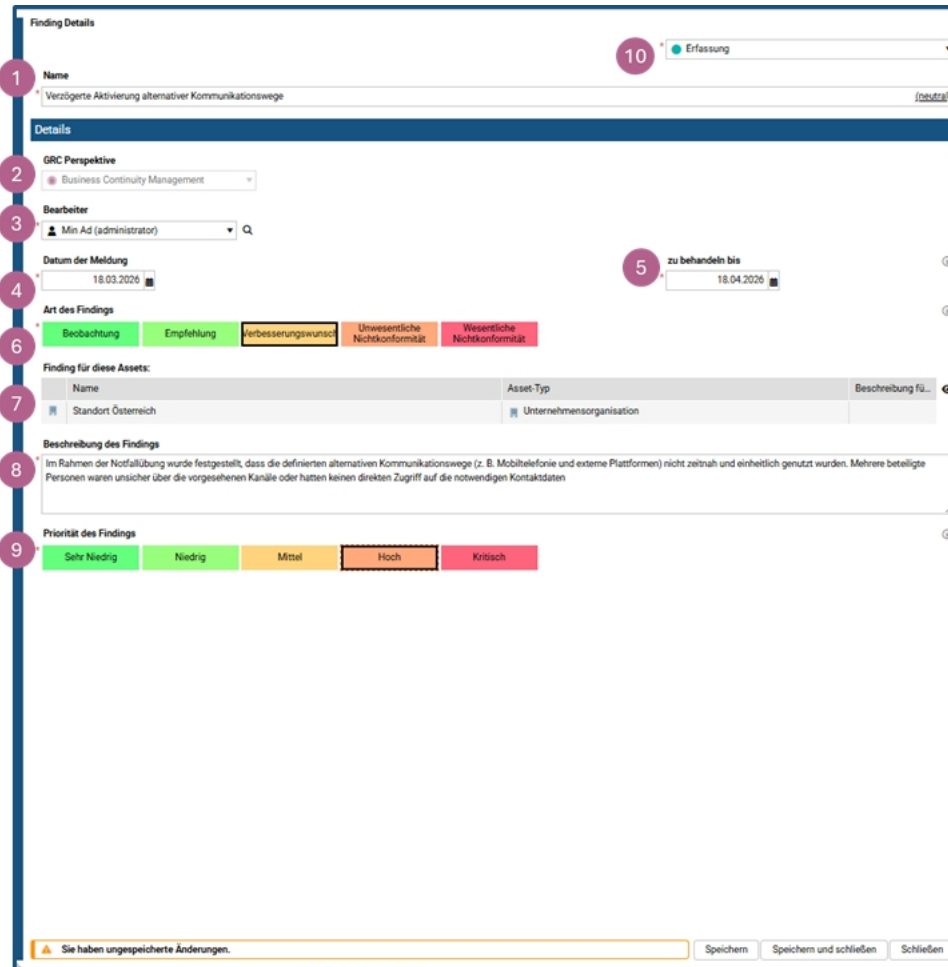
Schritt 1: Finding aus Notfallübung erstellen.



Ein *Finding* kann aus einer *Notfallübung* entstehen.
Die Erstellung erfolgt durch das Icon .

Das *Finding* geht automatisch in der *Notfallübung* auf.

Schritt 2: Finding dokumentieren



Finding Details

1 **Name**: Verzügerte Aktivierung alternativer Kommunikationswege (neutral)

2 **GRC Perspektive**: Business Continuity Management

3 **Bearbeiter**: Min Ad (administrator)

4 **Datum der Meldung**: 18.03.2026

5 **zu behandeln bis**: 18.04.2026

6 **Art des Findings**: Beobachtung, Empfehlung, Verbesserungswunsch, Unwesentliche Nichtkonformität, Wesentliche Nichtkonformität

7 **Finding für diese Assets**:

Name	Asset-Typ	Beschreibung fü...
Standort Österreich	Unternehmensorganisation	

8 **Beschreibung des Findings**: Im Rahmen der Notfallübung wurde festgestellt, dass die definierten alternativen Kommunikationswege (z. B. Mobiltelefonie und externe Plattformen) nicht zeitnah und einheitlich genutzt wurden. Mehrere beteiligte Personen waren unsicher über die vorgesehenen Kanäle oder hatten keinen direkten Zugriff auf die notwendigen Kontaktdaten.

9 **Priorität des Findings**: Sehr Niedrig, Niedrig, Mittel, Hoch, Kritisch

10 **Status**: Erfassung

Sie haben ungespeicherte Änderungen. [Speichern] [Speichern und schließen] [Schließen]

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 *Notfallübung* übernommen.

3 **Bearbeiter**: In das Attribut soll jener Bearbeiter eingetragen werden der für das *Finding* der *Notfallübung* 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 eine 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 *Notfallübung* ist.
- 7 **Finding für dieses Asset:** Das Asset wird nicht automatisch aus dem Work Item übernommen sondern muss 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 Dashboards verwendet werden kann.
- 10 **Statuswechsel:** Der Ersteller kann abschließend in den Status in "Behandlung" schalten. Mehr Informationen zu dem Statuswechsel in Finding sichten & behandeln.

Anschließend kann der Vorsorgekoordinator in die *Notfallübung* zurückkehren und mit der Dokumentation der Dokumentation des *Notfallübung* fortfahren. [Vorsorgekoordinator - - Notfallübung einleiten & durchführen.](#)

1.18 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](#)

1.18.1 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.

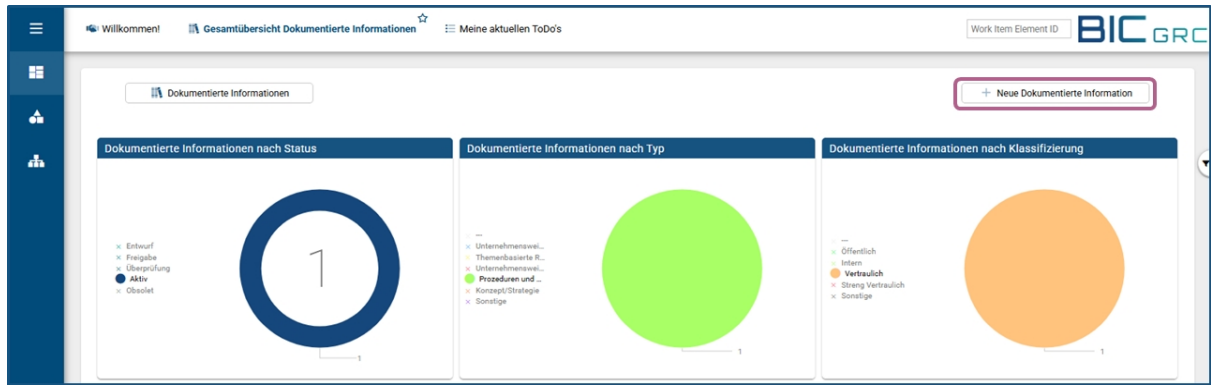
Schritt 1: Dokumentierte Information erstellen

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.

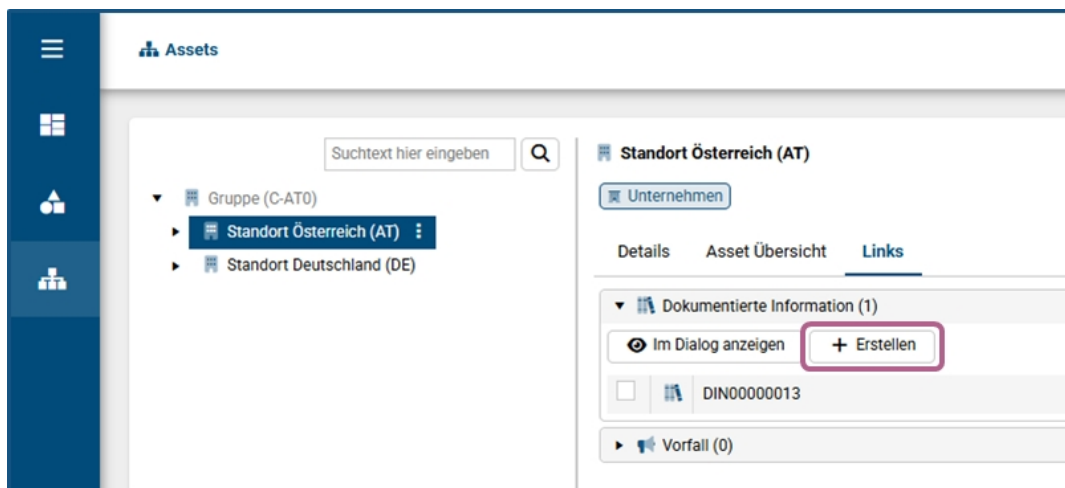


Ein neues Fenster öffnet sich anschließend automatisch.

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.

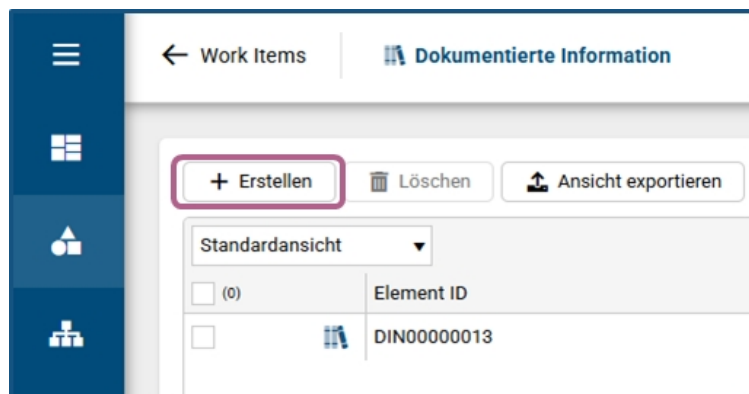


Ein neues Fenster öffnet sich anschließend automatisch.

3. Erstellung 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

Dokumentierte Information Details

Status Entwurf

* Name **1** (neutral)

Details

Details

2 Beschreibung

Diese Verfahrensanweisung beschreibt organisatorische und technische Maßnahmen zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse auch im Störfall. Sie enthält Vorgaben zur Identifikation kritischer Prozesse, zur Definition von Wiederanlaufzeiten (RTO), zur Absicherung durch IT-Systeme und externen Dienstleistern, sowie zur Durchführung regelmäßiger Tests von Notfall- und Wiederherstellungsverfahren.

3 Scope

Name	Asset-Typ	Beschrei...
Buchhaltungsprozess	Primary Asset	

4 Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

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

Dokumentierte Information Details Weiter

Element ID: DIN00000009 Status: Entwurf

Name: Verfahrensanweisung zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse (neutral)

Überprüfungszyklus: 1 Quartalsweise Nächste Überprüfung: 14.04.2026

Entwurf Freigabe Überprüfung Aktiv

Details Kommentare Diskussion Work Item Links

Details

2 **Bearbeiter**
 * DocumentOwner GEN (DocumentO...
Freigeber
 * DocumentManager GEN (Document...
Erstellt von
 DocumentOwner GEN

Leseberechtigung erteilen an
 * ApproverDomainSpecific...
 ApproverDomainSpecific...
 EditorDomainSpecific CS...
 Suchtext hier eingeben

3 **GRC Perspektiven**
 Information Security Management Business Continuity Management Privacy Management
 Enterprise Risk Management Internal Control Corporate Sustainability
 Auswählen...

4 **Zuordnung Primary Asset**

Name	Asset-Typ	Beschrei...
Kundenstammdaten	Primary Asset	

5 **Klassifizierung**
 Öffentlich Intern Vertraulich Streng Vertraulich Sonstige

6 **Zuordnung Dokumentation**
 Dateien hierher ziehen zum Hochladen

Verfahrensanweisung zur Sicherstellung	DocumentOwner GEN	13.01.2026 13:41
+		

Beschreibung
 * Diese Verfahrensanweisung beschreibt organisatorische und technische Maßnahmen zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse auch im Störfall.
 Sie enthält Vorgaben zur Identifikation kritischer Prozesse, zur Definition von Wiederanlaufzeiten (RTO), zur Absicherung durch IT-Systeme und externen Dienstleistern, sowie zur Durchführung regelmäßiger Tests von Notfall- und Wiederherstellungsverfahren.

7 **Typ**
 Unternehmensweite Leitlinie Themenbasierte Richtlinien Unternehmensweiter Standard **Prozeduren und Vorgaben** Konzept/Strategie Sonstige

Speichern Schließen

- 1 **Überprüfungszyklus:** Der Dokumenteneigner muss einen "Überprüfungszyklus" hinterlegen. Der Überprüfungszyklus gibt an, wie oft eine *Dokumentierten Information* zurück in den Status "Überprüfung" geschaltet wird, um die *Dokumentierten Information* in regelmäßigen Zeitabständen zu evaluieren.

Das Attributsfeld "Nächste Überprüfung" wird automatisch von BIC GRC gesetzt.

- 2 **Verantwortliche Personen:** Der Dokumenteneigner 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 freigeschalteten 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.

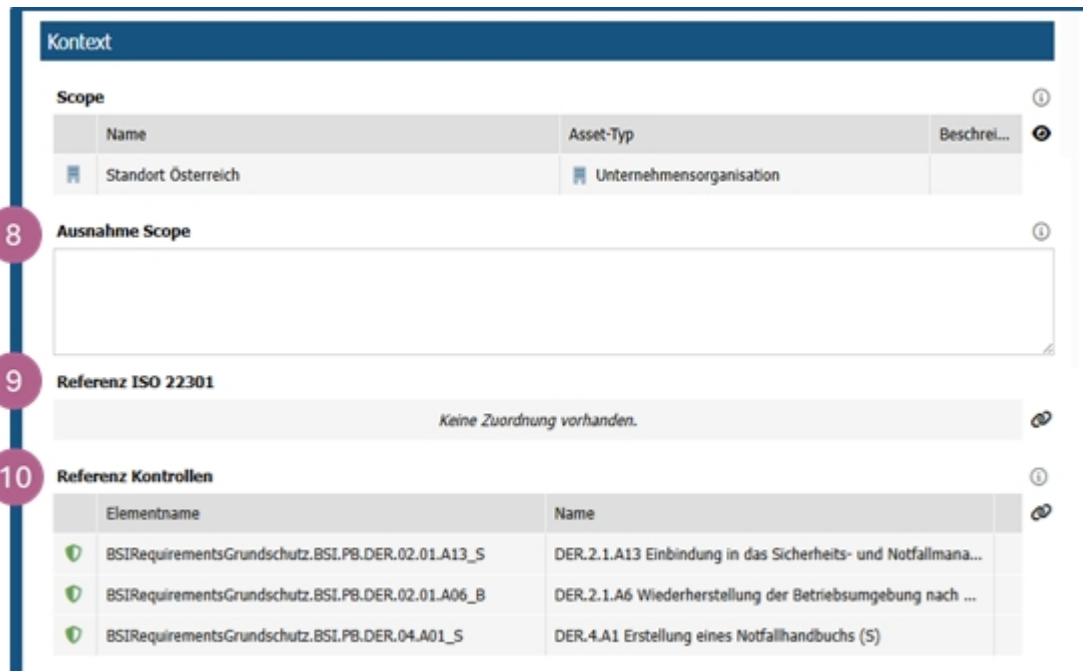
- 9 **Referenz ISO 22301:** Für das Modul Business Continuity Management sollte eine Referenz zu dem GRC Framework "ISO 22301:2019" mittels  vorgenommen werden.

- 10 **Referenz Kontrollen:** Die "Referenz Kontrolle" führt nicht zu Work Items des Typen *Kontrolle*, sondern zu den Kontrollkatalogen von

- BSI Anforderungen BCM

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

Der Dokumentenmanager wird mittels Notifikation automatisch über den Statusübergang informiert.



Kontext

Scope

Name	Asset-Typ	Beschrei...
Standort Österreich	Unternehmensorganisation	

8 **Ausnahme Scope**

9 **Referenz ISO 22301**

Keine Zuordnung vorhanden.

10 **Referenz Kontrollen**

Elementname	Name
BSIRequirementsGrundschutz.BSI.PB.DER.02.01.A13_S	DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmana...
BSIRequirementsGrundschutz.BSI.PB.DER.02.01.A06_B	DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach ...
BSIRequirementsGrundschutz.BSI.PB.DER.04.A01_S	DER.4.A1 Erstellung eines Notfallhandbuchs (S)

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 Dokumenteneigner ein Kommentar in dem Tab "Kommentar" hinterlassen und die *Dokumentierte Information* erneut in den Status "Entwurf" setzen. Der Dokumenteneigner wird über diesen Vorgang mittels Notifikation benachrichtigt.

1.18.2 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" geschaltet und der Benutzer bekommt erneut automatisch eine Notifikation zugesendet.

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

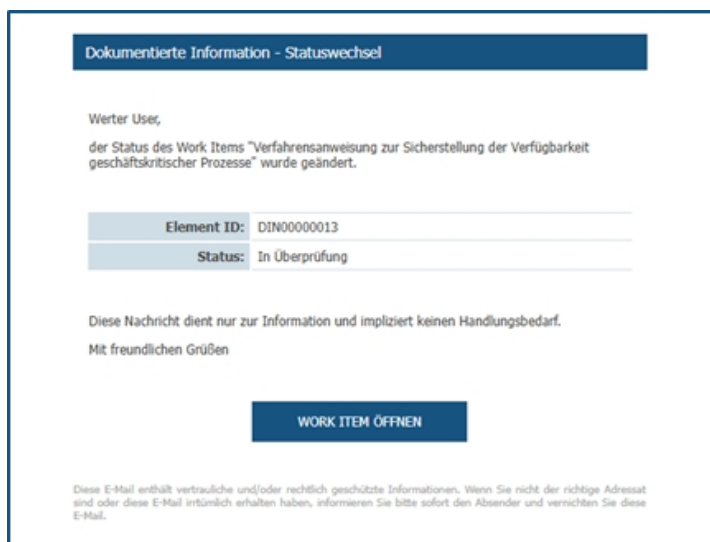
Wenn die *Dokumentierte Information* einer der Überprüfungszyklen "Alle ... Tage", "Anlassbezogen", "Täglich" oder "Wöchentlich" hat, wird der Status nicht automatisch zurückgesetzt und der Bearbeiter wird nicht über einen Statusübergang mittels Notifikation benachrichtigt.

Schritt 1: Navigation zu Dokumentierte Information

Der Dokumenteneigner hat zwei Möglichkeiten, eine zu bearbeitende *Dokumentierte Information* zu öffnen.

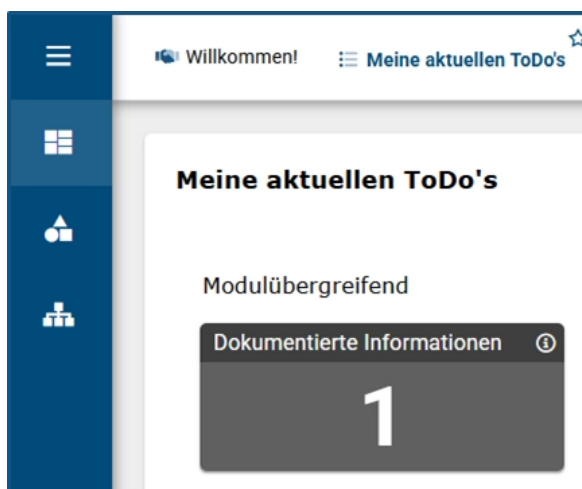
1. Öffnen über Notifikation

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.



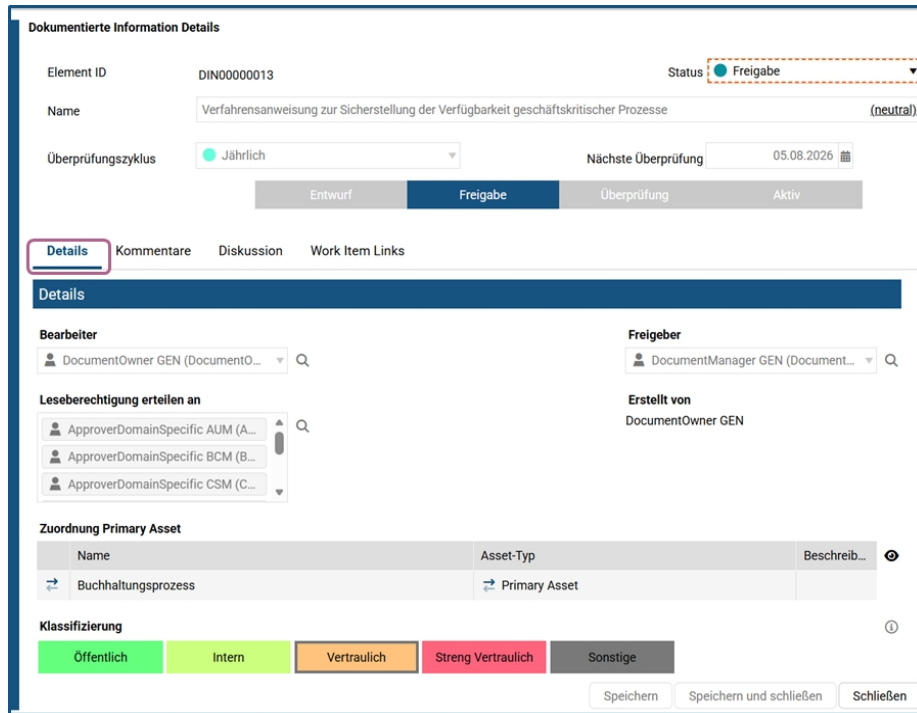
2. Öffnen über Dashboard "Meine aktuellen ToDo's"

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.

Dokumentierte Information Details

Entwurf
Freigabe

Element ID
DIN00000013

Status
Überprüfung

Name
Verfahrensanweisung zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse
(neutral)

Überprüfungszyklus
Jährlich
Nächste Überprüfung
05.08.2026

Entwurf
Freigabe
Überprüfung
Aktiv

Details
Anmerkungen
Kommentare
Diskussion
Work Item Links

Anmerkungen
Überprüfung

Überprüfungsdatum

Anmerkung Überprüfung

☐ Vollständigkeit und Aktualität des Dokuments wurde geprüft

Speichern
Speichern und schließen
Schließen

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.

1.19 Dokumentenmanager

Das Benutzerprofil Dokumentenmanager ist für die Freigabe und ordnungsgemäße Ablage einer spezifischen Information in BIC GRC verantwortlich.

1.19.1 Dokumentierte Information überprüfen & freigeben

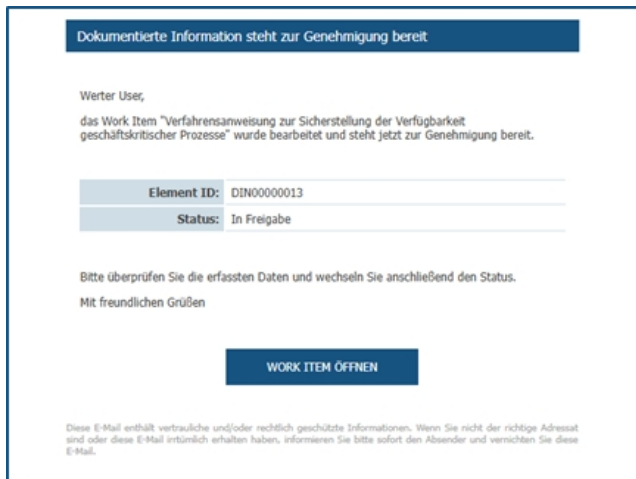
Nach der Erstellung und Hinterlegung einer *Dokumentierte Information* durch einen Dokumenteneigner, muss diese vor der Aktivierung einer Freigabe durch den Dokumentenmanager vollzogen werden.

Schritt 1: Navigation zur Dokumentierten Information

Der Dokumentenmanager hat zwei Möglichkeiten, eine zu bearbeitende *Dokumentierte Information* zu öffnen.

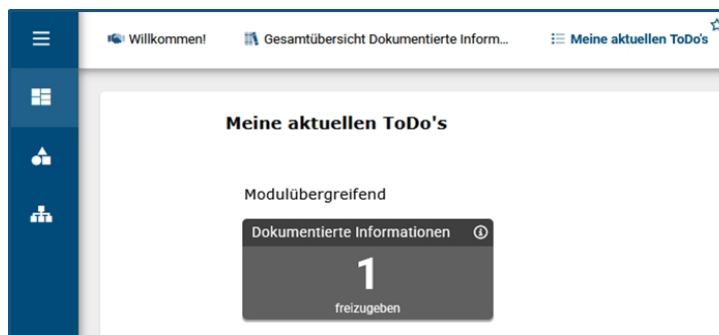
1. Öffnen über Notifikation

Der Dokumentenmanager bekommt eine E-Mail zugesendet, sobald der Dokumenteneigner den Status der *Dokumentierte Information* zu "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.

Dokumentierte Information Details

Entwurf

Aktiv

Element ID

DIN00000013

Status

Freigabe

Name

Verfahrensanweisung zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse

(neutral)

Überprüfungszyklus

Jährlich

Nächste Überprüfung

05.08.2026

Entwurf

Freigabe

Überprüfung

Aktiv

Details

Anmerkungen

Kommentare

Diskussion

Work Item Links

Anmerkungen

Überprüfung

Überprüfungsdatum

13.01.2026

Anmerkung Überprüfung

☐
Vollständigkeit und Aktualität des Dokuments wurde geprüft

Freigabe

Freigabedatum

Anmerkung Freigabe

☒
Dokument entspricht den notwendigen Vorgaben

Speichern

Speichern und schließen

Schließen

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.

1.20 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](#)

1.20.1 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.

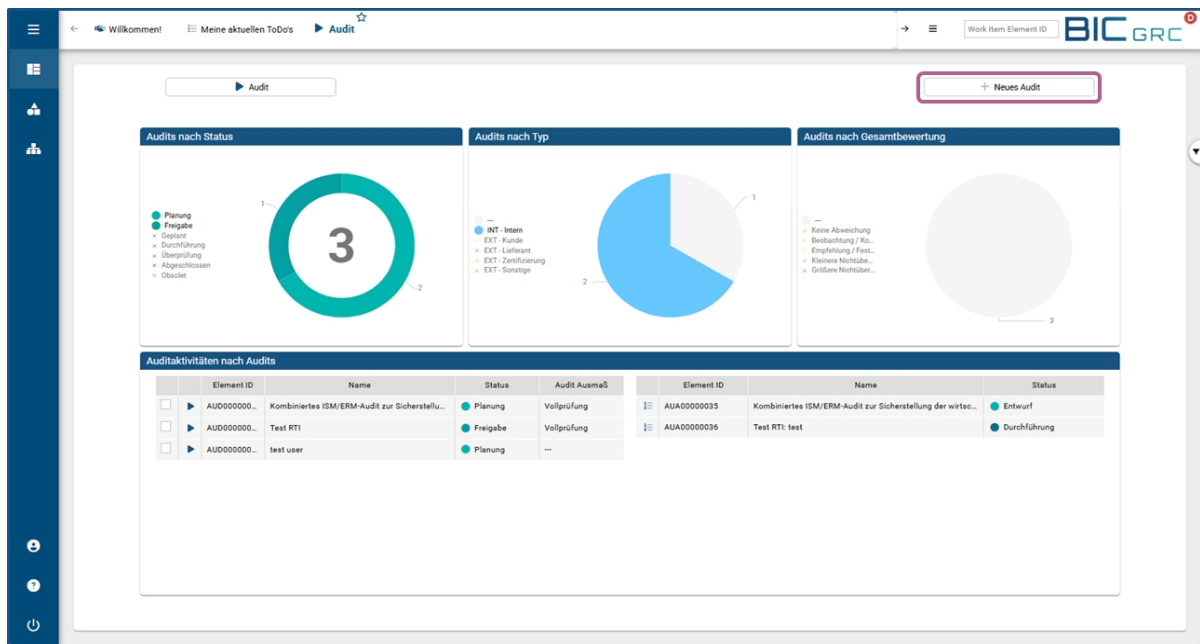
Schritt 1: Audit erstellen

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.

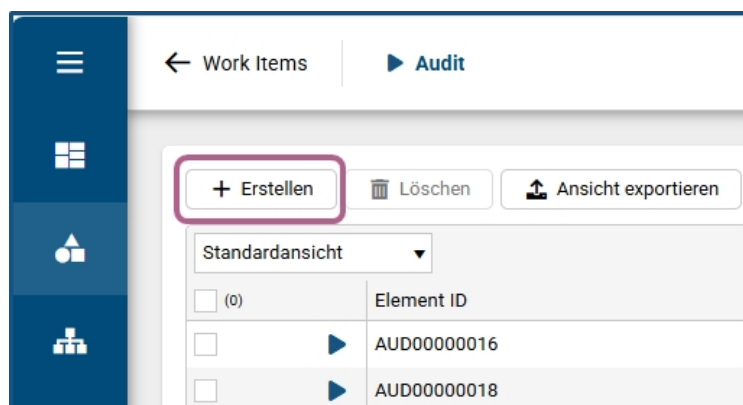


Ein neues Fenster öffnet sich anschließend automatisch.

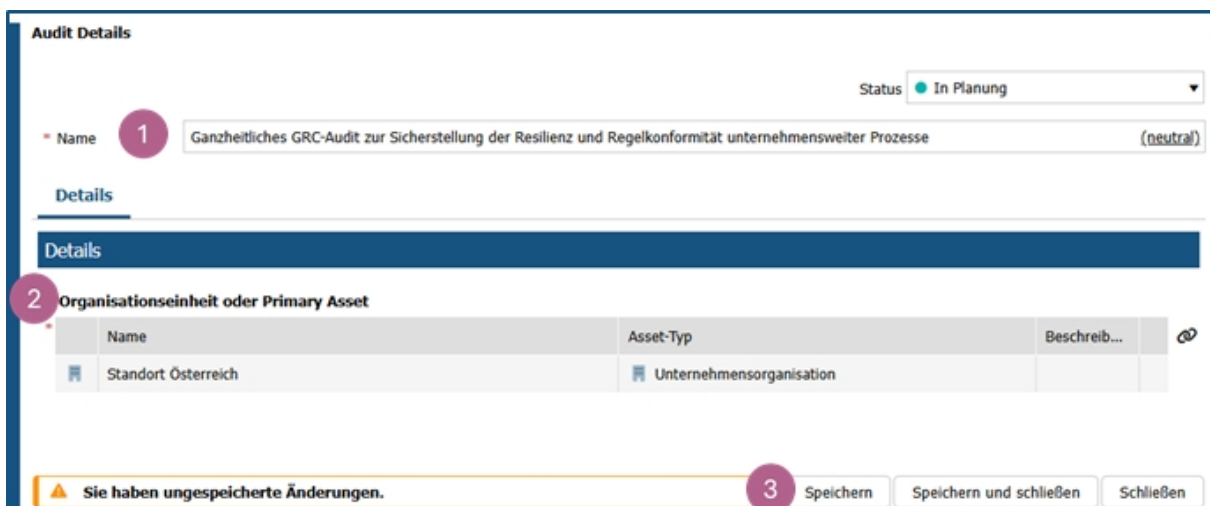
2. Erstellung über Work Item List

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

Ein neues Fenster öffnet sich anschließend automatisch.



Schritt 2: Details hinterlegen



The 'Audit Details' form shows the following fields and steps:

- Status:** In Planung
- Name (1):** Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse (neutral)
- Details (2):**

Name	Asset-Typ	Beschreib...
Standort Österreich	Unternehmensorganisation	
- Bottom Bar (3):** Sie haben ungespeicherte Änderungen. Speichern, Speichern und schließen, Schließen

- 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 Benutzer 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

Audit Details

Element ID: AUD00000001 Status: In Planung

Name: Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse (neutral)

In Planung | In Freigabe | Geplant | In Durchführung | In Überprüfung | Abgeschlossen

Details | Planung | Geplante Aktivitäten | Kommentare | Diskussion | Work Item Links | Dokumentation (0)

Details

- Bearbeiter**
EditorDomainSpecific AUM (AUM_Edi...)
- Grad der Vertraulichkeit**
Öffentlich | Intern | **Vertraulich** | Streng Vertraulich
- Von**
06.08.2025 00:00
Bis
06.08.2025 23:59

Organisationseinheit oder Primary Asset

Name	Asset-Typ	Beschreibun...
Standort Österreich	Unternehmensorganisation	

- Prüfgebiet & -felder**
IT- und Fachbereichsverantwortung in den GRC-Domänen
- Prüfgegenstände**
-Prozesse und Maßnahmen zur Sicherstellung der Verfügbarkeit, Steuerbarkeit und Schutzfähigkeit geschäftskritischer Prozesse.
-Umsetzung von Richtlinien und Standards aus ISMS, BCMS, DPM, IKS, ERM, CSM und AUM.
-Verzahnung der GRC-Domänen zur Stärkung organisationaler Resilienz.
- Prüfstandards**
-ISO/IEC 27001:2022 (ISMS)
-ISO 22301:2019 (BCMS)
-ISO/IEC 27701:2019 (DPM)
-COSO ERM
- Mitwirkende**
ApproverDomainSpecific ICS (ICS_ApproverDomainS...
Executive ICS (ICS_Executive)
ApproverDomainSpecific ISM (ISM_ApproverDomain...
Executive ISM (ISM_Executive)
- Weitere Audit Mitwirkende**
Externe Fachexperten für Business Continuity, Datenschutz und Informationssicherheit
- Grund des Audits**
Reguläres Audit

- 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 mitwirkende 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.

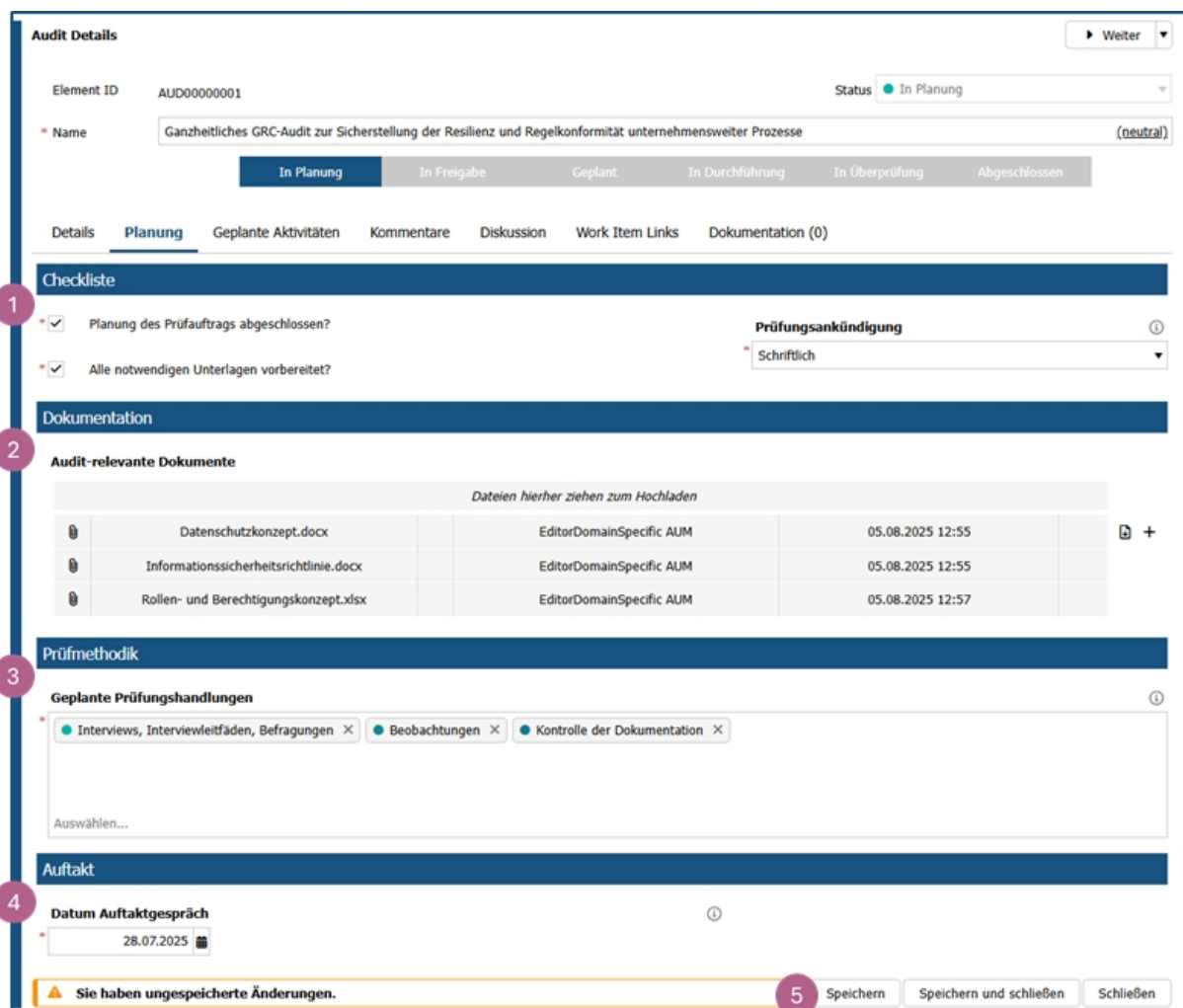
- 12 **Audit Beschreibung:** Schlussendlich muss der Bearbeiter das Audit in Worten beschreiben. Dabei können noch wichtige Informationen hinterlegt werden die zu keiner Angabe zuvor passend gewesen wäre.
- 13 **Audit Nicht-Ziele:** Neben dem Scope kann der Bearbeiter auch dezidiert festlegen was nicht 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.

The screenshot shows the 'Kontext' (Context) form in the GBTEC system. The form is divided into several sections, each with a numbered callout:

- 9 Audit Typ:** A dropdown menu with 'INT - Intern' selected.
- 10 Audit Kategorie:** A dropdown menu with 'Prozessaudit' selected.
- 11 Audit Ausmaß:** A dropdown menu with 'Vollprüfung' selected.
- 12 Audit Beschreibung:** A text area containing the description: 'Dieses Audit überprüft domänenübergreifend, ob die GRC-Komponenten des Unternehmens (insbesondere ISMS, BCMS, Datenschutz, IKS, ERM und AUM) wirksam ineinandergreifen, um die Verfügbarkeit, Steuerbarkeit und Schutz geschäftskritischer Prozesse zu gewährleisten – auch unter Stör- oder Krisenbedingungen. Geprüft werden Policy-Umsetzungen, organisatorische Resilienzmechanismen, technische Schutzmaßnahmen, Richtlinienkonformität sowie das Zusammenwirken von Risiko-'. There is a small icon in the top right corner of the text area.
- 13 Audit Nicht-Ziele:** A text area containing the text: 'Dieses Audit überprüft keine operativen Einzelrisiken, sondern fokussiert auf die Domänen-übergreifende GRC-Verzahnung zur Sicherstellung kritischer Prozessverfügbarkeit.' There is a small icon in the top right corner of the text area.
- 14 Speichern:** A button labeled 'Speichern' (Save) is highlighted. To its left is a warning icon and the text 'Sie haben ungespeicherte Änderungen.' (You have unsaved changes). To the right of the 'Speichern' button are two other buttons: 'Speichern und schließen' (Save and close) and 'Schließen' (Close).

Schritt 4: Planung hinterlegen



Audit Details Weiter

Element ID: AUD00000001 Status: In Planung

* Name: Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse (neutral)

Planung | In Planung | In Freigabe | Geplant | In Durchführung | In Überprüfung | Abgeschlossen

Details | **Planung** | Geplante Aktivitäten | Kommentare | Diskussion | Work Item Links | Dokumentation (0)

1 Checkliste

* ☒ Planung des Prüfauftrags abgeschlossen? Prüfungsankündigung

* ☒ Alle notwendigen Unterlagen vorbereitet? Schriftlich

2 Dokumentation

Audit-relevante Dokumente

Dateien hierher ziehen zum Hochladen

Datenschutzkonzept.docx	EditorDomainSpecific AUM	05.08.2025 12:55
Informationssicherheitsrichtlinie.docx	EditorDomainSpecific AUM	05.08.2025 12:55
Rollen- und Berechtigungskonzept.xlsx	EditorDomainSpecific AUM	05.08.2025 12:57

3 Prüfmethodik

Geplante Prüfungshandlungen

* Interviews, Interviewleitfäden, Befragungen × Beobachtungen × Kontrolle der Dokumentation ×

Auswählen...

4 Auftakt

Datum Auftaktgespräch

* 28.07.2025

5 Sie haben ungespeicherte Änderungen. Speichern Speichern und schließen Schließen

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 relevante Dokumente hinterlegen, die im Rahmen des Audits herangezogen werden sollen.

Dabei kann es sich um interne 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 *Auditaktivitäten* 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.

1.20.2 Auditaktivität definieren & planen

Nach der Erstellung eines *Audits* können passende *Auditaktivitäten* geplant und im Rahmen des *Audits* durchgeführt werden.

Schritt 1: Auditaktivität erstellen

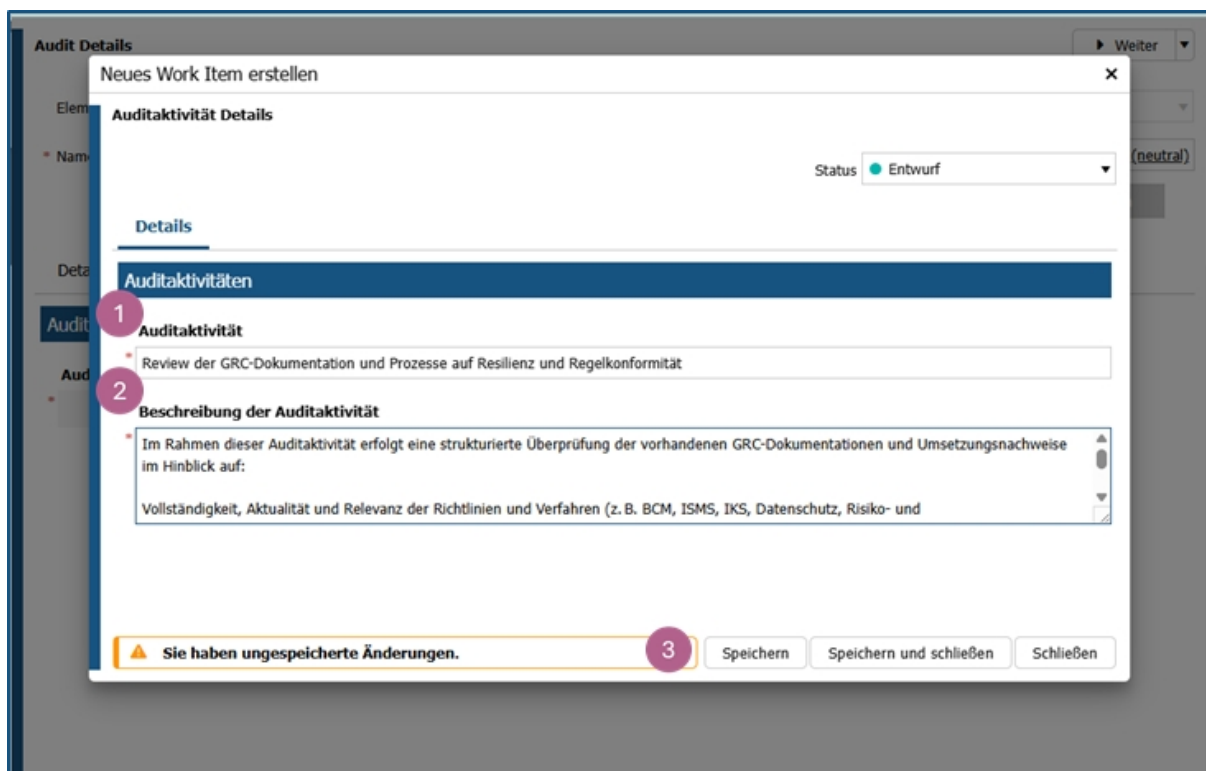
Die *Auditaktivität* kann nur mittels Erstellung aus dem Work Item *Audit* durch den verantwortlichen Bearbeiter erfolgen.

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.

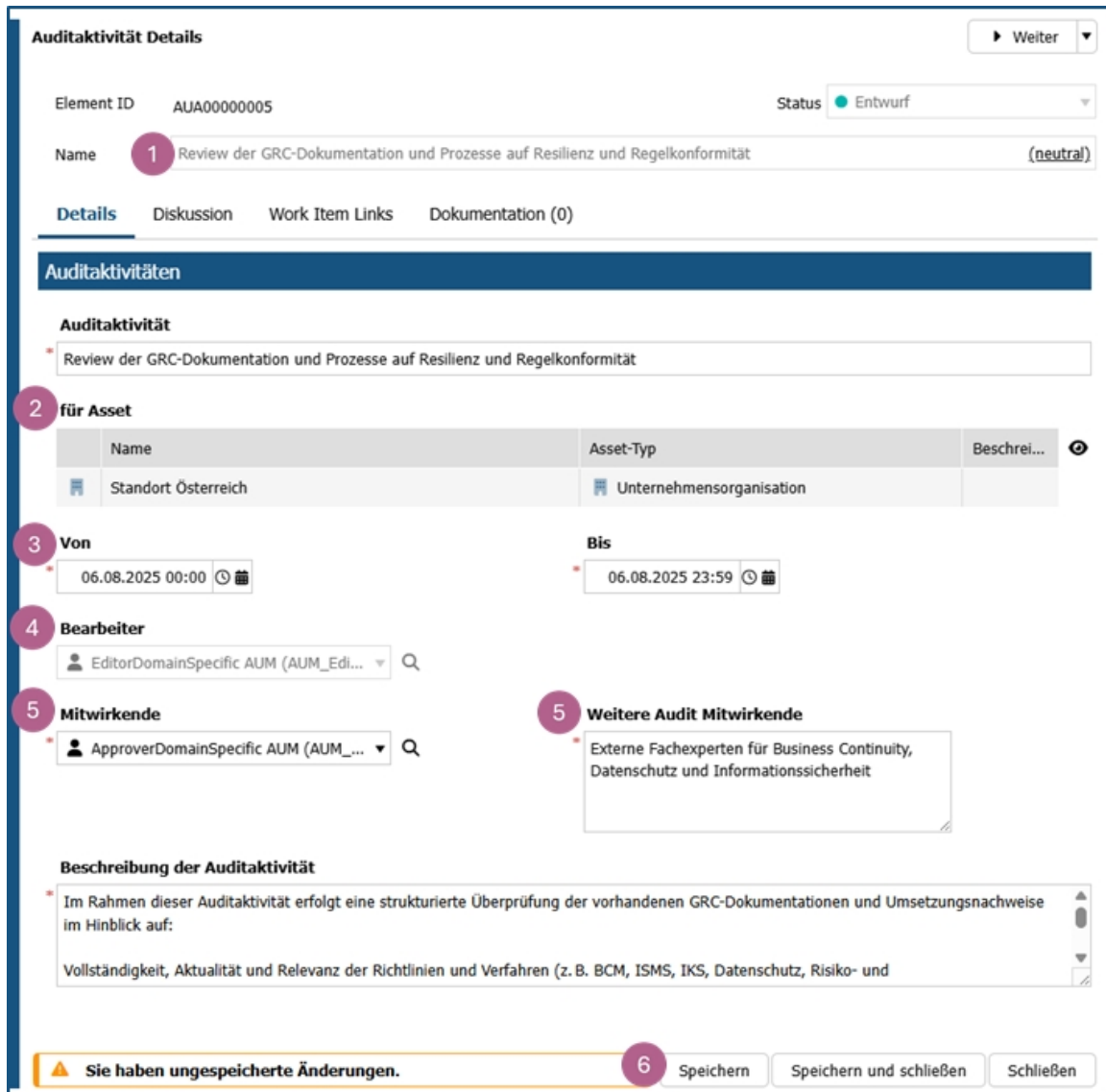
2 Beschreibung der Auditaktivität: Es kann vom Bearbeiter eine genaue Beschreibung angegeben werden, was während der *Auditaktivität* zu tun ist.

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



Auditaktivität Details Weiter

Element ID: AUA00000005 Status: Entwurf

Name: 1 Review der GRC-Dokumentation und Prozesse auf Resilienz und Regelkonformität (neutral)

Details Diskussion Work Item Links Dokumentation (0)

Auditaktivitäten

Auditaktivität

* Review der GRC-Dokumentation und Prozesse auf Resilienz und Regelkonformität

2 **für Asset**

Name	Asset-Typ	Beschrei...
Standort Österreich	Unternehmensorganisation	

3 **Von** 06.08.2025 00:00 **Bis** 06.08.2025 23:59

4 **Bearbeiter** EditorDomainSpecific AUM (AUM_Edi...

5 **Mitwirkende** ApproverDomainSpecific AUM (AUM_...

5 **Weitere Audit Mitwirkende** Externe Fachexperten für Business Continuity, Datenschutz und Informationssicherheit

Beschreibung der Auditaktivität

* Im Rahmen dieser Auditaktivität erfolgt eine strukturierte Überprüfung der vorhandenen GRC-Dokumentationen und Umsetzungsnachweise im Hinblick auf:

Vollständigkeit, Aktualität und Relevanz der Richtlinien und Verfahren (z. B. BCM, ISMS, IKS, Datenschutz, Risiko- und

Sie haben ungespeicherte Änderungen. 6 Speichern Speichern und schließen Schließen

- 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.

1.20.3 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 *Auditaktivitäten* 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.

1.20.4 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.

Auditaktivität Details

Element ID: AUA00000005 Status: Geplant

Name: Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse: Revie... (neutral)

Details Diskussion Work Item Links Dokumentation (0)

Auditaktivitäten

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

Abgeschlossen

Element ID: AUA00000005
Status: ● In Durchführung

Name: Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse: Revie... (neutral)

Details
Prüfungsfeststellung
Diskussion
Work Item Links
Dokumentation (0)

1 Prüfungsfeststellung

Soll-Zustand

Es ist sichergestellt, dass alle geschäftskritischen Prozesse durch geeignete organisatorische, technische und dokumentierte Maßnahmen auch im Störfall verfügbar, geschützt und steuerbar bleiben. Dazu zählen:

Eine vollständige und aktuelle Dokumentation der Prozesse

Ist-Zustand

Die Dokumentation der Wiederanlaufverfahren liegt nur für einige Prozesse in aktueller Form vor. Es fehlen Nachweise regelmäßiger Tests der Notfall- und Wiederherstellungspläne. Die Verantwortlichkeiten in Krisenlagen sind nicht durchgängig geregelt. Zugriffsschutzkonzepte sind nicht einheitlich umgesetzt und werden teilweise nicht dokumentiert überprüft.

2 Ergebnis

Ergebnisbewertung

Keine Abweichung

Beobachtung / Kommentar

Empfehlung / Feststellung

Kleinere
Nichtübereinstimmung

Größere
Nichtübereinstimmung /
Mangel

Beschreibung der Abweichung

Es bestehen kleinere Abweichungen zur dokumentierten Verfahrensanweisung zur Sicherstellung der Verfügbarkeit geschäftskritischer Prozesse. Insbesondere fehlen vollständige Nachweise zu den Testzyklen und zur Evaluierung der RTO-Vorgaben. Die Unklarheit bei Verantwortlichkeiten kann im Ernstfall zu Verzögerungen in der Krisenreaktion führen.

Handlungsempfehlung

Durchführung eines internen Trainings zur Krisenreaktion und Verfügbarkeitssicherung

Aufnahme der Maßnahmen in das übergreifende ISMS/BCM-Review

4 Finding

Finding

Element ID	Name	Verantwortlich	Status	Datum der Mel...	zu behandeln bis
FIN00000017	Unvollständige Umset...	EditorDomainSpecific...	●	05.08.2025	

⚠ Sie haben ungespeicherte Änderungen.

5 Speichern

Speichern und schließen

Schließen

- 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 *Auditaktivität* in den Status "Abgeschlossen" geschaltet werden.

Zurück zu dem Schritt [Bearbeiter Audit - Audit starten & durchführen](#) Schritt 5.

1.20.5 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".

Findings				
	Name	Status	B...	
	Dokumentationslücke beim Notfalltestprotokoll 2025	● Erfassung		

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 eine 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 Dashboards verwendet werden kann.

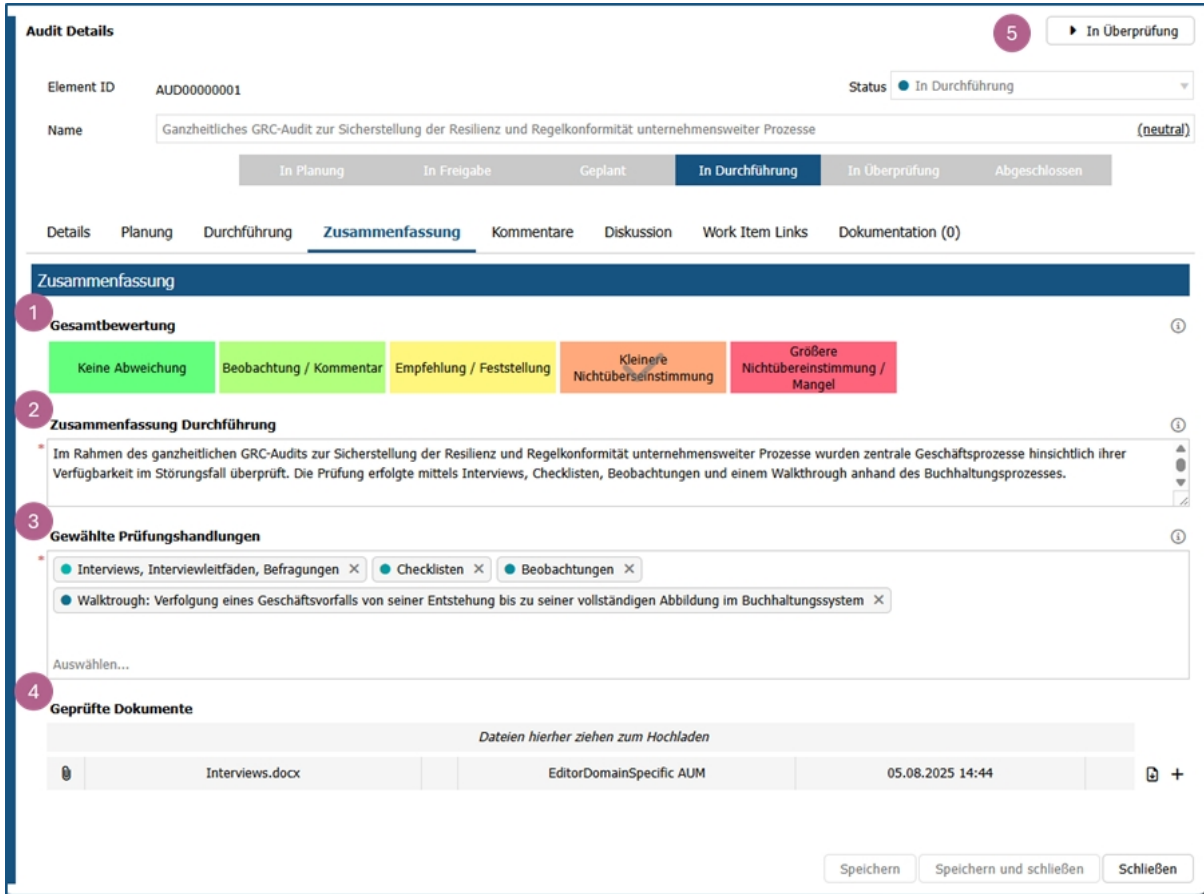
10 **Statuswechsel:** Der Ersteller kann abschließend in den Status "Behandlung" schalten. Mehr Informationen zu dem Statuswechsel in Finding sichten & behandeln.

Anschließend kann der Bearbeiter Management Review in die *Auditaktivität* zurückkehren und dort mit der Arbeit fortfahren. [Bearbeiter Audit - Auditaktivität starten & durchführen](#).

1.20.6 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.

1.21 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](#)

1.21.1 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.

Audit steht zur Genehmigung bereit

Werter User,

das Work Item "Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse" wurde bearbeitet und steht jetzt zur Genehmigung bereit.

Element ID:	AUD00000001
Status:	In Freigabe

Bitte überprüfen Sie die erfassten Daten und wechseln Sie anschließend den Status.
Mit freundlichen Grüßen

WORK ITEM ÖFFNEN

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail.

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.

Audit Details

Planung
Weiter

Element ID
AUD00000018

Status
Freigabe

Name
Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmensweiter Prozesse
(neutral)

Planung
Freigabe
Geplant
Durchführung
Überprüfung
Abgeschlossen

Details
Planung
Geplante Aktivitäten
Kommentare
Diskussion
Work Item Links
Dokumentation (0)

Kommentare

Kommentar

Tragen Sie hier Ihren Kommentar ein.

(0/1000)

Kommentar hinzufügen

Alle Kommentare

Speichern
Schließen

GBTEC Austria GmbH

239/252

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.

1.22 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:

- [Security-Risiko überprüfen & freigeben](#)
- [Management Review sichten & freigeben](#)
- [Bericht\(e\) öffnen & generieren](#)

1.22.1 Security-Risiko freigeben

Ein *Security-Risiko* wird vom Bearbeiter Risiko erstellt und bewertet, bevor es von unterschiedlichen Instanzen freigegeben wird. Wenn das *Security-Risiko* einen besonders hohen Risikowert ausgibt, kann der Manager darüber informiert werden, indem dieses spezifische *Security-Risiko* in den Status "Managementfreigabe" geschaltet wird.

Diese Option muss in der "Solution Configuration" freigeschalten werden.

Schritt 1: Navigation zu spezifischem Security-Risiko

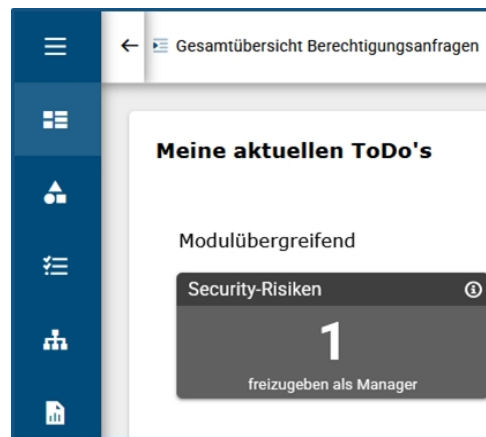
Der Manager hat zwei Möglichkeiten ein *Security-Risiko* zu öffnen.

1. Öffnen über Notifikation

Der Manager bekommt eine E-Mail zugesendet, sobald der Freigeber Risiko den Status des *Security-Risikos* zu "Managementfreigabe" wechselt. Der Link zu dem spezifischen *Security-Risiko* 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 *Security-Risiko* automatisch.

Schritt 2: Freigabe durchführen

Der Manager hat in dem erstellten und bewerteten *Security-Risiko* alle Leserechte, um auf Basis der eingegebenen Informationen zu entscheiden, ob das *Security-Risiko* 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 *Security-Risiko* 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.

Security-Risiko Details

◀ Bewertung

▶ Aktiv

Element ID

SRI00000044

Status

Managementfreigabe

Name

Ausfall eines geschäftskritischen Dienstleisters (neutral)

Bewertungszyklus

Monatlich

Nächste Bewertung

24.10.2025

Entwurf

In Bewertung

In Freigabe

Managementfreigabe

Aktiv

Risikowert

0

40.00

55.00

56.00

100

◀ Kontext

Risikoanalyse

Bruttobewertung

Nettobewertung

Risikobehandlung

Kommentare

Diskussion

Work Item ▶

Kommentare

Kommentar

Tragen Sie hier Ihren Kommentar ein.

(0/1000)

Kommentar hinzufügen

Alle Kommentare

Speichern

Schließen

Sollten die Eingaben weitgehend akzeptabel sein kann der Manager direkt in den Status "Aktiv" schalten. Mit dem Statuswechsel ist das *Security-Risiko* als abgeschlossen im Risikoinventar aufgenommen.

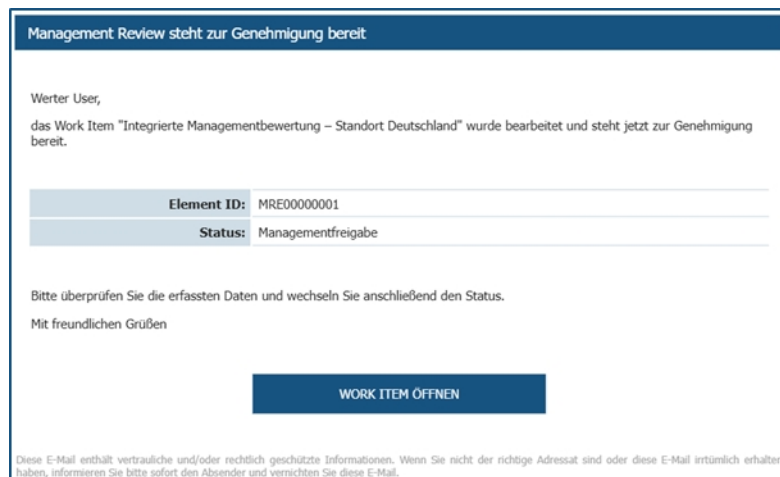
Nach dem Statusübergang kann das Fenster geschlossen werden.

1.22.2 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.

Schritt 4: Bericht generieren

Nachdem der *Management Review* in den Status "Abgeschlossen" geschaltet wurde können der Bearbeiter DS und der Manager einen Bericht generieren.

Der Bericht ist eine Zusammenfassung des gesamten *Management Reviews*.

Die Generierung des Berichts wird in der oberen rechten Fensterseite des Work Items durchgeführt. Bei der Ausgabedatei handelt es sich um ein PDF.

Management Review Details
Report

Element ID: MRE00000001
Status: Abgeschlossen

Name: Integrierte Managementbewertung – Standort Deutschland (neutral)

Planung Geplant Durchführung Überprüfung Managementfreigabe Abgeschlossen

Planung Ergebnisse Kommentare Diskussion Systeminformationen Work Item Links Dokumentation (0) Verlauf

Planung

Management Review
MRE00000001

Name
Integrierte Managementbewertung – Standort Deutschland

Status
Abgeschlossen

Planung

Bearbeiter
EditorDomainSpecific

Datum Management Review
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

1.23 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](#)

1.23.1 Interne Anfrage beantworten & bearbeiten

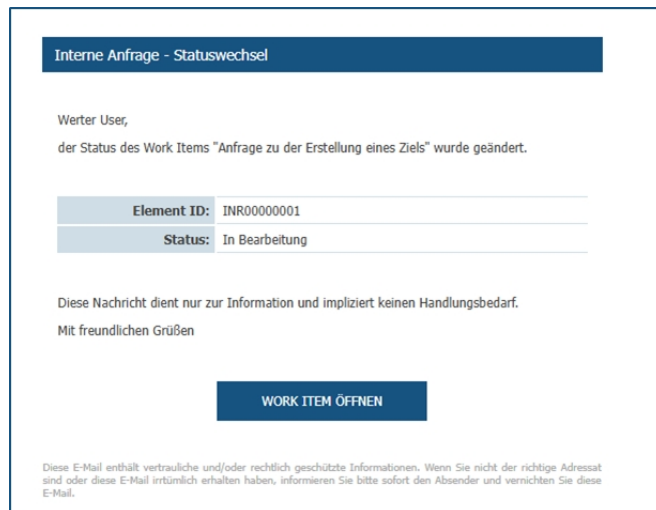
Nachdem ein Standard Benutzer eine *Interne Anfrage* gestellt hat muss ein Benutzer - der ein Mitglied der Gruppe "Internal Request Receiver" ist - diese beantworten.

Schritt 1: Navigation zur Internen Anfrage

Der Empfänger hat zwei Möglichkeiten eine *Internen Anfrage* zu öffnen.

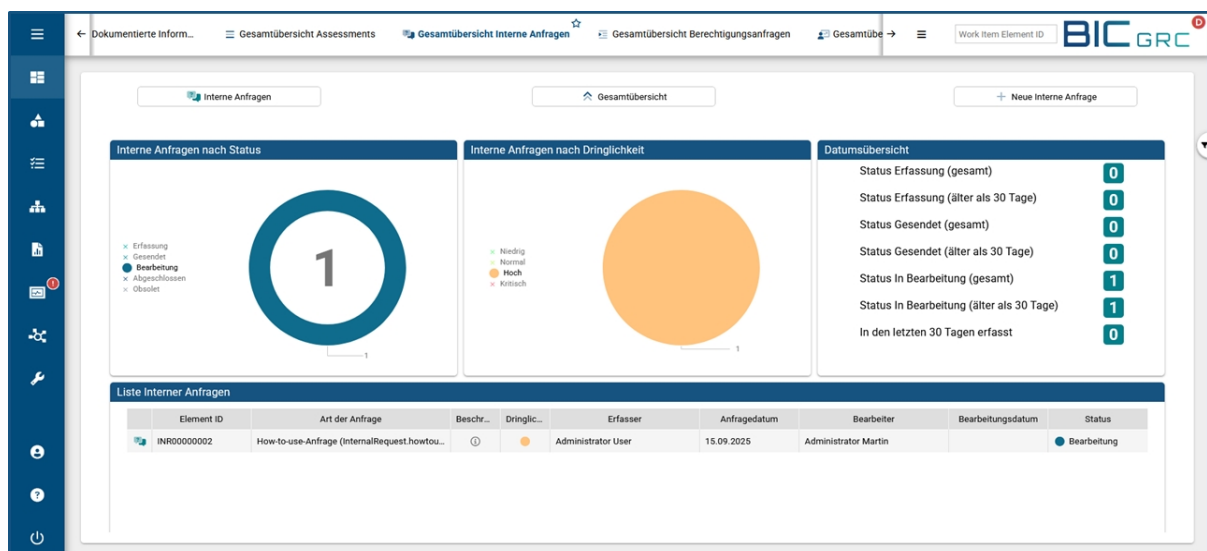
1. Öffnen über Notifikation

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.

Interne Anfrage Details

In Bearbeitung

Element ID
INR00000001
Status
Gesendet

* Name
Anfrage zu der Erstellung eines Ziels
(neutral)

Anfrage
Diskussion
Systeminformationen
Work Item Links
Dokumentation (0)
Verlauf

Interne Anfrage

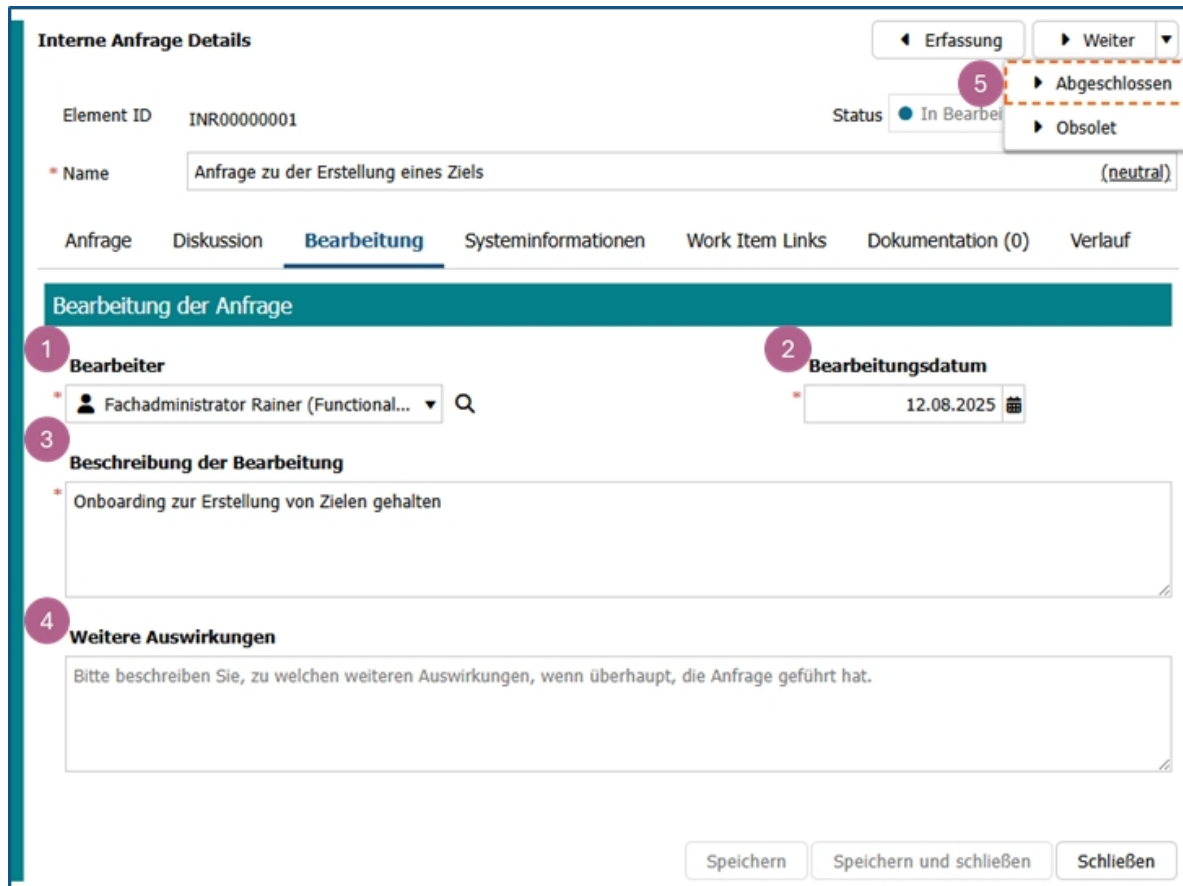
Erfasser
Standard GEN (StandardUser)
Anfragedatum
08.07.2025

Art der Anfrage

Name	Katalog	B...
How-to-use-Anfrage	Typen Interner A...	

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.

1.23.2 Berechtigungsanfrage beantworten & bearbeiten

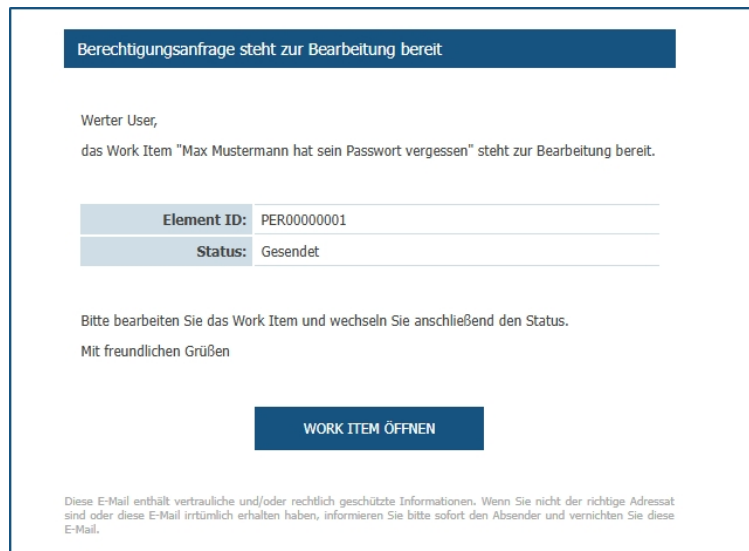
Nachdem ein Standard Benutzer eine *Berechtigungsanfrage* gestellt hat muss ein Benutzer - der ein Mitglied der Gruppe "Permission Request Receiver" ist - diese beantworten.

Schritt 1: Navigation zur Berechtigungsanfrage

Der Empfänger hat zwei Möglichkeiten eine *Berechtigungsanfrage* zu öffnen.

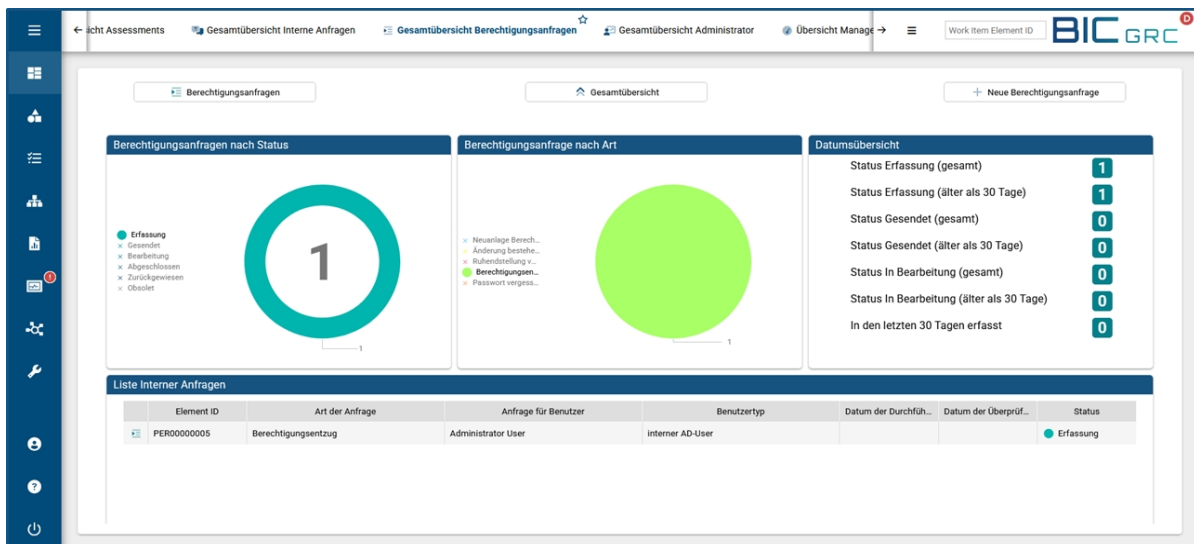
1. Öffnen über Notifikation

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.



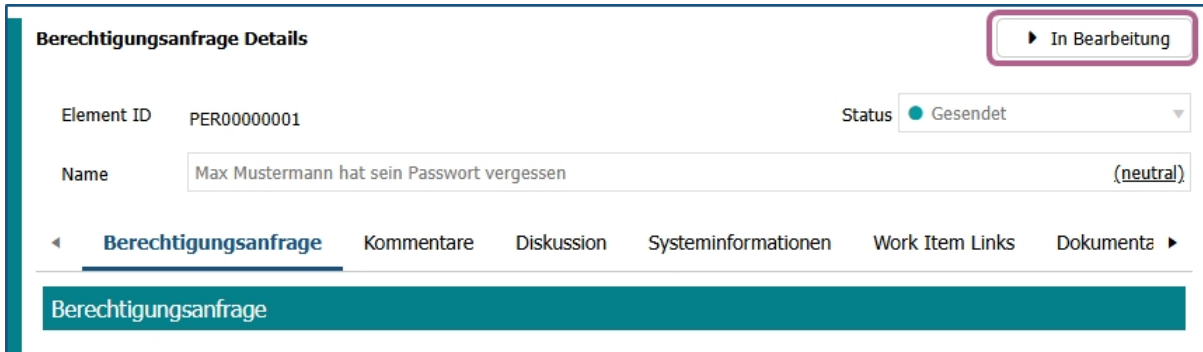
Bei Klick auf den Notifikationslink oder ein Listenelement in BIC GRC öffnet sich automatisch ein neues Fenster für die *Berechtigungsanfrage*.

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.



Berechtigungsanfrage Details ▶ In Bearbeitung

Element ID: PER00000001 Status: ● Gesendet ▼

Name: Max Mustermann hat sein Passwort vergessen (neutral)

◀ **Berechtigungsanfrage** Kommentare Diskussion Systeminformationen Work Item Links Dokumenta ▶

Berechtigungsanfrage

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

Berechtigungsanfrage Details 6

Element ID: PER00000001 Status: In Bearbeitung

* Name: Max Mustermann hat sein Passwort vergessen (neutral)

◀ Berechtigungsanfrage **Bearbeitung** Kommentare Diskussion Systeminformationen Work Item Links ▶

Bearbeitung der Anfrage

1 ☒ Eine spezielle Freigabe ist notwendig

Freigeber *

Verhältnis zum User *

2 **Geplante Überprüfung der Berechtigungen** *

3 **Anmerkungen zur Freigabe**

4 ☒ Ich bestätige hiermit die Legitimität der Anfrage.

5 **Datum der Durchführung** *

- 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

This document contains trademarks and information protected by the corresponding copyright laws and by the license agreements concluded with GBTEC Austria GmbH. The user is entitled to download information, to enter and store said information in local databases and to forward it in electronic format. The information may not be changed in any form or by any means, electronic or mechanical, without the express written permission of GBTEC Austria GmbH. Any names of companies and products of third parties mentioned in this document may be registered trademarks of the corresponding rights holder. Images and logos of third parties are purely for illustration purposes and indicate compatibility between the products of GBTEC Austria GmbH and the devices or applications of the corresponding third party. All copyright and trademarks of such images and logos are the property of the corresponding third party. No liability is assumed for the completeness of the information contained in this document. This document is for information purposes only and is subject to change without prior notification. GBTEC Austria GmbH MAKES NO EXPRESS GUARANTEES OR ANY GUARANTEES IMPLYING LEGAL INTENT WITHIN THIS DOCUMENT. The content of this document is not intended to represent any recommendation on the part of GBTEC Austria GmbH.

Any names and/or data shown in screenshots are fictitious. Changes and errors excepted.

Copyright © by GBTEC Austria GmbH, 2026

All rights reserved.