

BIC Data Protection - User Manual

BIC Integrated GRC 2026 Summer

Dokument Version: June 2026



Table of Contents

1 Who is this user manual intended for?	10
1.1 Spelling	10
1.2 Overview of symbols	11
1.2.1 General	11
1.2.2 Dashboard	11
1.2.3 Work Item	11
2 BIC Data Protection - Work Item Typen	12
2.1 Standard User	12
2.1.1 Report & create Data Breach	12
Step 1: Create Data Breach	12
Step 2: Enter details	14
Step 3: Add details	15
2.1.2 Define & create an Internal Request	16
Step 1: Create an Internal Request	16
Step 2: Enter details	18
Step 3: Complete Internal Request	19
Optional step 4: Start Discussion	20
2.1.3 Define & create a Permission Request	20
Step 1: Create a Permission Request	20
Step 2: Enter details	22
Step 3: Complete the Permission Request	27
2.2 Asset Owner	28
2.3 Asset Manager	28
2.3.1 Prepare & maintain Assets	28
Step 1: Navigate to Assets	28
Step 2: Create Assets	28
Step 3: Tag Assets	31
Step 4: Maintain Asset Properties	32
2.3.2 Prepare & assign GRC Framework Items for Assessments	32
Step 1: Assign GRC Framework Items to Asset Types	32
Step 2: Assign GRC Framework Items to the Asset	33
2.4 Assessor	33
2.4.1 ISO 27701 - Create & start Assessment	34
Step 1: Navigate to Assessment	34
Step 2: Enter Assessment details	35
Step 3: Check GRC Framework Items Assignments	35
Step 4: Start Assessment	36
2.4.2 ISO 27701 - Perform & evaluate evaluation	36

Step 1: Overview of the Assessment screen	36
Step 2: Enter assessment details	37
2.4.3 ISO 27701 - Complete & evaluate Assessment	39
Step 1: Complete Assessment	39
Step 2: Evaluate results	39
Step 3: Further procedure	40
2.5 Editor Risk	40
2.5.1 Identify & create Threats	41
Step 1: Create threat	41
Step 2: Enter details	42
2.5.2 Identify & create Vulnerability	43
Step 1: Create Vulnerability	43
Step 2: Enter details	44
2.5.3 Derive & create Risk Scenario	45
Step 1: Create Risk Scenario	45
Step 2: Enter details	46
Step 3: Define basics	46
Step 4: Further procedure	49
2.5.4 Define & create Objectives	50
Step 1: Create objective	50
Step 2: Define the Objective	52
Step 3: Enter Additional Information	54
Step 4: Perform update execution	55
2.5.5 Define & create Milestones	55
Step 1: Create a Milestone	55
Step 2: Define the Milestone	56
2.5.6 Identify & Create Security Risk	57
Step 1: Create Security Risk	57
Step 2: Enter details	58
2.5.7 Add & analyze Security Risk	60
Optional step 1: Navigating to a specific Security Risk after external creation	60
Optional step 2: Reviewing the creator's entries	61
Step 3: Finalize assignment	61
Step 4: Complete the entries	62
Optional - Step 5: Perform Risk Analysis	63
2.5.8 Assessing & evaluating Security Risks	65
Step 1: Perform evaluation	65
Step 2a: Perform qualitative Gross Evaluation	65
Step 3a: Perform qualitative Net Evaluation	67
Step 4a: Perform a qualitative Current Evaluation	69

Step 2b: Perform quantitative Gross Evaluation	69
Step 3b: Perform quantitative Net Evaluation	71
Schritt 4b: Perform Quantitative Target Evaluation	74
2.5.9 Derive & create Measure Evaluation	75
Step 1: Create a Measure Evaluation	75
Step 2: Assign measure	76
Step 3: Document the effect of the measure	76
Step 4: Next steps	76
2.5.10 Identify & create Measure	77
Step 1: Create a Measure from a Measure Evaluation	77
Step 2: Enter details	78
2.5.11 Derive & create Control	79
Step 1: Create Control from Security Risk	79
Step 2: Enter details	80
2.5.12 Implementation & review of Objectives	81
Step 1: Navigate to the Objective	81
Step 2: Evaluate Milestones	81
Step 3: Perform review	82
2.6 Approver Risk	83
2.6.1 Review & approve Security Risk	83
Step 1: Navigate to specific Security Risk	83
Step 2: Perform review	84
Step 3: Perform status transition execution	85
2.7 Editor Measure	86
2.7.1 Define & create Measures	86
Step 1: Create Measure	86
Step 2: Enter details	88
2.7.2 Add & edit a Measure	89
Optional step 1: Navigating to a specific Measure after external creation	89
Optional step 2: Reviewing the creator's entries	90
Step 3: Add entries	90
2.7.3 Set up & plan Measure	91
Step 1: Perform planning	91
2.7.4 Manage & implement a Measure	92
Step 1: Navigate to a specific Measure	92
Step 2: Document implementation	94
2.7.5 Optional: Review & improve Measure	95
Step 1: Navigate to the Measure	95
Step 2: Perform review	96
2.7.6 Identify & create Finding	98

Step 1: Create Finding from Measure	98
Step 2: Documenting Finding	99
2.7.7 Manage & handle Findings	100
Step 1: Navigating to a specific Finding after external creation	100
Step 2: Handle Finding	101
2.8 Approver Measure	102
2.8.1 Review & approve Measure	102
Step 1: Navigating to the Measure	102
Step 2: Perform approval	103
2.9 Editor Control	104
2.9.1 Derive & create Control	105
Step 1: Create Control	105
Step 2: Enter details	106
Step 3: Finalize assignment	107
2.9.2 Edit & review Control	108
Optional step 1: Navigating to a specific Control after external creation	108
Optional step 2: Reviewing the Creator's entries	108
Step 3: Add to Control	109
Step 4: Store Control Executors & Testers	111
2.9.3 Initiating & creating Control Testing	114
Step 1: Navigate to Control	114
Step 2: Create Control Testing	114
Step 3: Enter details	115
2.9.4 Manage & handle Findings	116
Step 1: Navigating to a specific Finding after external creation	116
Step 2: Handle Finding	117
2.9.5 Review & approve Control Testing	118
Step 1: Navigate to Control Testing	118
Step 2: Perform review	119
Step 3: Perform status transition execution	119
2.10 Approver Control	119
2.10.1 Review & approve Control	119
Step 1: Navigate to Control	119
Step 2: Perform review	120
Step 3: Execution of the status change	121
2.11 Control Executer	121
2.11.1 Create & perform Control Execution	122
Step 1: Navigate to the Control	122
Step 2: Reviewing the entries made by the Editor Control	122
Step 3: Create Control Execution	123

2.12 Tester	124
2.12.1 Perform & evaluate Control Testing	124
Step 1: Navigate to Control	124
Step 2: Enter details	125
2.12.2 Identify & create Finding	127
Step 1: Create Finding from Control Testing	127
Step 2: Documenting Finding	128
2.13 Editor Domain Specific	129
2.13.1 Define & Create Category of Personal Data	130
Step 1: Create Category of Personal Data	130
Step 2: Enter details	131
2.13.2 Determine & create Processing Activity	132
Step 1: Create Processing Activity	132
Step 2: Define details	133
Step 3: Enter Additional Information	134
Step 4: Document the Legitimate Interest Assessment	138
Step 5: Evaluation of risks	139
Step 6: Check mandatory privacy impact assessment	141
2.13.3 Define & create Data Subject Data	143
Step 1: Create Data Subject Data	143
Step 2: Categorize Data Subject Data	144
Step 3: Enter further details	145
Step 4: Enter storage information	146
2.13.4 Define & create Data Processing Agreement	148
Step 1: Create the Data Processing Agreement	148
Step 2: Describe the Data Processing Agreement	149
Step 3: Supplement the Data Processing Agreement	150
Step 4: Go through the checklist	151
2.13.5 Determine & create Transfer Impact Assessment	152
Step 1: Create Transfer Impact Assessment	152
Step 2: Describe the Transfer Impact Assessment	153
Step 3: Finalize the Transfer Impact Assessment	155
2.13.6 Determine & create Privacy Impact Assessment	156
Step 1: Create a Privacy Impact Assessment	156
Step 2: Describe the Privacy Impact Assessment	157
Step 3: Finalize the Privacy Impact Assessment	158
Step 4: Perform legal evaluation	159
Step 5: Perform Risk Analysis	160
2.13.7 Define & create Privacy Request	162
Step 1: Create Privacy Request	162

Step 2: Enter details	163
Step 3: Add further details	164
2.13.8 Review & edit Privacy Requests	165
Optional step 1: Navigate to specific Privacy Request after external creation	166
Optional step 2: Reviewing the creator's entries	166
Step 3: Complete the Privacy Request	167
2.13.9 Define & create Management Review	168
Step 1: Create Management Review	168
Step 2: Define details	169
Step 3: Enter Additional Information	171
Step 4: Document the Management Review	172
2.13.10 Perform & review Management Review	173
Step 1: Navigate to Management Review	173
Step 2: Perform Management Review	173
Step 3: Perform status transition	174
2.13.11 Identify & create Finding	175
Step 1: Create Finding from Management Review	175
Step 2: Document the Finding	176
2.14 Approver "Domain Specific"	177
2.14.1 Review & approve Processing Activity	178
Step 1: Navigate to Processing Activity	178
Step 2: Review Processing Activity	179
Step 3: Perform status transition execution	179
Step 4: Generate report	179
2.14.2 Review & approve Data Processing Agreement	179
Step 1: Navigate to the Data Processing Agreement	179
Step 2: Review the Data Processing Agreement	180
Step 3: Perform status transition execution	181
Step 4: Further procedure	181
2.14.3 Viewing & editing Data Breaches	181
Step 1: Navigate to specific Data Breach	181
Step 2: Review Data Breach	182
Step 3: Provide further details	182
Step 4: Perform evaluation	186
Step 5: Document the response	187
2.15 Document Owner	189
2.15.1 Defining & creating Documented Information	189
Step 1: Create Documented Information	189
Step 2: Enter details	191
Step 3: Complete entries	192

2.15.2 Evaluating & reviewing Documented Information	195
Step 1: Navigate to Documented Information	195
Step 2: Review Documented Information	195
Step 3: Leave a comment	195
2.16 Document Manager	196
2.16.1 Review & release Documented Information	196
Step 1: Navigating to the Documented Information	196
Step 2: Review Documented Information	197
Step 3: Leave a note	197
2.17 Editor Audit	198
2.17.1 Define & Create Audit	199
Step 1: Create Audit	199
Step 2: Enter details	200
Step 3: Add details	201
Step 4: Save Planning	204
Step 5: Plan Audit Activities	205
Step 6: Change status	205
2.17.2 Define & plan Audit Activity	205
Step 1: Create Audit Activity	205
Step 2: Define Audit Activity	206
Step 3: Further procedure	207
2.17.3 Start & Execution of Audit	208
Step 1: Navigate to Audit	208
Step 2: Perform Audit Activities	209
Step 3: Complete Audit Activities	209
2.17.4 Start & Execution of Audit Activity	209
Step 1: Open Audit Activity	209
Step 2: Perform Audit Activity	211
Step 3: Complete Audit Activity	212
2.17.5 Identify & create Finding	212
Step 1: Create Finding from Audit Activity	212
Step 2: Documenting Finding	213
2.17.6 Evaluate & complete Audit	214
Step 1: Evaluate Audit	215
2.18 madcApprover Audit	216
2.18.1 Review & approve Audit	216
Step 1: Navigate to Audit	216
Step 2: Review Audit	217
Step 3: Perform status transition execution	217
2.19 Executive	217

2.19.1 Review & approve Security Risk	218
Step 1: Navigate to specific Security Risk	218
Step 2: Perform Approval	218
2.19.2 Review & approve Management Review	219
Step 1: Navigate to the specific Management Review	219
Step 2: Perform review	219
Step 3: Perform status transition execution	220
Step 4: Generate report	220
2.20 Special User Profiles	220
2.20.1 Respond to & process Internal Requests	221
Step 1: Navigating to the Internal Request	221
Step 2: View Internal Request	221
Step 3: Edit Internal Request	222
2.20.2 Respond to & edit Permission Requests	223
Step 1: Navigate to the Permission Request	223
Step 2: View Permission Request	223
Step 3: Edit Permission Request	224

1 Who is this user manual intended for?

This user manual is intended for users of BIC Integrated GRC. It should help you find your way around BIC GRC and should help you learn about and perform specific tasks in the tool.

1.1 Spelling

The following notation is used in this manual:

- Terms in double quotation marks: All names such as dialog titles, tab titles, menu options, field names, etc. are marked with double quotation marks. Example: Click on "Create".
- Terms in single quotation marks: To identify special terms.
- Command paths: The instruction 'Select **Architecture >> Dashboards >> Tiles**' means that you must select the "Architecture" option in the sidebar, then the "Dashboards" option, and then "Tiles".
- Bold type: Particularly important information is highlighted in **bold**.
- References: References to other chapters or other documents are displayed as hyperlinks.
- Backgrounds: Certain text content in BIC GRC has a background color with the following meanings:

General information: Information users should take note of when working in BIC GRC.

Important information: Information that is crucial to users working in BIG GRC.

Additional information: Information interesting to know for users when working in BIC GRC.

Technical information and examples

Warning: Explanations for error messages or specific behavior in BIG GRC.

1.2 Overview of symbols

BIC GRC contains a large number of Icons that users will encounter while working in BIC Enterprise GRC. The following is an overview of all common and necessary Icons in BIC GRC.

The respective Icon name is displayed when you move the mouse pointer over the symbol.

1.2.1 General

	Edit		Display graph
	Filter		List Settings
	Search		Value Not Specified

1.2.2 Dashboard

	Scroll to the display area		Pin
	Show detailed list of all elements		Detach

1.2.3 Work Item

	Search for users		Informationen
	Create		Link
	Info		Successful Simulation
	Note		Error
	Link - Show attributes		Description
	Work Item Links - Expand		Additional options

2 BIC Data Protection - Work Item Typen

The following chapter provides the description of the different user profiles and their associated tasks within BIC GRC. The user profiles consist of groups and roles that have already been predefined by GBTEC within the framework of BIC Solutions.

Each user profile is briefly explained, followed by the associated tasks.

Please inform you yourself in advance at your Technical Administrator, which user profile is assigned to you.

2.1 Standard User

The "Standard User" profile is a general user profile that should be assigned to every user by default.

The Standard User can also be regarded as a basic profile.

The Standard User can perform the following tasks in BIC GRC:

- [Report & create a Data Breach](#)
- [Define & create an Internal Request](#)
- [Define & create a Permission Request](#)

2.1.1 Report & create Data Breach

If a *Data Breach* is detected in the Data Protection area, it can be created and reported by any User.

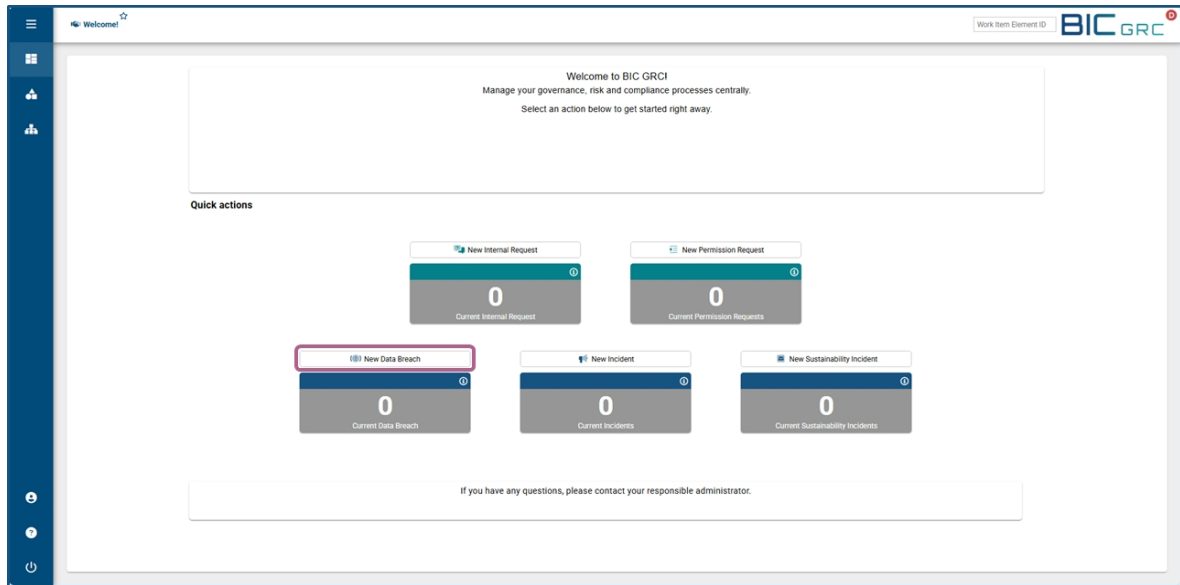
The creation of Work Items of the type *Data Breach* is also enabled for other active modules when the "Data Protection" module is active. This allows users from all modules to report *Data Breaches* as needed, including users from the "Data Protection" area.

Step 1: Create Data Breach

Standard Users can create *Data Breaches* in several places in BIC GRC.

1. Create via dashboard

The user navigates via the sidebar to **Dashboards >> Welcome >> "New Data Breach."**

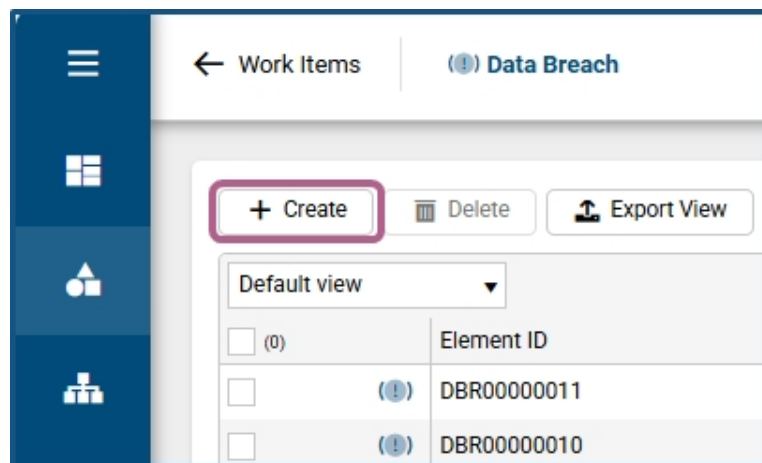


A new window will then open automatically.

2. Creation via Tile

The Editor navigates to **Work Items >> Data Breach >> "Create"** via the sidebar.

A new window will then open automatically.



Step 2: Enter details

Data Breach Details

Status: ● Registration

* Name 1 Unauthorized access to customer data in the CRM system (neutral)

Report

Notification Details

2 **Legal Entity**

Name	Asset Type	End-use...	
4wheels Automotive Production GmbH	Business Structure		

3 **Type of Data Breach**

Name	Catalog	E...	
Unauthorized access to personal data by employees for private purposes	Types of D...		

⚠ You have unsaved changes. 4 Save Close

1 **Name:** The first step should be to enter a short but meaningful name for the *Data Breach*. This "name" in combination with the "Element ID" makes the *Data Breach* unique.

2 **Legal Entity:** A "Legal Entity" must be assigned to the Data Breach. This "Legal Entity" is an Asset in BIC GRC.

Only one Business Unit with the tag "Company" may be assigned to the scope of application.

If the user does not see any "Assets", an Asset is yet to be assigned to the user in the "rol.StandardUser" role. Using the Work Item Permission Request, the user can request the appropriate authorization for the Asset. For more information, see [Standard User - Define & Create Permission Request](#).

3 **Type of Data Breach:** The creator must specify the "Type of Data Breach." A GRC framework is displayed for selection.

Authorized users can add company-specific "Types of Data Breaches" to the GRC Framework as needed.

4 **Save:** After entering the necessary information, the Data Breach can be saved for the first time.

During the save process, the creator is automatically entered as the "Creator."

Step 3: Add details

Data Breach Details

Element ID

DBR00000013

Status

Registration

Name

Unauthorized access to customer data in the CRM system

(neutral)

Registration

Reported

Progress

Completed

Report

Comments

Discussion

Work Item Links

Documentation (0)

Notification Details

Registrator

Standard GEN

Legal Entity

Name	Asset Type	End-user ...
4wheels Automotive Production GmbH	Business Structure	

Type of Data Breach

Name	Catalog	En...
Unauthorized access to personal data by employees for private purposes	Types of Dat...	

Description

Internal audits revealed that an employee had accessed personal customer data in the central CRM system without authorization. The access took place outside the scope of the authorizations intended for the activity and without any business purpose. The data affected was customer master data processed in the CRM system.

At the time of recording, there is still no complete information available on the scope, duration, and specific effects of the access.

Moment of Data Breach

15/12/2025

☐ Incident is still ongoing
 ☐ Recurrence of the incident is to be feared

Moment of Identification

16/01/2026

Identifier

Full Name

Max Mustermann

Postal Address

Musterstraße 80/0, X-0000 Musterhausen

E-Mail Address

Musterstraße 80/0, X-0000 Musterhausen

Delete

Report

Save

Close

- 1 Description:** The Creator must provide a description of exactly what happened in the Data Breach, which data or persons are affected, and, if applicable, what steps have already been taken.

It is also important for the subsequent user to know what type of breach has occurred, e.g., unencrypted E-Mail transmission, and what consequences the creator expects.

- 2 **Time of the incident:** In addition to the "Description", the date on which the *Data Breach* or Security Incident occurred must be entered in a separate attribute.

Below the date "Time of Security Incident" there is a separate checkbox that the Creator can click to indicate that the exact date is currently unavailable. If the checkbox is clicked, the date field becomes Read Only. If a date has been entered, the checkbox is no longer displayed.

- 3 **Time of discovery:** Time of discovery: The "Time of discovery" may differ from the "Time of Security Incident," so this date must be entered separately. In any case, the date of discovery must be set after the date of the Security Incident.

- 4 **Security Incident ongoing:** If the *Data Breach* or Security Incident is still ongoing, this can be indicated by clicking the checkbox.

- 5 **Repetition to be anticipated:** Furthermore, the Creator must indicate whether, in their opinion, it is an isolated case or whether the *Data Breach* could be repeated.

This information is relevant for downstream users so that they can take appropriate steps for the future.

- 6 **Full name:** Information about the person reporting the incident must be provided.

For example, this includes the "Full Name" with title and any other relevant information.

- 7 **Address:** An address must also be provided, including the street address and country.

- 8 **E-Mail-Address:** Finally, the reporter's E-Mail Address is required in order to finalize the *Data Breach*.

- 9 **Further action:** Two buttons are displayed to the Creator:

- Delete: If the Creator wishes to withdraw the Report, they can click the button to set the *Data Breach* to "Obsolete" Status.
- Report: If the report is current and they want to officially report it to the Data Protection Officer, they can select this button and the workflow will be started.

The approver DS (Data Protection Officer) is informed of the status change by email.

2.1.2 Define & create an Internal Request

Every user in BIC GRC has the option to submit an *Internal Request*.

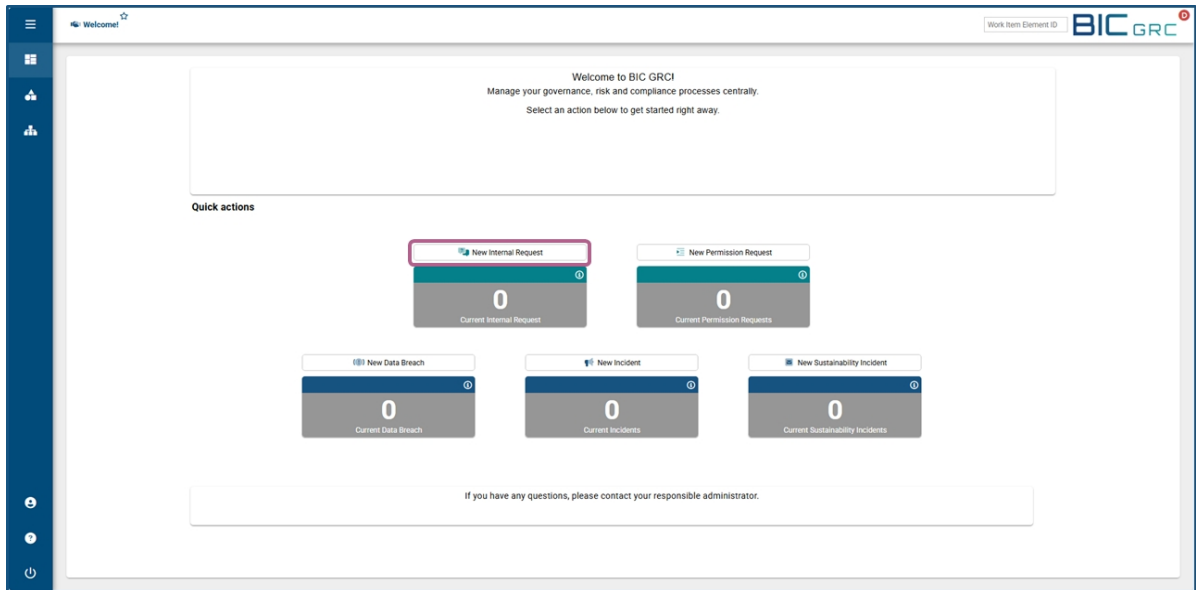
This request can be used to apply for new profiles or individual permissions. Adjustments to existing profiles can also be requested.

Step 1: Create an Internal Request

Standard Users can create *Internal Requests* in several places in BIC GRC.

1. Creation via dashboard

The user navigates to **Dashboards >> Welcome >> "New Internal Request"** via the sidebar.

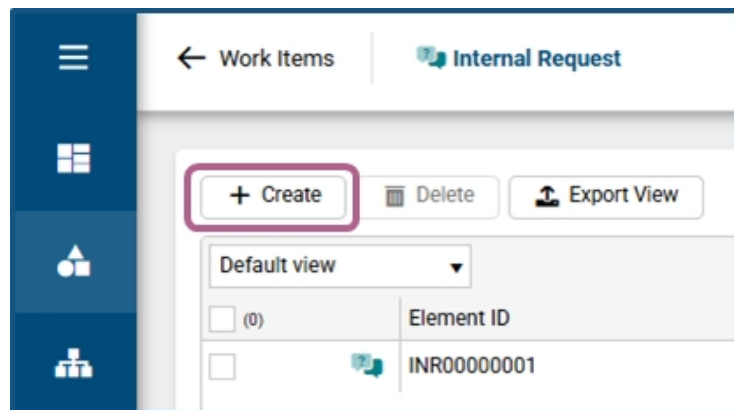


A new window will then open automatically.

2. Creation via Work Item List

The user navigates via the sidebar to **Work Items >> Internal Request >> "Create"**.

A new window will then open automatically.



Step 2: Enter details

Internal Request Details

Status: Registration

* Name 1 Request for the creation of a goal (neutral)

Request Discussion

Internal Request

2 **Type of Request**

Name	Catalog	E...
how-to-use request	Types of Interna...	

3 **Asset Link**

Name	Asset Type	End-us...
Location Germany	Business Structure	

4 **Description**

I need to define a goal for my location and don't know how to get started. I need someone to guide me through this, as I was sick on the first day of onboarding.

5 **Priority**

Low Normal High Critical

6 **Recipient**

Fachadministrator Rainer (Functional...)

7 You have unsaved changes. Save Save and Close Close

- 1 **Name:** The first step is to enter a short but meaningful name for the *Internal Request*.
- 2 **Type of Request:** The User must then specify the type of *Internal Request*. Behind the link is a GRC framework with predefined "Types of request" that can be linked using the icon

The GRC Framework "Internal Request Types" is maintained by your own management and can be expanded by them as needed.

- 3 **Asset Link:** A link to an "Asset" using the icon is required.

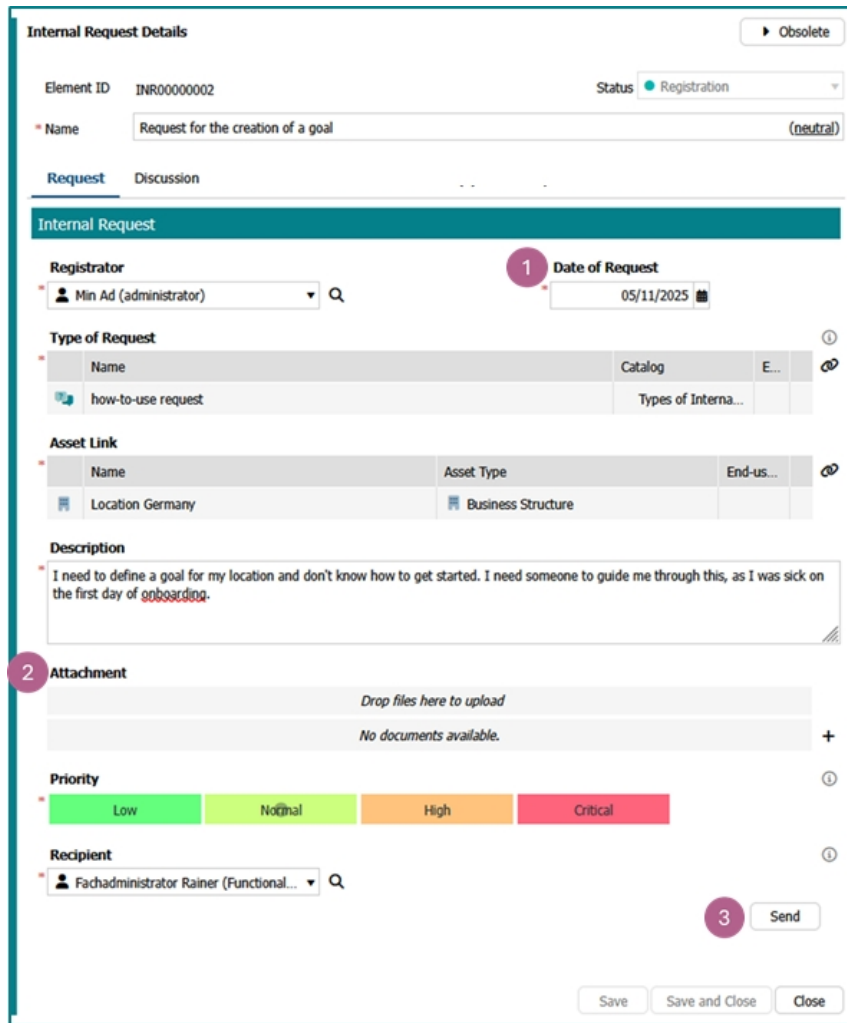
If the user does not see any Assets displayed, this indicates that an Asset has not yet been assigned to the user on the "rol.StandardUser" role. Using the *Permission Request* Work Item, the user can request the appropriate authorization for an Asset. For more information, see [Standard User - Define & Create Permission Request](#).

- 4 **Description:** The user can specify what their request is about. This can help the next user in the workflow to better classify the request.
- 5 **Priority:** The user can specify the "priority" with which the *Internal Request* should be answered using four predefined classifications.
- 6 **Recipient:** The user must select a "Recipient" who will respond to their *Internal Request*.

Only users who have a suitable group assignment to "grp.InternalRequestReceiver" are suggested as "Recipients."

7 Save: Once the information has been entered, the user can save it.

Step 3: Complete Internal Request



After saving for the first time, the Date of Request is automatically filled in **1**. Furthermore, if necessary, an attachment can be added voluntarily **2**.

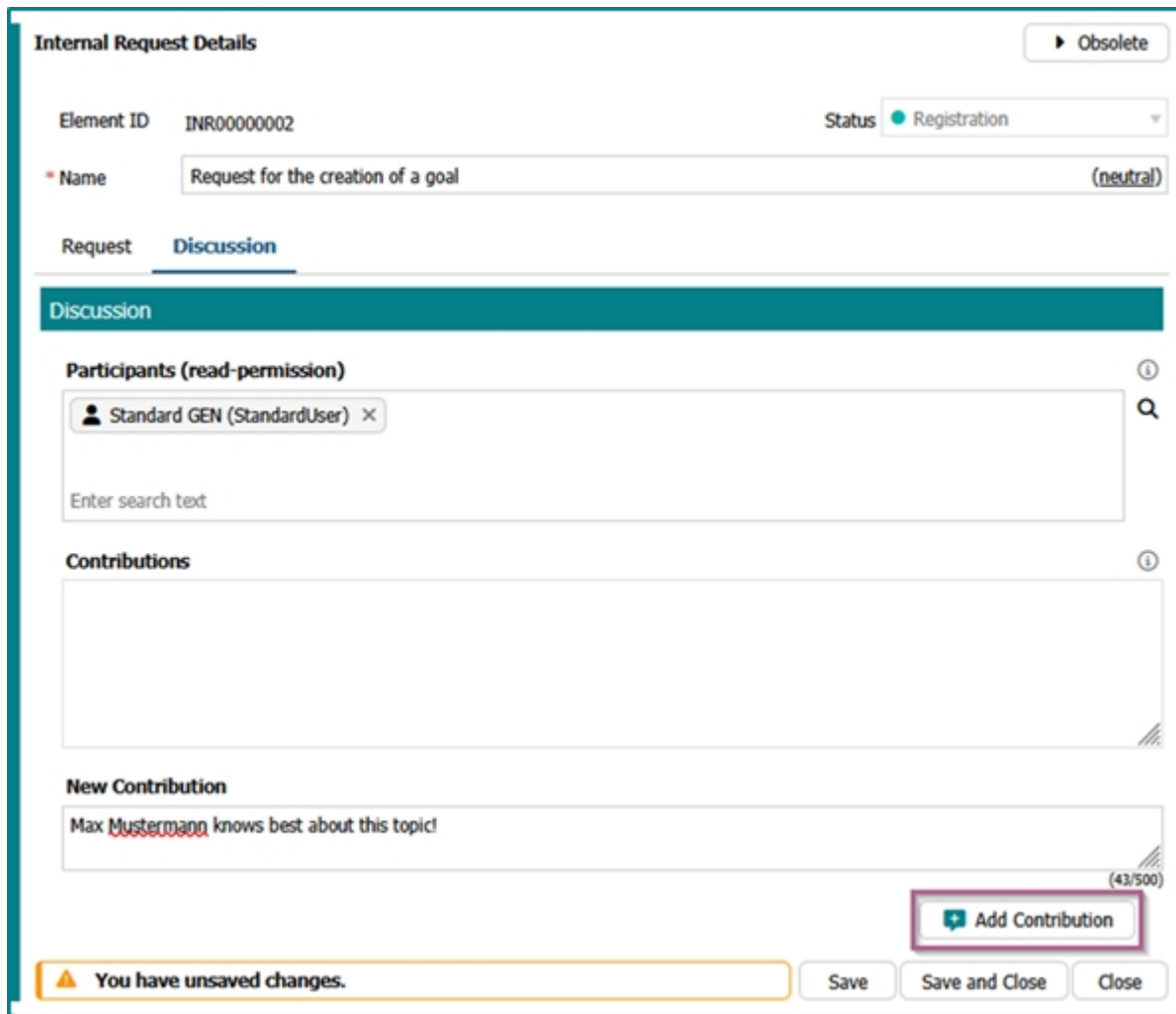
When all additions are complete, the status transition can be triggered by clicking the "Send" button **3**.

The next step is performed by the [Internal Request Recipient - Answer & edit Internal Request](#). The Internal Request Recipient reviews the request, adds to it if necessary, and decides whether to approve or reject it.

The user receives a notification as soon as the Recipient begins processing the *Internal Request*.

Optional step 4: Start Discussion

It is possible to start a discussion on the respective *Internal Request* at any time. This feature may be used to clarify any question regarding an Internal Request between participants.



The screenshot shows the 'Internal Request Details' form with the 'Discussion' tab selected. The form includes fields for 'Element ID' (INR00000002), 'Status' (Registration), and 'Name' (Request for the creation of a goal). Below these, there are tabs for 'Request' and 'Discussion'. The 'Discussion' section contains a 'Participants (read-permission)' list with 'Standard GEN (StandardUser)' and a search bar. There is also a 'Contributions' section with a text area for 'New Contribution' and an 'Add Contribution' button. At the bottom, there is a warning message 'You have unsaved changes.' and buttons for 'Save', 'Save and Close', and 'Close'.

2.1.3 Define & create a Permission Request

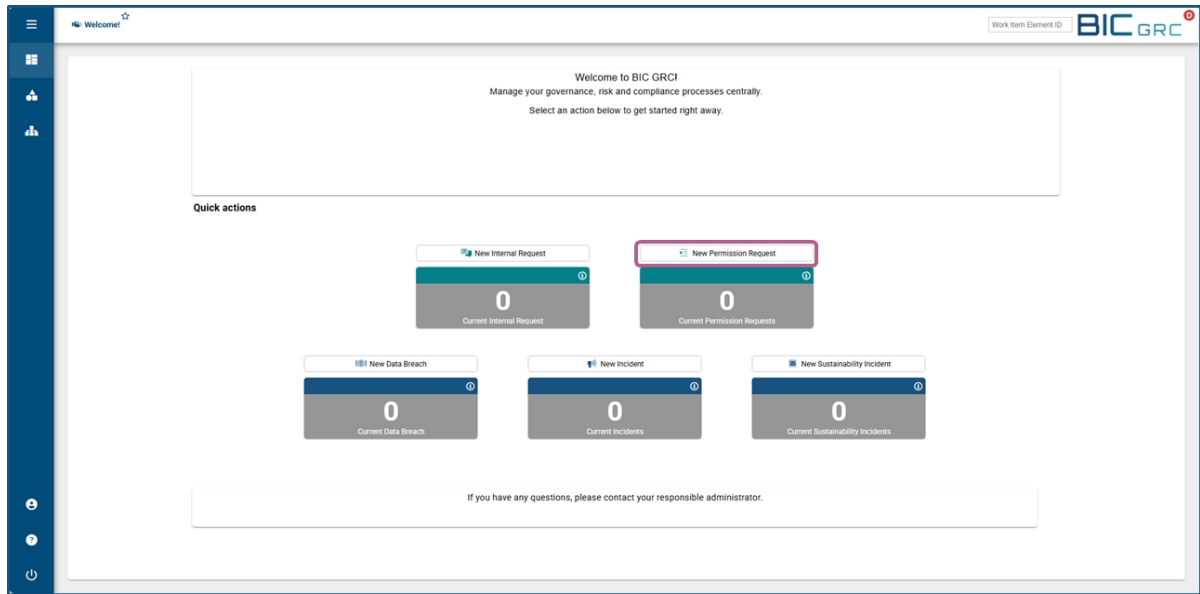
Every user in BIC GRC has the option to submit a *Permission Request*.

Step 1: Create a Permission Request

Standard Users can create *Permission Requests* in several places in BIC GRC.

1. Creation via dashboard

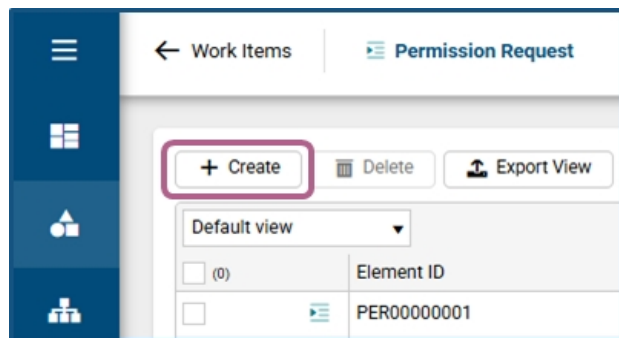
The user navigates via the sidebar to **Dashboards >> Welcome >> "New Permission Request"**.



A new window will then open automatically.

2. Creation via Work Item List

The Editor navigates to **Work Items**
>> Permission Request >> "Create"
 via the sidebar.



Step 2: Enter details

The screenshot shows the 'Permission Request Details' form. At the top right, there is a 'Status' dropdown menu set to 'Registration'. Below this, a 'Name' field (callout 1) contains the text 'Max Mustermann forgot his password' with a '(neutral)' status indicator. A section header 'Permission Request' is followed by another 'Permission Request' label. Below this, there are two dropdown menus: 'Type of Request' (callout 2) set to 'password forgotten' and 'Type of User' (callout 3) set to 'internal AD user'. Below these is a 'Request for User' field (callout 4) showing 'Mustermann Max (Max.Mustermann)' with a search icon. A 'Further Remarks' text area (callout 10) contains the text 'Please reset the password of Max.Mustermann'. At the bottom, a yellow warning bar (callout 11) states 'You have unsaved changes.' followed by 'Save', 'Save and Close', and 'Close' buttons.

- 1 **Name:** The first step is to enter a short but meaningful name for the *Permission Request*. The *Permission Request* is unique when the "Name" is combined with the "Element ID."
- 2 **Type of Request:** The user must then specify the type of *Permission Request*. The type of request primarily differentiates between requests for existing users and requests for users to be created in BIC GRC.
- 3 **Type of User:** The "User Type" depends on the "Type of Request." This allows you to select different user types—from internal and external AD users to internal or external users that need to be created manually.

It is senical to only specify manually created users for "New permissions," since they have not yet been created in BIC GRC. On the other hand, permissions can only be revoked for user who have already been created.

- 4 **Request for User:** To display this attribute, the "User Type" must be specified as internal or external AD user. A user can be searched for and selected using the icon  only when the user already exists in BIC GRC.
- 5 **Request for New User:** Three attributes must be filled in for the "Request for new user":
 - Surname
 - Forename
 - E-Mail address

Under "Further Notes," you can add information such as the new user's position in your company or specify which dashboard should appear as their Standard

dashboard.

- 6 **Basis for permissions:** Depending on the selected "Type of request" and "User Type," the applicant will be shown different bases for granting authorization. If the applicant does not find a suitable selection for the "Basis for authorization," the applicant can select "Other." A text field will then appear where an "Other basis" must be specified.

- 7 **Requested Profiles:** The applicant can select the appropriate profile from all user profiles.

The applicant is shown all user profiles that exist according to the standard solution. If additional user profiles have been added (customized), these can be included in this list manually.

If the last value – Additional Authorization – is selected, a text field with Additional Information must be filled in.

- 8 **Asset Ownership:** Since an Asset-centered authorization concept forms the basis for all authorizations in BIC GRC, the user must be assigned a suitable profile as well as an Asset for which the profile should apply.

If, for example, the authorization should apply to a business unit and all subordinate elements, the checkbox "The Asset authorizations also extend to subordinate elements" needs to be checked so that the request administrator knows that he must set the authorizations accordingly.

The applicant will only see Assets for which they have the appropriate permissions.

- 9 **From and To date:** If the applicant requests a suspension (period) or the withdrawal of permissions (from date), they should enter a date.

- 10 **Further Remarks:** Additional Information can be entered in this text field. This allows special circumstances to be documented, such as the suspension of permissions due to prolonged sick leave or parental leave models for a User.

- 11 **Save:** Once the information has been entered, the user can save it.

Further examples:

Permission Request Details ▶ Obsolete

Element ID PER00000002 Status ● Registration ▼

Name **1** New employment contract with Max Musterman (neutral)

Permission Request Comments Discussion

Permission Request

Registrator
Standard GEN (StandardUser) 🔍

Type of Request
creation of new permission set ▼

Request for User
Mustermann Max (Max.Mustermann) 🔍

Basis for Permissions
new employment contract ▼

Requested Profiles
AssetOwner X

Select...

Processor
--- 🔍

Type of User
internal AD user ▼

Name	Asset Type	End-us...
Location Germany	Business Structure	

☐ The Asset permissions shall extend to subelements

Further Remarks



Permission Request Details

Obsolete

Element ID

PER00000003

Status

Registration

Name

1 Karenz von Max Mustermann

(neutral)

Permission Request

Comments

Discussion

Permission Request

Registrator

Standard GEN (StandardUser)

Processor

2 Type of Request

inactivation of permissions

3 Type of User

internal AD user

4 Request for User

Mustermann Max (Max.Mustermann)

6 Basis for Permissions

inactive employment contract

9 Inactivation of Permissions

from

01/07/2025

to

30/11/2025

10 Further Remarks

Max Mustermann wird bis Ende November in Karenz sein

Step 3: Complete the Permission Request

Permission Request Details

Element ID: PER00000001 Status: In Progress

Name: Max Mustermann hat sein Passwort vergessen (neutral)

Permission Request Processing Comments Discussion

Registrator
Standard GEN (StandardUser)

Processor
Fachadministrator Rainer (Functional...)

Type of Request
password forgotten

Type of User
internal AD user

Request for User
Mustermann Max (Max.Mustermann)

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

Attachment
No documents available.

After saving for the first time, the Creator is automatically stored and a Processor must be specified

1. Furthermore, if necessary, an attachment can be added voluntarily 2.

Once all additions are complete, the status transition can be triggered by clicking the "Send" button

3.

The next step is performed by the [Permission Request Recipient - Answer & edit Permission Request](#).

The user receives a notification as soon as the Recipient begins processing the Permission Request.

2.2 Asset Owner

The term "Asset Owner" refers to a User Profile with responsibility for one or more Assets within BIC GRC. Depending on the module, organizational units, Primary Assets (information & processes), or Supporting Assets (e.g., software, hardware, etc.) can be maintained as Assets in BIC GRC.

An Asset Owner has the following tasks in BIC GRC:

- [Identify & create a Measure](#)

2.3 Asset Manager

The Asset Manager is responsible for a specific node within the Asset hierarchy—for example, a Business Unit—as well as all Assets below it (e.g., Primary Assets or Supporting Assets).

The Asset Manager is responsible for creating, editing, and maintaining Assets. This role helps to ensure a complete and up-to-date Asset data within the Asset Hierarchy.

An Asset Manager has the following tasks in BIC GRC:

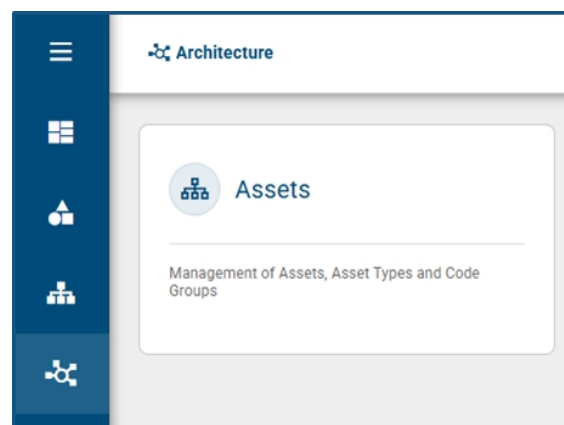
- [Prepare & maintain Assets](#)
- [Prepare & assign GRC Framework Items for Assessments](#)

2.3.1 Prepare & maintain Assets

If one or more Assets have been assigned to an Asset Manager, they are responsible for managing them.

Step 1: Navigate to Assets

Using the side bar **Administration >> Assets**, they can navigate to the Asset Hierarchy in BIC GRC. The layout may vary depending on the user based on an individual's permission level.

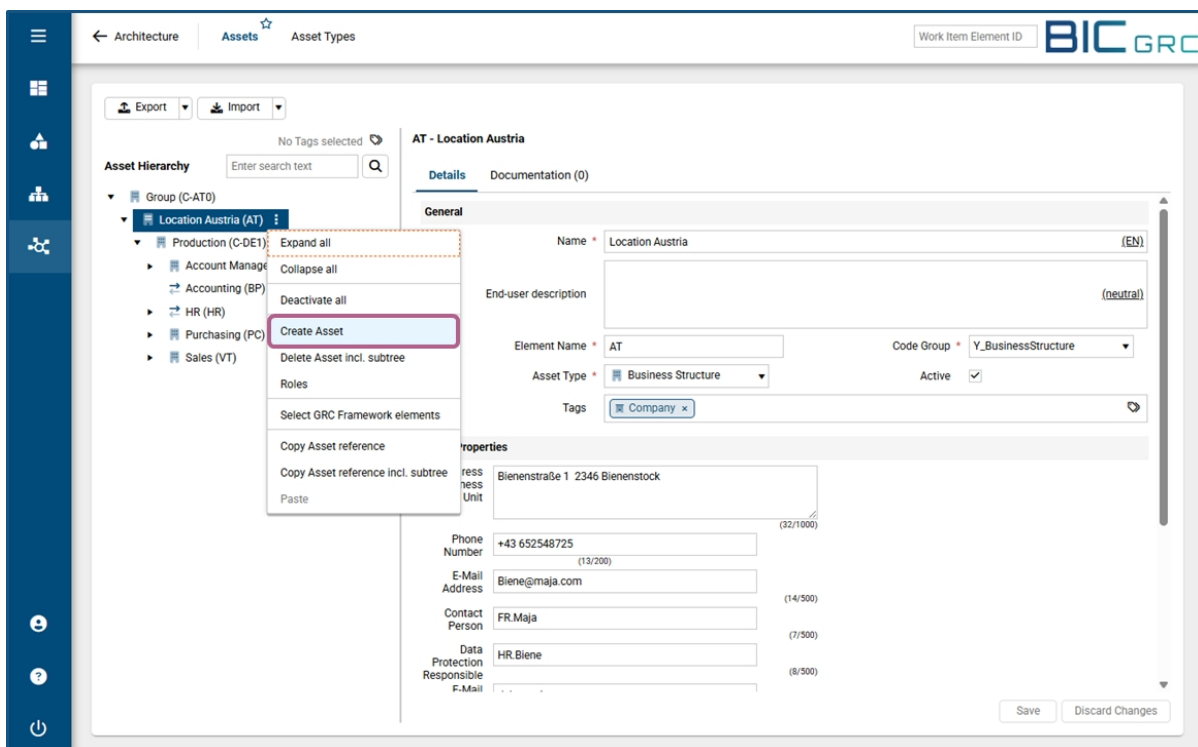
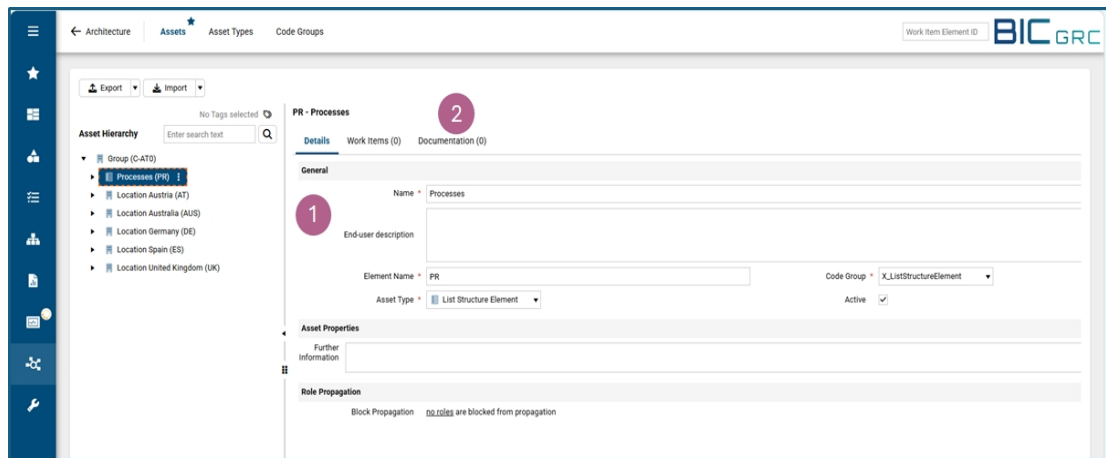


Step 2: Create Assets

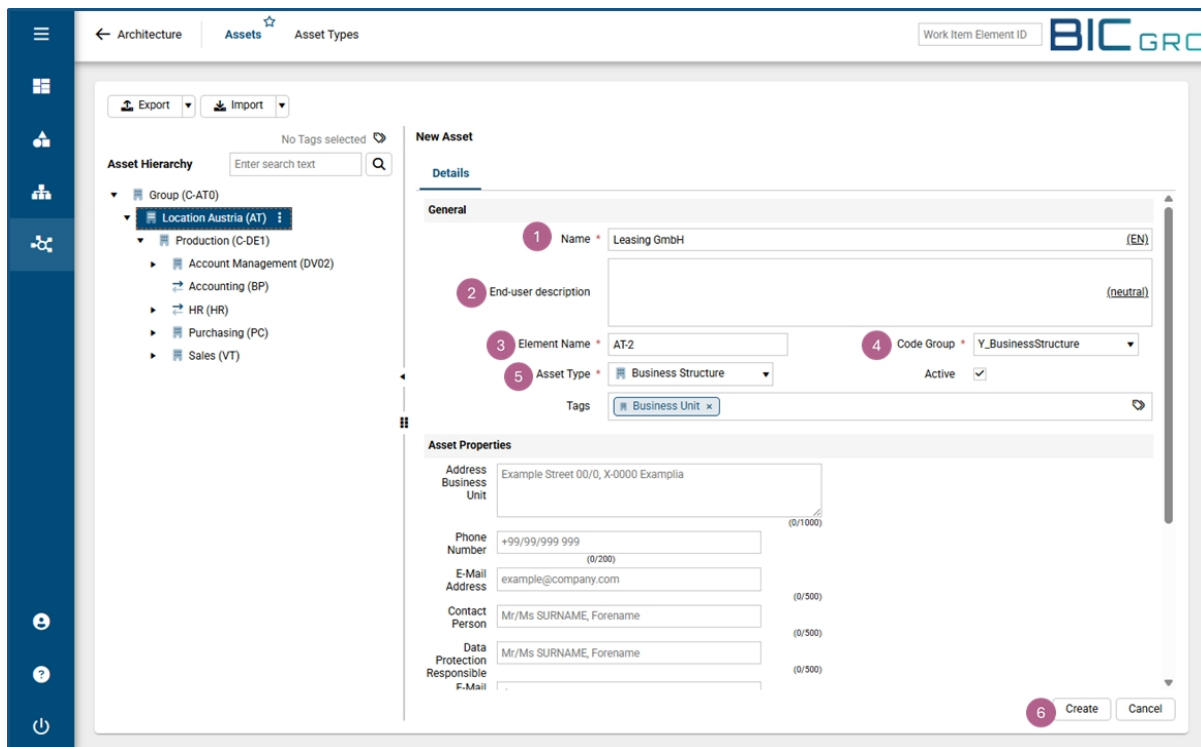
The Asset Manager sees a two-part view on the Assets menu tab:

- Left side: Tree structure of the Asset hierarchy. This tree can be expanded and collapsed using the corresponding icon ▶.

- Right side: Detailed view of the selected Asset with information ¹ and stored documentation ².



A new Asset is created by right-clicking (or clicking on the three dots ) on an existing Asset and selecting "Create Asset." The "New Asset" window then appears on the right-hand side, where relevant information can be stored.



1 **Name:** Enter a suitable "Name" for the Asset.

It is important to ensure that the "Neutral Name" as well as the German and English versions of the Asset Name are maintained.

The "Neutral Name" is used for display in several places in BIC GRC, so there is a strong recommendation that you choose a meaningful name.

2 **End User Description:** It is recommended to enter a description for an Asset in order to explain the importance or basic structures of the Asset to end users.

3 **Element Name:** The "Element Name" makes the Asset unique in BIC GRC. The "Element Name" is always displayed next to the name of the Asset in the Asset Hierarchy.

4 **Code Group:** Only certain Code Groups are relevant for creating Assets. The following Code Groups should be used for Assets:

- X_ListStructureElement: Should be used for Assets of the Type "List Structure Element."
- Y_BusinessStructure: Should be used for assets of the type "Business Structures"
- Z_Asset: Should be used for assets of the types "Primary Asset" and "Supporting Asset"

5 **Asset Type:** There are four different asset types in BIC GRC:

- Business Structure: Represent the highest possible level after the top node in the Asset hierarchy.
- Primary Asset: These are classified directly below the Business Structures and are information or processes.

- Supporting Asset: Represents all elements that support the Process or information.
- List Structure Element: Should help users create a structure in the asset hierarchy.

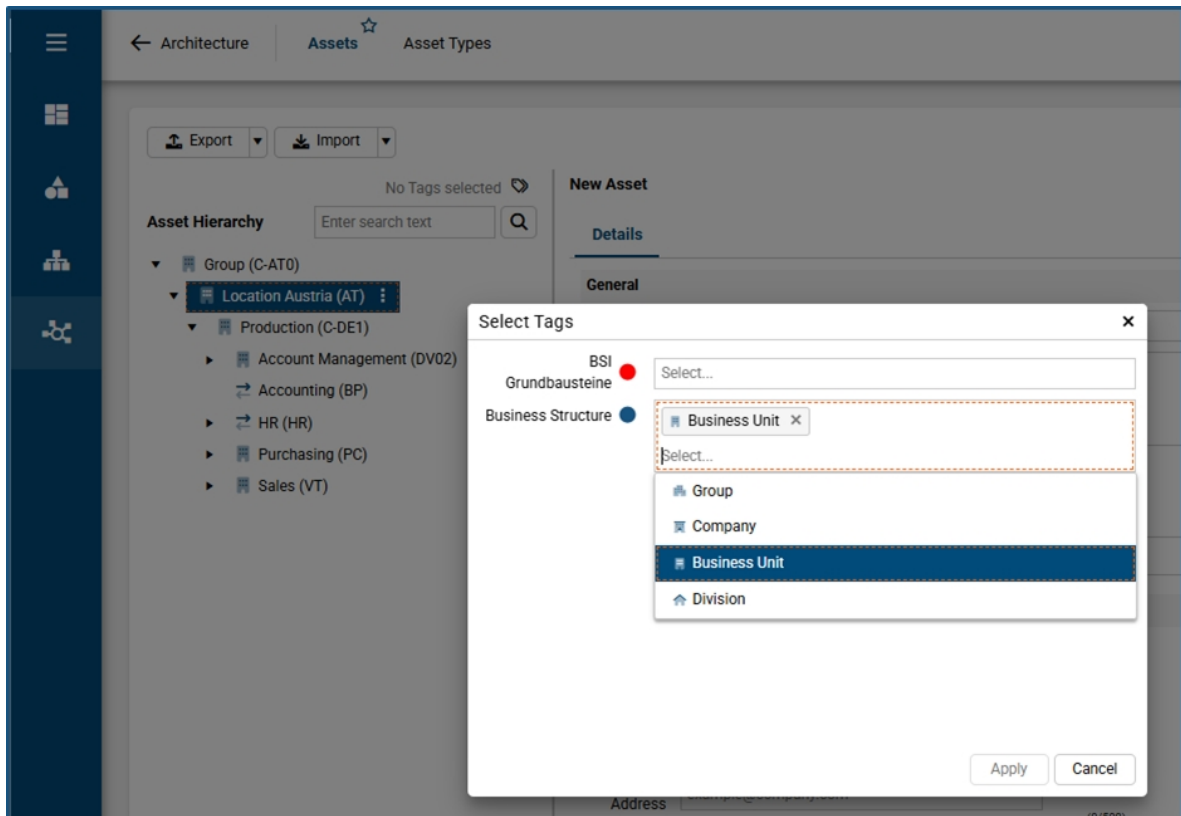
To ensure optimal function of in BIG GRC, one should not change an Asset's Type after its creation.

6

Create: Once these entries have been made, the Asset can be created.

Step 3: Tag Assets

After the Asset has been created, appropriate tags can be assigned. Clicking on the corresponding icon  suggests all available tags that can be assigned to the Asset.



Depending on the Asset Type, different Tag categories are suggested to the Asset Manager.

This step is essential for the optimal use of BIG GRC, as its many areas require not only the appropriate Asset Type but also the appropriate Tag.

Step 4: Maintain Asset Properties

Additional properties can be maintained for the Assets that have the Asset Types "Company Organizational Unit" or "Supporting Assets." These Asset Properties can be expanded or reduced by the Company as needed.

If a structural change of Asset properties is necessary, it is possible to add or reduce properties. For more information, please contact the Responsible Functional Administrator at your company.

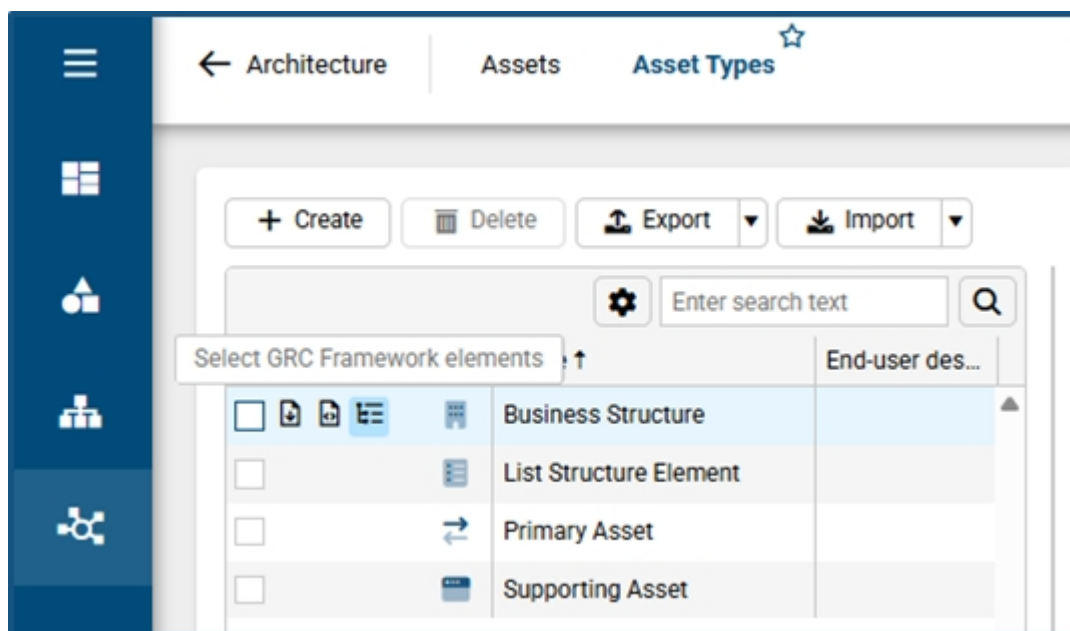
"Primary Assets" also have Asset properties, however, they should not be editable by the Asset Manager. Instead, these are automatically populated by various mechanisms in BIC GRC.

2.3.2 Prepare & assign GRC Framework Items for Assessments

Assessments are performed in BIC GRC. Assessments are always viewed in the context of an Asset. Therefore, if GRC Framework Items are to be queried as part of an Assessment for a specific Asset Type, this must be specified before starting an Assessment.

Step 1: Assign GRC Framework Items to Asset Types

The Asset Manager can navigate to the Asset Types via the sidebar **Administration >> Assets >> "Asset Types"** tab.



An User may "Select GRC Framework elements" via the icon  next to the name of the Asset Type on the left-hand side or via an Excel file when using the "Export" button.

The Asset Manager is then shown a dialog where he can select an Assessment Type and its active phases, and subsequently select the GRC Framework items.

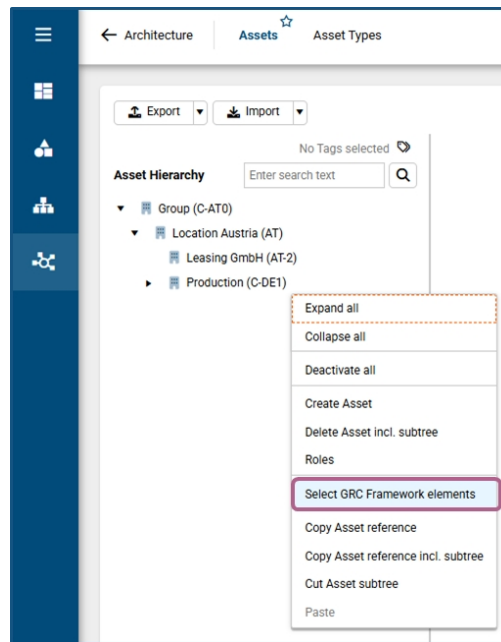
For additional information on selection of GRC Frameworks please refer to the BIC GRC Administrator's Manual.

Step 2: Assign GRC Framework Items to the Asset

Using the sidebar **Administration >> Assets >> "Assets"** tab, the Asset Manager can also make assignments of GRC Framework Items to Assets in addition to the Asset Types.

By right-clicking on an Asset or clicking on the three dots next to the Asset name  on the left-hand side, elements can be added to the "Select GRC Framework Items" menu item for the types "Company Organizational Unit" or "Supporting Asset".

The Asset Manager then sees an analogous dialog as described above.



2.4 Assessor

An Assessor is a user who has the task of performing various Assessments on their Asset.

Assessments can be thought of as questionnaires with questions on specific topics, such as ISO 27701.

An Assessor has the following tasks in BIC GRC:

ISO 27701

- [Create & start Assessment](#)
- [Perform & conduct Control Assessment and evaluate it](#)
- [Complete & evaluate Assessment](#)

The Assessor can also create additional Work Items in BIC GRC. While this is beyond their primary responsibility, we will refer to other user profiles at this point:

- [Define & create Objective](#)
- [Define & create Milestone](#)
- [Define & create Measure](#)

- [Define & create Control](#)
- [Define & create Security Risk](#)

2.4.1 ISO 27701 - Create & start Assessment

An ISO 27701 assessment is crucial if your organization aims to establish, expand, or review its Privacy Management system—especially in the context of an existing ISMS according to ISO 27001.

The standard specifically expands ISO 27001 to include requirements for Privacy management, particularly with regard to Personal Data (PII). An Assessment therefore serves to systematically analyze, improve, and make Privacy processes auditable.

In the ISO 27701 assessment, the assessor is responsible for preparing the assessment and carrying out the Evaluation.

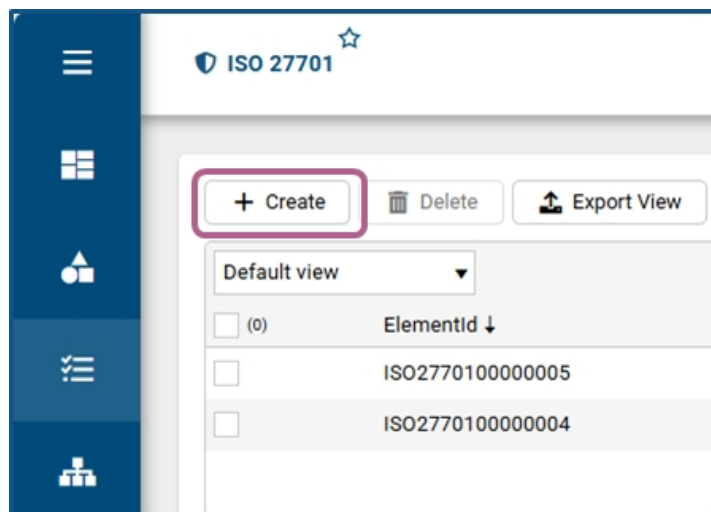
The following activities should have taken place before the Assessment for a specific Asset is created:

- [Asset Manager - Prepare & maintain assets](#)
- [Asset Manager - Prepare & assign GRC Framework Items for Assessments](#)

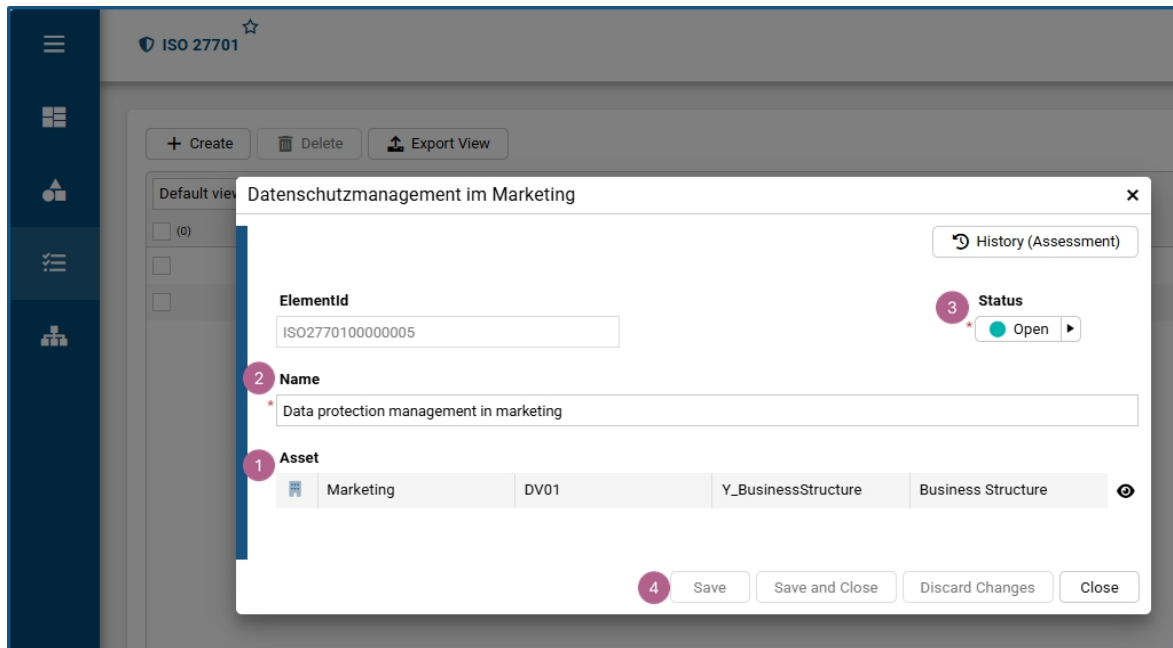
Step 1: Navigate to Assessment

The assessor creates an assessment of the type "ISO 27701" via the sidebar **Assessments** "Create" or **Assets** >> **Select a business unit or Supporting Assets** >> **Links** >> **Open the "ISO 27701" tab** >> **"Create"**.

Assessments of this type can be performed on a "Supporting Asset" or a "Business Unit."



Step 2: Enter Assessment details



- 1 **Asset:** Using a wizard, the assessor first selects an asset for which they want to create an assessment of the Type "ISO 27701". Once an asset has been selected using a checkbox, you can navigate to the next step.

After selection, the Asset is automatically linked in the Assessment and remains fixed.

- 2 **Name:** The next step should be to enter a short but meaningful name for the Assessment. The Assessment is unique when the "Name" is combined with the "Element ID."
- 3 **Element ID and Status:** The Element ID is automatically assigned a value after "Create" and remains unchanged. The status stays in "Evaluation" until all necessary entries have been made in the Assessment. Once all entries are complete, the status can be set to "Completed."
- 4 **Save:** Once these entries have been made, the Assessment can be created.

Step 3: Check GRC Framework Items Assignments

Before starting the Assessment, it is recommended to review the stored information and the GRC Framework Items that have been linked so far. The information that is already "activated" in the Assessment was specified for the Asset or Asset Type by authorized persons and then automatically activated for the Assessment.

To do this, the assessor clicks on the three dots to the left of the Element ID  on "Assign GRC Framework Items ". The next step is to review the assessment phase "Control Assessment" for correctness or whether additions to the previous selections are necessary before clicking on "Save." After the Assessor has made additions, not only are the GRC Framework Items taken from the Asset activated, but also the additionally selected Items.

If the Assessor adds GRC Framework Items later, e.g., when the Control Assessment has already begun, the newly added GRC Framework Items are automatically activated and can be evaluated as part of the current Assessment.

If the Assessor deselects GRC Framework Items, the previous evaluations for the specific element will be cleared.

Step 4: Start Assessment

Once the assessment has been created and the GRC Framework Items have been checked, the assessment can be started. To do this, the Assessor clicks on the icon  and selects "Control Assessment" in the wizard that opens.

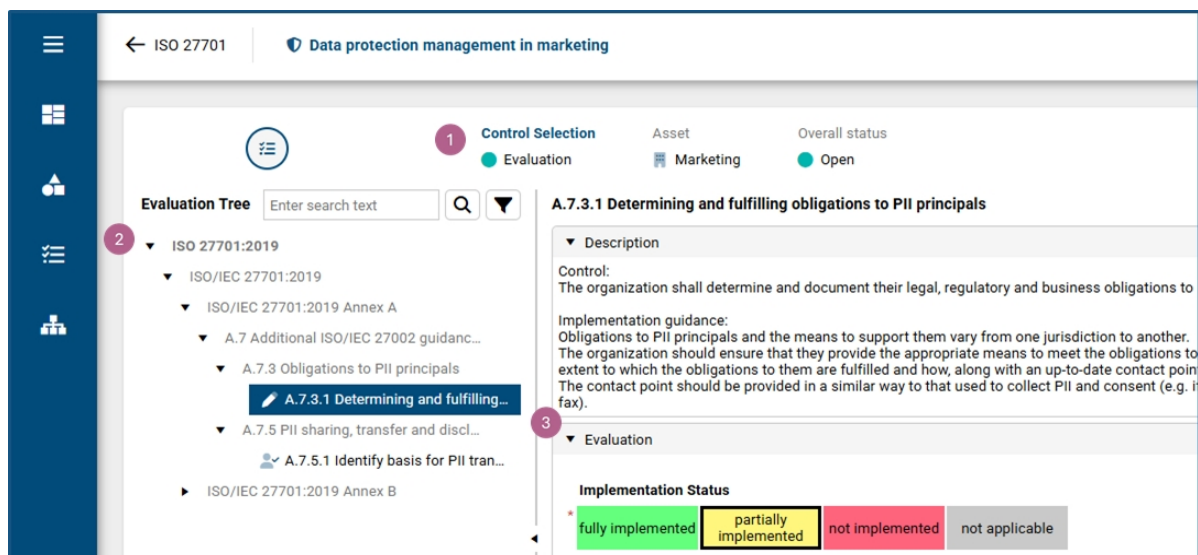
The assessor can find the next steps under [Assessor - Perform & conduct evaluation](#).

2.4.2 ISO 27701 - Perform & evaluate evaluation

Once the Assessor has started the Assessment for "ISO 27701" for a specific Asset, they can begin the Evaluation.

Step 1: Overview of the Assessment screen

The Assessor has three sections that are relevant for the execution of the "Control Assessment."



In the upper section, the Assessor will find basic information such as Status and Asset ¹.

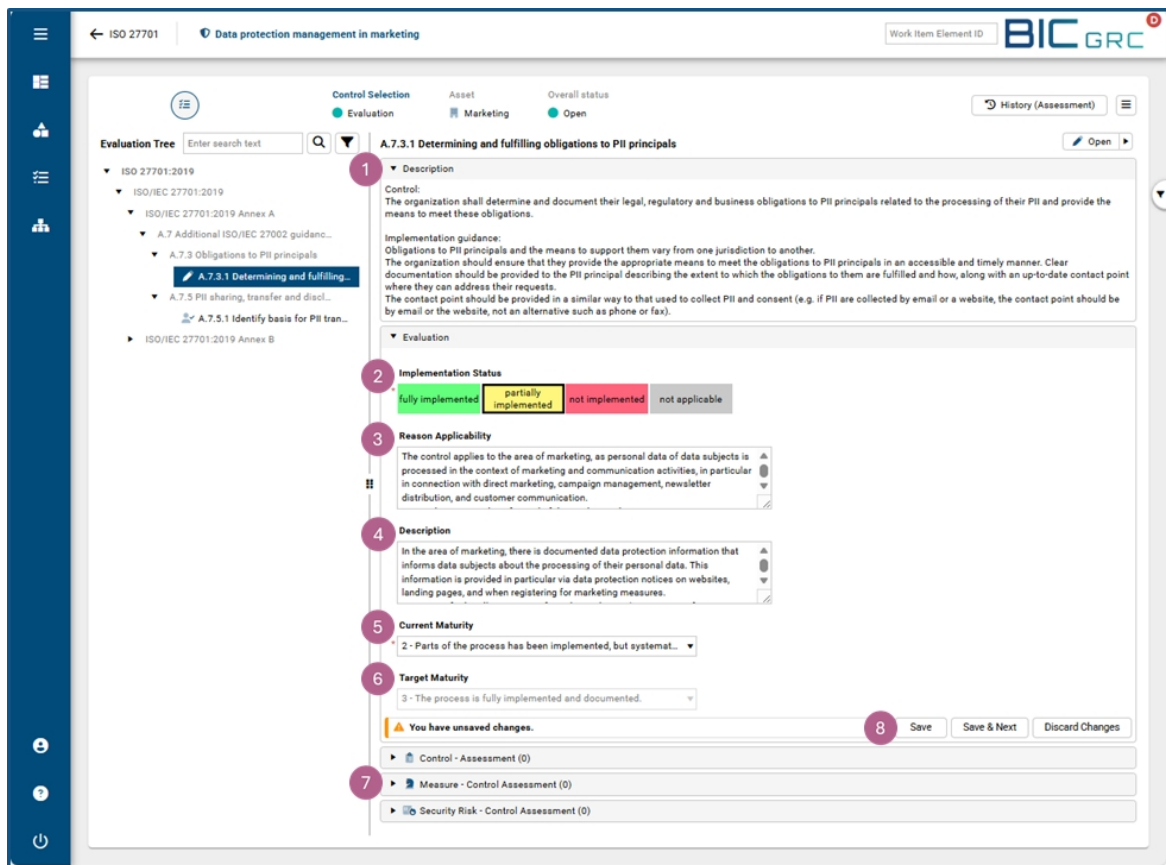
On the left side of the window, they will find the GRC Framework ² to be evaluated. In the assessment for "ISO 27701," the Assessor must perform the evaluation of all activated GRC Framework Items. The GRC Framework can be opened by clicking on the icon .

In the "Control Assessment" for the GRC Framework "ISO 27701:2019," the Assessor focuses on evaluating the lowest GRC Framework Items.

GRC Framework Items to be evaluated have the icon , while Completed GRC Framework Items have the icon .

On the right side of the window, the Assessor will find the main mask for evaluation ³. This will be described in more detail in the next steps.

Step 2: Enter assessment details



The screenshot shows the BIC GRC assessment interface. On the left is an 'Evaluation Tree' with a search bar and a list of ISO 27701:2019 items. The selected item is 'A.7.3.1 Determining and fulfilling obligations to PII principals'. The main panel on the right is titled 'A.7.3.1 Determining and fulfilling obligations to PII principals' and contains several sections: 'Description' (1), 'Implementation Status' (2), 'Reason Applicability' (3), 'Description' (4), 'Current Maturity' (5), 'Target Maturity' (6), and a 'You have unsaved changes' warning (8). At the bottom, there are buttons for 'Save', 'Save & Next', and 'Discard Changes'. A sidebar on the left contains icons for navigation and a power button at the bottom.

1 Panel - Description: First, the Assessor sees a description taken from the GRC Framework "ISO 27701:2019." This is the description that was stored directly in the GRC Framework.

The description is intended to provide additional information for this GRC Framework Item and remains unedited by the Assessor.

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

2 Implementation Status: The "Implementation Status" should reflect the extent to which a specific requirement, control, or measure has been implemented in accordance with ISO 27701:2019.

If the requirement is applicable, points 5 & 6 will be displayed to the Assessor.

If the control is still in progress but applicable, it is recommended to create or link a Work Item *Security Risk*.

3 Applicability Rationale: The Assessor can provide a justification for why the requirement is applicable. When the assessor indicates that the requirement is "not applicable," they must provide a justification.

4 Description: The Assessor can then add an additional description.

5 Current Maturity Level: The Assessor can select a Current Maturity Level between 0 and 5, depending on how the Current State of implementation, integration, and communication is evaluated. The objective is to achieve the Target Maturity Level.

6 Target Maturity Level: The Target Maturity Level is transferred from the GRC Framework "ISO 27701:2019."

The default setting is the Target Maturity Level "3 - The process is fully implemented and documented." This suggestion can be overridden by an authorized User before the start of all Assessments.

The Target Maturity Level is fixed for the Assessor.

7 Assignments: As part of the "Control Assessment," the Assessor can create or assign the following Work Items:

- Control
- Measure
- Security Risk

Security-Risk may arise because, for example, the implementation of the requirement is still pending.

When creating the *Security Risk* from the Assessment, the Asset link and the link to the "Control Assessment" are filled in automatically.

8 Status change: Once all information has been entered, the status is changed to "Completed" in the upper right window.

Once the status transition of an evaluation has been completed, the evaluation is locked and remains unchanged.

Once all evaluations on the left side of the window display the  icon, the status of the entire "Control Assessment" phase automatically changes to "Completed."

Further steps can be found under [Assessor - Complete & evaluate Assessment](#).

2.4.3 ISO 27701 - Complete & evaluate Assessment

Once the Assessor has started the Assessment for "ISO 27701" for a specific organizational unit and finalized the Evaluation, the final step can begin - completing the Assessment.

Step 1: Complete Assessment

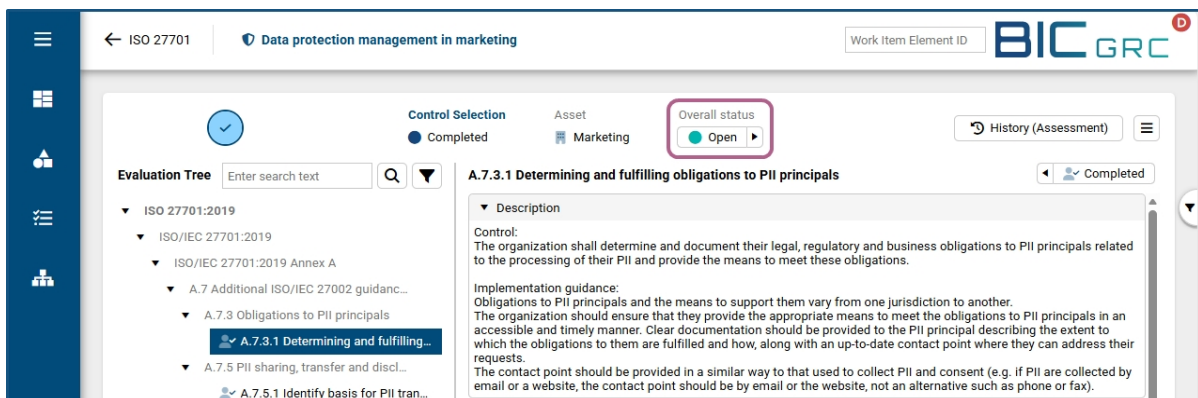
In order to complete the Assessment, the phase must be completed.

The Assessor is the designated role for completing the Assessment.

The Assessment can be completed in two ways.

1. Completion in the phase

The Assessor can change the status directly in the phase.



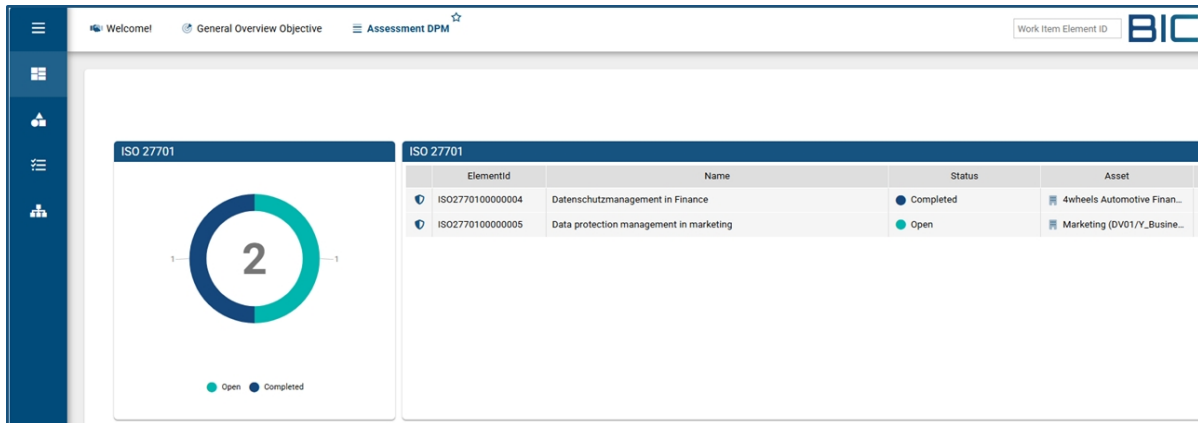
The status is displayed only when the phase is completed, and it remains Read Only outside this condition.

2. Completion in the Assessment Type

In addition to the phase, the assessor can also complete the Assessment via the Assessment Type. The assessor can open the Assessment Type and change the status via the  icon in the list.

Step 2: Evaluate results

In BIC GRC, there is a dashboard for evaluating the Assessment for "ISO 27701" under the menu item **Dashboards >> Assessment DPM**.



Step 3: Further procedure

The Assessment can be reopened at any time. To do this, the Assessor can set the Status back to "Evaluation" (see step 1 above). The phases must then be reopened manually so that they can be reviewed.

The Assessor will not receive a notification when a new Evaluation is required.

2.5 Editor Risk

In BIC GRC, the *Editor Risk* is primarily responsible for creating, evaluating, and handling one or more risks. They have the authority to assess a risk based on its probability of occurrence and frequency and its monetary damage potential from its current state to the target value.

The Editor of Risk has the following preparatory tasks:

- [Identify & create Threats](#)
- [Identify & create Vulnerabilities](#)
- [Derive & create Risk Scenario](#)
- [Define & create Objective](#)
- [Define & create Milestone](#)

An Editor has the following ongoing tasks in BIC GRC:

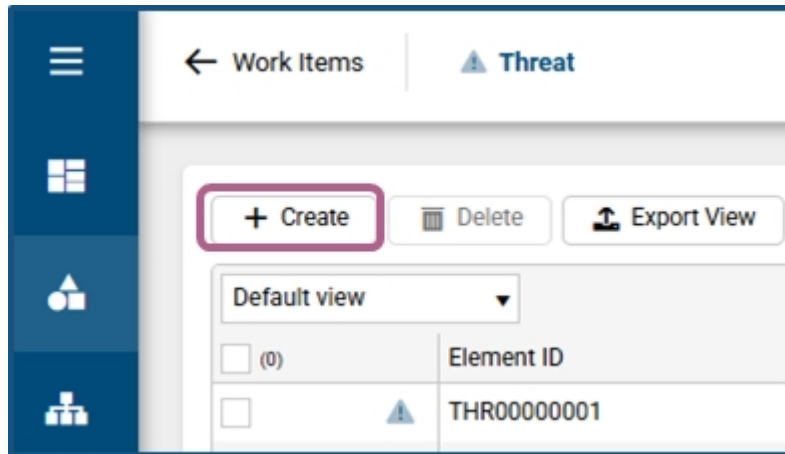
- [Identify & create Security Risks](#)
- [Supplement & analyze Security Risks](#)
- [Assess & evaluate Security Risks](#)
- [Derive & create Measure Evaluations](#)
- [Identify & create Measures](#)
- [Derive & create Controls](#)
- [Implement & review Objectives](#)

2.5.1 Identify & create Threats

To derive a *Risk Scenario*, a suitable *Threat* should be created in advance.

Step 1: Create threat

The Editor Risk navigates to **Work Items >> Threat >> "Create"**.



A new window will then open automatically.

Step 2: Enter details

Threat Details Next

Element ID: THR00000002 Status: Draft

* Name **1** Cyberattack against an IT service provider (e.g., ransomware) (EN)

Description Discussion Technical Attributes Work Item Links Documentation (0) History

Description of the Threat

2 Editor User Demo (ERM_DemoUser) **Created by** EditorRisk ERM

3 Type of Threat Intentional Threat

4 Description of the Threat
An external IT service provider on whose systems the company relies for central digital services becomes the target of a cyber attack (e.g. ransomware, DDoS, targeted sabotage). This results in partial or complete failure of the services and infrastructure provided. (266/5000)

5 Drop files here to upload
No documents available. +

4 Description of Attack Vectors
Compromise of admin access at the service provider
Infiltration of malware via third-party components or unprotected interfaces
Distributed denial of service (DDoS) on hosting platforms
Social engineering (e.g. phishing campaigns targeting service provider employees) (270/5000)

4 Description of Exploits
Use of ransomware (e.g. LockBit, Clop) on productive systems
Exploitation of known vulnerabilities (e.g. Log4j, Fortinet vulnerabilities, Exchange Zero Days)
Bypassing authentication mechanisms via faulty API implementation
Lack of segmentation within the service provider's systems (285/5000)

6 Save Save and Close Close

1 **Name:** Here a short but meaningful name for the *Threat* is entered.

2 **Editor:** An Editor responsible for the *Threat* is entered.

Regardless of the GRC perspective, only users with the "Editor Risk" user profile can be selected here.

Users entered as Editor will be notified via a notification.

- 3 **Type of Threat** : The Editor can choose between three threat types:
 - Natural threat
 - Unintentional threat
 - Intentional threat
- 4 **Descriptions of Threat**: After classification, the *Threat* is described. The Editor has three different description fields at their disposal to describe the *Threat* in as much detail as possible.
The Editor should then save the Work Item for the first time.
- 5 **Documents**: Once the *Editor Risk* has saved the Work Item, they can add documents if necessary.
- 6 **Status change**: Once the Editor has made all entries, they can change the status to "Active."

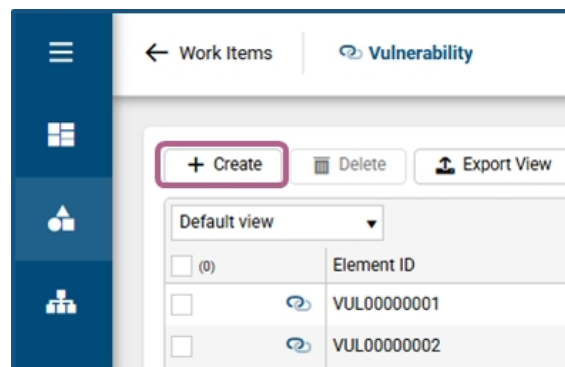
There are no notifications for the creation and "Activation" of a *Threat*.

2.5.2 Identify & create Vulnerability

To derive a *Risk Scenario*, a *Vulnerability* should be created in advance, in addition to a *Threat*.

Step 1: Create Vulnerability

The Editor Risk navigates to **Work Items >> Vulnerability >> "Create"**.



A new window opens automatically.

Step 2: Enter details

Vulnerability Details Next

Element ID: VUL00000002 Status: Draft

* Name **1** Lack of security and resilience requirements in service provider contracts (EN)

Description Discussion Technical Attributes Work Item Links Documentation (0) History

Description of the Vulnerability

2 Editor Created by EditorRisk ERM

* EditorRisk ERM (ERM_EditorRisk) Q

3 **Description of the Vulnerability**

* The existing contract with the IT service provider lacks binding requirements regarding security measures, business continuity, patch management and reporting obligations in the event of damage. There are no defined SLAs for recovery time or the integrity of the transmitted data. There is no emergency strategy for changing service providers. (343/5000)

3 **Description of the Attack Surface**

External hosting infrastructure on which business-critical applications are operated
Administration interfaces (e.g. web portals, APIs) without additional access control
Insufficiently controlled third-party components operated via the service provider
Customer databases or configuration data stored with the service provider (329/5000)

4 Drop files here to upload
No documents available. +

5 Save Save and Close Close

1 **Name:** Here a short but meaningful name for the *Vulnerability* is entered.

2 **Editor:** This field is for the editor responsible for processing the *Vulnerability*.

Regardless of GRC perspective, only users with the "Editor Risk" user profile can be entered.

Users entered as Editor are then notified via notification.

3 **Descriptions:** After classification, the *Vulnerability* can be described. The Editor has two different description fields at their disposal to describe the *Vulnerability* in as much detail as possible.

4 **Documents:** Once the Editor Risk has saved the Work Item, they can add documents if necessary.

5 **Status change:** Once the Editor has made all entries, they can change the status to "Active."

No Notifications are sent when a *Vulnerability* is created or made "Active"

2.5.3 Derive & create Risk Scenario

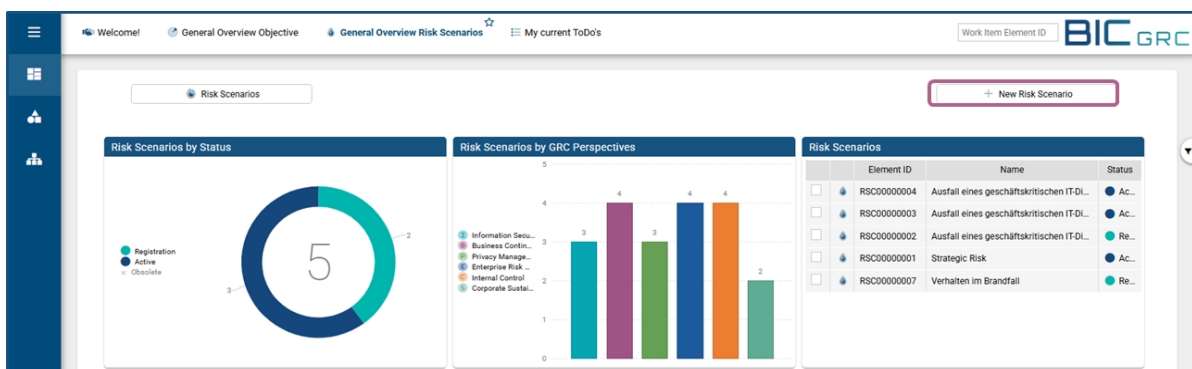
In BIC GRC, it is possible to derive risks. To do this, the Editor can use the *Risk Scenario* Work Item Type.

Step 1: Create Risk Scenario

The Editor can create *Risk Scenarios* in several places in BIC GRC.

1. Creation via the "Risk Scenario Overview" dashboard

The Editor navigates to **Dashboards >> General Overview Risk Scenarios >> "New Risk Scenario."**

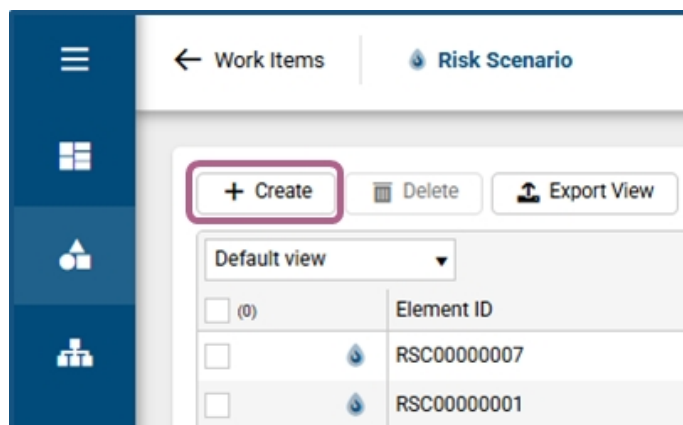


A new window then opens automatically.

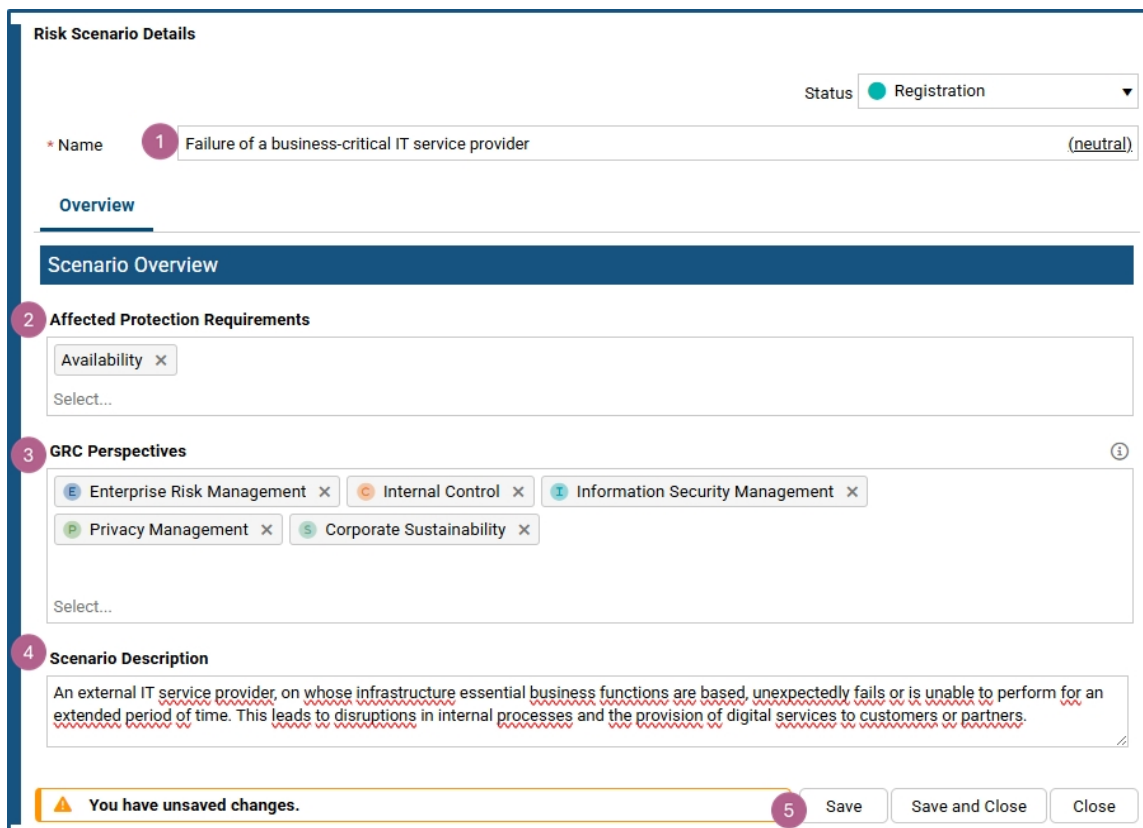
2. Creation via Work Item list

The Editor navigates to **Work Items >> Risk Scenario >> "Create."**

A new window then opens automatically.



Step 2: Enter details



- 1 **Name:** The first step is to enter a short but meaningful name for the *Risk Scenario*. This "Name" in combination with the "Element ID" makes the *Risk Scenario* unique.
- 2 **Affected Protection Requirements:** The Editor can define three protection goals:
 - Confidentiality: Protection against unauthorized access to information.
 - Integrity: Protection against unnoticed or unauthorized modification of information.
 - Availability: Ensuring that information and systems are available when needed.
- 3 **Scenario description:** The *Risk Scenario* should be documented and described in as much detail as possible so that other perspectives can also recognize a connection.
- 4 **Saving process:** Once the necessary information has been entered, the *Risk Scenario* can be saved for the first time.

During the save process, the creator is automatically entered in the "Editor" user field.

Step 3: Define basics

As a next step, the Editor should switch to the "Background" tab to enter additional information.

Risk Scenario Details

Next

Element ID

RSC00000004

Status

Registration

Name

Failure of a business-critical IT service provider

(neutral)

Overview

Background

Discussion

Technical Attributes

Work Item Links

Documentation (0)

History

Risk Identification

1 Used Methods

Name	Catalog	E...	
 Business Impact Analysis (BIA)	Identification Methods		

2 Other Methods

Interview

3 Attachment

Drop files here to upload

No documents available.

+

Risk Analysis

4 Possible Causes

Unexpected insolvency of the service provider

Risk Types by Origin

Name	Element Name	E...	
 Technical Risk	RiskTypes.01origin.01		

5 Possible Consequences

Partial or complete loss of digital customer access

Risk Types by Impact

Name	Element Name	E...	
 Reputation Risk	RiskTypes.02impact...		

Save

Save and Close

Close

- 1 **Used Methods:** The Editor can choose from a predefined GRC Framework which method they used to derive the *Risk Scenario*.

In most cases, *Risk Scenarios* are derived using common identification methods. For a better overview of which method has produced the most or most important *Risk Scenarios*, this link between the *Risk Scenario* and the GRC Framework can be established, which can later be evaluated on dashboards, for example.

- 2 **Other methods:** If the required identification method is not yet available in the maintained GRC Framework, a method can be specified in text form.

- 3 **Attachment:** Additional information is stored here via documents.

The meeting minutes of a previous workshop are an exemplary attachment.

- 4 **Possible Causes:** The *Risk Analysis* also specifies the causes that may lead to the risk. This can be done either in writing or by performing allocation using a link to a GRC Framework.

- 5 **Possible Consequences:** In addition to the origin, the impact of the *Risk Scenario* can also be specified. A GRC Framework can also be linked.

The Editor is shown only elements of frameworks tagged with the appropriate GRC Perspective.

The information on the cause and impact (both text and link) can be transferred to a *Security Risk* created from this *Risk Scenario*. The information is transferred and displayed when the configuration allows the *Risk Analysis* to be displayed in the *Security Risk*.

- 6 **Risk derivation:** Finally, an assignment to

- a Risk Catalog or
- a Threat and a Vulnerability

can be specified.

- 7 **Status change:** After all information has been entered, it can be saved and the status may be changed to "Active" in the upper right corner.

The creation and "activation" of a *Risk Scenario* does not come with any notification.

Risk Scenario Details Next

Element ID: RSC00000004 Status: Registration

* Name: Failure of a business-critical IT service provider (neutral)

Overview **Background** Discussion Technical Attributes Work Item Links Documentation (0) History

6 Risk Derivation

Risk Catalog

Element Name	Name
BSI_IT_BaselineProtection.G23	G 0.23 Unauthorized Access to IT-Systems

Control Catalog

No existing mapping.

Vulnerability

Name	Status	D...
Lack of security and resilience requirements in service provider contracts	Draft	

Threat

Name	Status	D...
Cyberattack against an IT service provider (e.g., ransomware)	Draft	

7 Save Save and Close Close

Step 4: Further procedure

Both users with the *Editor Risk* user profile and *Approver Risk* users from other GRC Perspectives have access to the *Risk Scenario*. All users except the *Editor Risk* have read-only rights, and the *Editor Risk* retains full editing rights.

Risk Scenario Details Registration Obsolete + Risks

Element ID: RSC00000062 Status:

Name: Failure of a business-critical IT service provider

Overview **Background** Discussion Technical Attributes Work Item Links Documentation (0) History

Create new Security Risk
Create new Enterprise Risk
Create new Process Risk
Create new Sustainability Risk

If adjustments or additions are necessary for the respective perspective, this can be discussed using the "Discussion" tab.

The *Risk Scenario* can be linked after the activation of a *Security Risk*.

In addition, Editors and Approvers of other perspectives/modules have the option of creating other risk types, such as *Enterprise Risk*, directly from the *Risk Scenario*. However, the GRC perspective must match the one entered in the *Risk Scenario* to display the creation in the upper right window.

2.5.4 Define & create Objectives

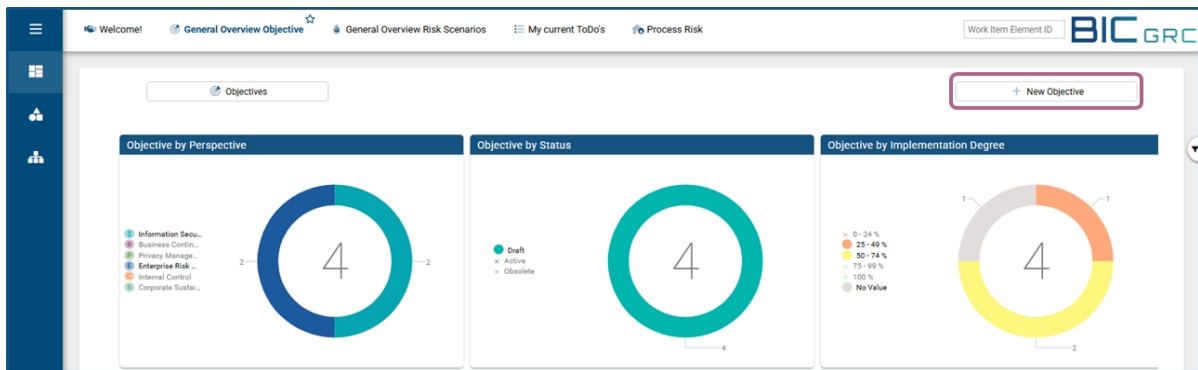
In BIC GRC, it is possible to define *Objectives* and link them in different contexts.

Step 1: Create objective

The Editor can create *Objectives* in several places in BIC GRC.

1. Creation via the "General Overview Objectives" Dashboard

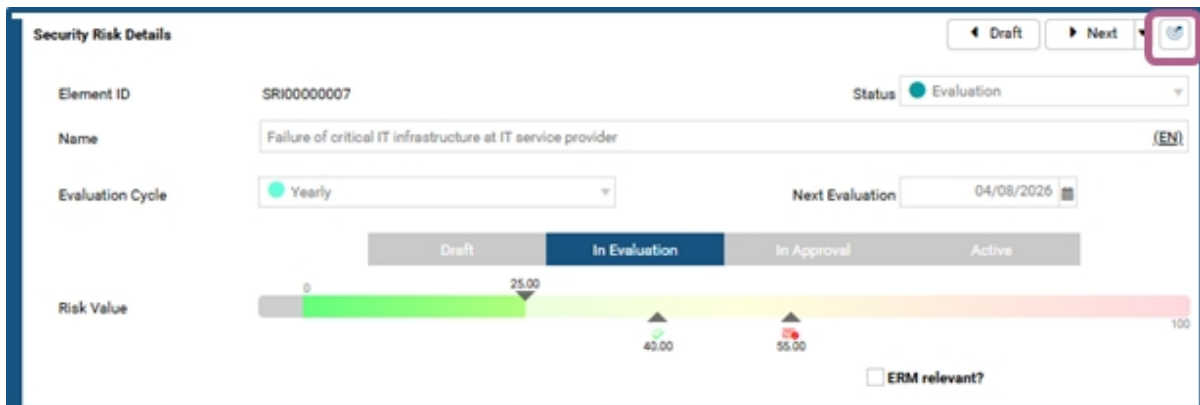
The Editor navigates via to **Dashboards >> General Overview Objectives >> "New Objective."**



The creation of a new *Objective* is performed by clicking a button in the upper right corner of the window.

2. Creation via *Security Risk*

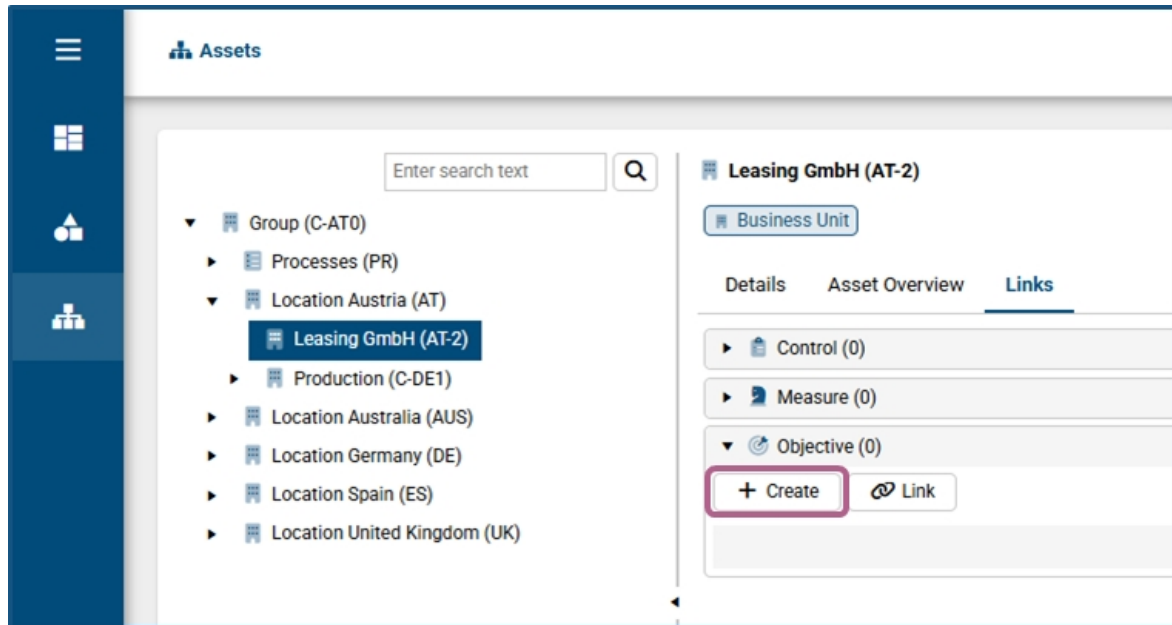
The *Editor Risk* can create a goal from the *Security Risk*. The option is displayed in the upper right corner of the window in "Draft," "Evaluation," and "Treatment" status.



3. Creation via Asset Overview "Links"

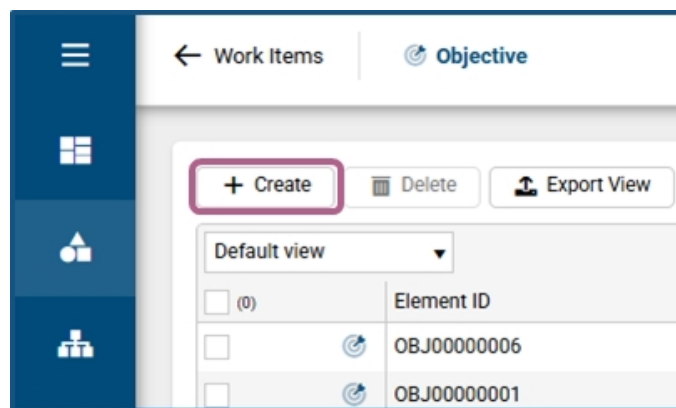
The Editor navigates to **Assets >> Selection of a business unit >> Links >> Open the "Objective" tab >> "Create"**.

A new *Objective* is created by clicking the "Create" button in the middle of the window.



4. Creation via Work Item List

The Editor navigates to **Work Items >> Objective >> "Create"**.



Step 2: Define the Objective

Objective Details

Status Draft

Name

1 Business-critical processes remain available, protected and controllable even in the event of a malfunction... (neutral)

Definition

Objective

2 GRC Perspective

Privacy Management

3 Description

The achievement of objectives is based on a systematic survey of all business-critical processes, their evaluation according to protection requirements (availability, confidentiality, integrity) and the evaluation of existing measures from the perspective of BCM, ISMS, data protection, ICS and risk. Fulfilment is measured using a target process catalogue with defined key figures (e.g. protection coverage, tested emergency plans).

4 Scope

Name	Element Name	Asset Type
Location Australia	AUS	Business Structure
Location Austria	AT	Business Structure

5 Key Performance Indicator

Availability of tested emergency and protective measures for critical processes

Target Value

100.00

Unit

Name
Percent (%)

Target Date

27/02/2026

☒ Yes, the objective is reasonable and realistic.

6 You have unsaved changes.

Save Save and Close Close

1 **Name:** Here a short but meaningful name for the *Objective* is entered.

2 **GRC Perspective:** The Editor can select one or more GRC Perspectives for which they have creation permissions.

The number of GRC Perspectives displayed depends on the modules activated in BIG GRC:

3 **Description:** The *Objective* is documented and described in as much detail as possible so that other perspectives can also recognize a context or connection.

4 **Scope:** The *Objective* must be assigned to a scope.

The scope must be either a Business Structure or a Primary Asset.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request..](#)

5

SMART: The Editor can create the *Objective* according to the SMART definition. All components are available in the tab and can be interpreted as follows:

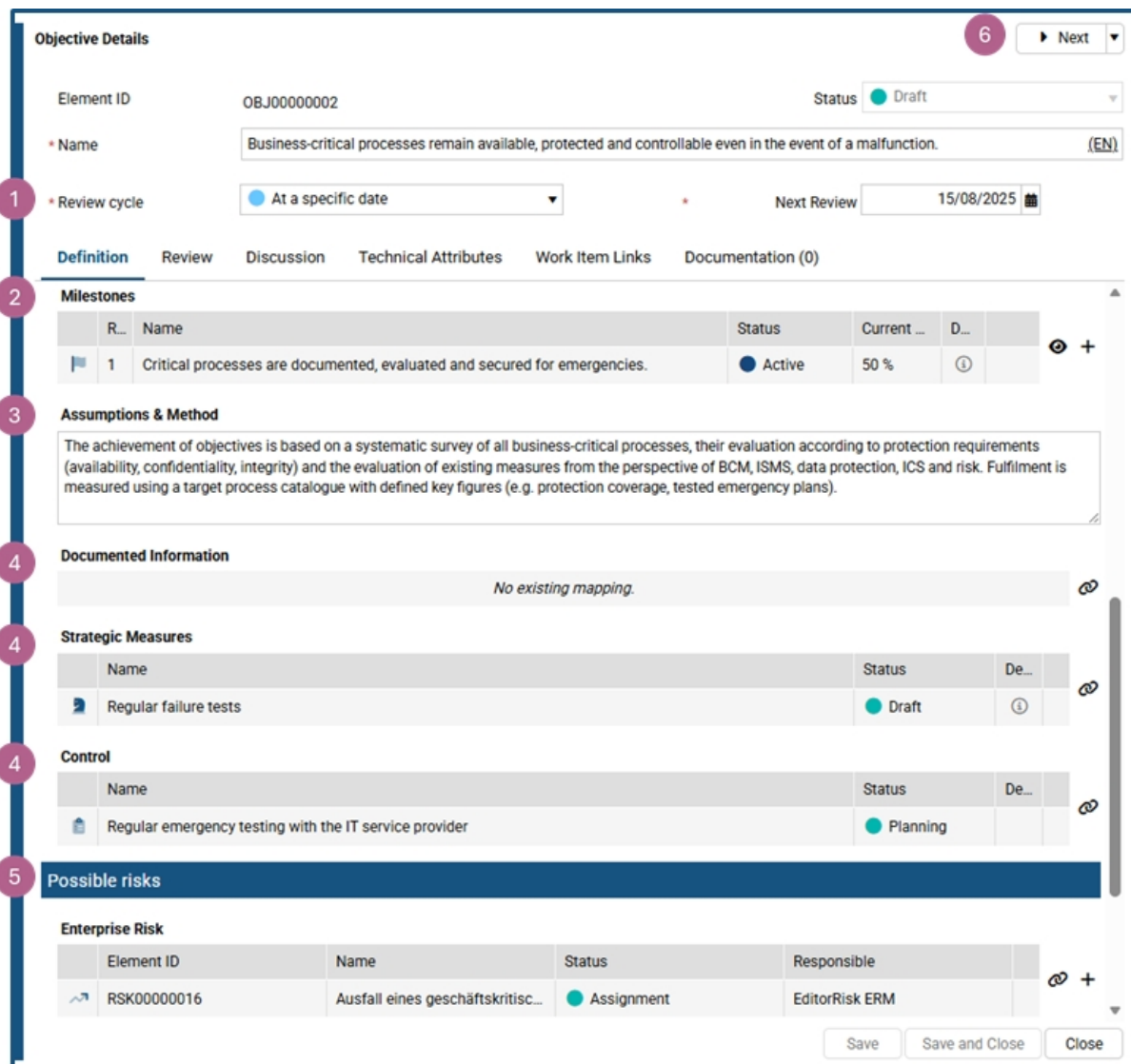
- Specific: Defined using the "Description" text field
- Measurable: Defined using the appropriate attributes with a specific "Key Performance" and a "Target Value"
- Appropriate: Determined using the "Yes, the objective is reasonable and realistic" checkbox
- Realistic: Conclusion reached using the "Yes, the objective is reasonable and realistic" checkbox
- Time-bound: Defined using the "Target Date"

6

Save: After entering the necessary information, the *Objective* can be saved for the first time.

During the save process, the Creator is automatically entered as the "Responsible."

Step 3: Enter Additional Information



Objective Details 6 [Next](#)

Element ID: OBJ0000002 Status: ● Draft

* Name: Business-critical processes remain available, protected and controllable even in the event of a malfunction. (EN)

1 * Review cycle: ● At a specific date * Next Review: 15/08/2025

Definition Review Discussion Technical Attributes Work Item Links Documentation (0)

2 **Milestones**

R...	Name	Status	Current ...	D...
1	Critical processes are documented, evaluated and secured for emergencies.	● Active	50 %	①

3 **Assumptions & Method**

The achievement of objectives is based on a systematic survey of all business-critical processes, their evaluation according to protection requirements (availability, confidentiality, integrity) and the evaluation of existing measures from the perspective of BCM, ISMS, data protection, ICS and risk. Fulfilment is measured using a target process catalogue with defined key figures (e.g. protection coverage, tested emergency plans).

4 **Documented Information**

No existing mapping.

4 **Strategic Measures**

Name	Status	De...
Regular failure tests	● Draft	①

4 **Control**

Name	Status	De...
Regular emergency testing with the IT service provider	● Planning	

5 **Possible risks**

Enterprise Risk

Element ID	Name	Status	Responsible
RSK00000016	Ausfall eines geschäftskritisc...	● Assignment	EditorRisk ERM

[Save](#) [Save and Close](#) [Close](#)

- 1 **Review Cycle:** The Editor enters a "Review Cycle." The Review Cycle specifies how often an *Objective* is switched back to "Draft" status in order to evaluate the *Objective* at regular intervals.

The "Next Review" attribute field is set automatically by BIC GRC.

- 2 **Milestones:** The Editor can define *Milestones* using the appropriate Work Item.

Milestones help the user better structure the *Objective* and also present interim results.

For more information, see [Editor Risk - Define & create Milestone](#).

- 3 **Assumptions & Method:** Stores additional information that is relevant to the development and underlying method of the *Objective*.
- 4 **Documented Information:** The Editor can establish a context for *Documented Information*, (Strategic) *Measures*, and *Controls*.

Both *Documented Information* and (Strategic) *Measures* and *Controls* can be linked and created outside of an *Objective*.

- 5 **Possible risks:** A reference to risks in BIC GRC can be established.

When an *Objective* is created from a risk type, the link to the respective risk is automatically filled in.

- 6 **Status change:** After all information has been entered, a status change to "Active" is executed in the upper right window.

Approval for the release of an *Objective* is not applicable.

Step 4: Perform update execution

The Editor should regularly review the *Objective* to ensure that it remains realistic and correct in its nature.

The "Next review" field supports this by allowing you to review at regular intervals. Two weeks before the date is reached, the Editor automatically receives a notification reminding them of the upcoming review.

On the day of the "Next Review," the *Objective* is switched from "Active" to "Draft" status, and the User automatically receives another notification.

The date is automatically reset after the status change depending on the time specified in "Review Cycle."

If the *Objective* has one of the review cycles "Every ... days," "Event-related," "Daily," or "Weekly," the status is not automatically reset and no automatic notification are sent to corresponding users..

2.5.5 Define & create Milestones

Objectives are often achieved through multiple steps or years. Therefore, it makes sense to structure *Objectives* using *Milestones* and set individual steps in order to ultimately achieve the overall *Objective*.

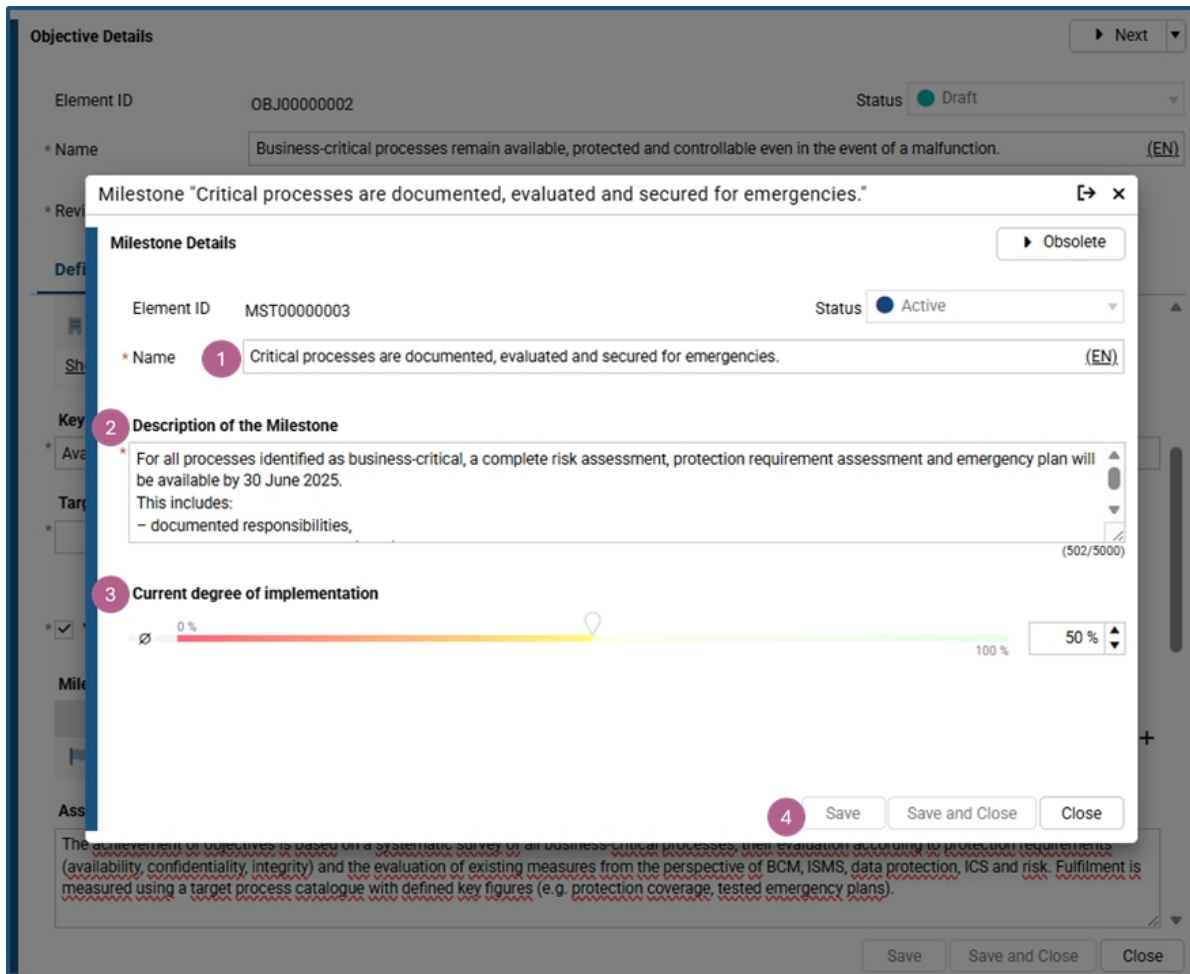
Step 1: Create a Milestone

A *Milestone* can only be created from the Work Item *Objective* by the responsible Editor. To create it, a new *Milestone* is created in the "Definition" tab in the "Objective" section using the  icon.

Milestones					
R...	Name	Status	Current ...	D...	
1	Critical processes are documented, evaluated and secured for emergencies.	Active	50 %	ⓘ	⊕

The *Milestone* is integrated into the Work Item *Objective* rather than opened in a new window.

Step 2: Define the Milestone



Objective Details

Element ID: OBJ00000002 Status: Draft

Name: Business-critical processes remain available, protected and controllable even in the event of a malfunction. (EN)

Milestone "Critical processes are documented, evaluated and secured for emergencies."

Milestone Details

Element ID: MST00000003 Status: Active

1 Name: Critical processes are documented, evaluated and secured for emergencies. (EN)

2 Description of the Milestone: 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, (502/5000)

3 Current degree of implementation: 0 % 100 % 50 %

4 Save Save and Close Close

- 1 **Name:** The first step should be to enter a short but meaningful name for the *Milestone*.
- 2 **Description of the Milestone:** The editor should describe the *Milestone* in as much detail as possible. Any information that ensures that the *Milestone* is relevant to the achievement of the *Objective* can be helpful here.
- 3 **Current Degree of Implementation:** Using a slider or direct input, the Editor can specify how far along the *Milestone* is in its implementation.

The value can be between 0 and 100%.

Each time the *Milestone* is changed, the *Objective* is automatically updated to ensure that the information between the Work Items remains consistent.

4

Save & Close: After clicking on the "Save" button, the Editor must specify a rank. This rank determines the order in which the individual *Milestones* should be processed in the workflow so that individual steps proceed in the correct sequence.

Should the rank change later or a new *Milestone* be added, BIC GRC recalculates the order depending on where the new rank has been entered.

In contrast to the "Active" statuses for other Work Items, the Editor can still make changes.

If the *Objective* is set to "Obsolete" status, the *Milestone* is also automatically set to "Obsolete" status.

After saving, the Editor can close the Work Item and continue with [Define & Create Objective](#).

2.5.6 dcaIdentify & Create Security Risk

Once a risk has been identified in the Data Protection domain, a new Work Item *Security Risk* can be created by the Editor.

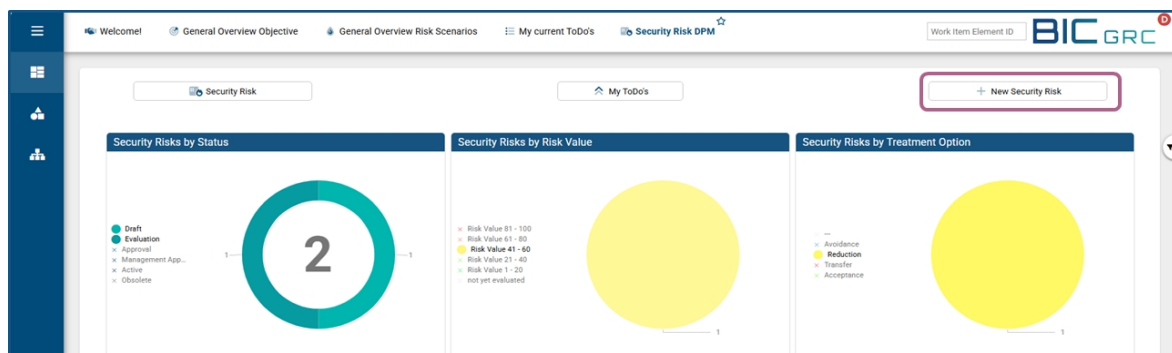
Step 1: Create Security Risk

The Editor can create *Security Risks* in several places in BIC GRC.

1. Creation via the "Security Risk" Dashboard

The editor navigates to **Dashboards >> Security Risk DPM >> "New Security Risk."**

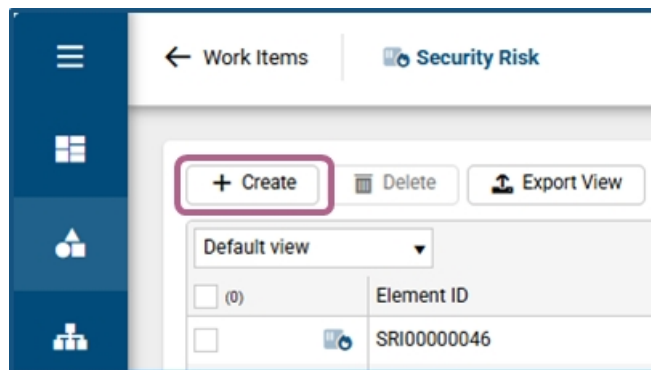
A new *Security Risk* is created using a button in the upper right corner of the window.



A new window will then open automatically.

2. Creation via Work Item list

The Editor navigates to **Work Items >> Security Risk >> "Create"**



Step 2: Enter details

Security Risk Details

Status Draft

Name

1 Failure of critical IT infrastructure at IT service provider (neutral)

Context

Details

2 Supporting Asset or Organizational Unit

Name	Asset Type	End-use...
4wheels Automotive Production GmbH	Business Structure	

3 GRC Perspective

Privacy Management

4 Editor

EditorRisk DPM (DPM_EditorRisk)

4 Approver

ApproverRisk DPM (DPM_Approver...)

5 Risk Description

Technical malfunctions, cyberattacks, or maintenance errors can cause central components such as servers, replication services, or network connections to fail at IT service providers. This impairs the availability of business-critical data and systems, making it impossible to carry out key processes (e.g., financial

(498/5000)

6 Risk Catalog

Element Name	Name
BSI_IT_BaselineProtection.G23	G 0.23 Unauthorized Access to IT-Systems

You have unsaved changes.

7 Save Close

1 **Name:** Here a short but meaningful name for the *Security Risk* is entered.

2 **Asset Assignment:** At this point, the Editor Risk can select either a "Supporting Asset" or a "Organizational Unit."

If the *Security Risk* is created via "2. Create via Asset Overview Links," the link to the asset is automatically set by BIC GRC.

Assets of the type "Primary Asset" are currently not supported by BIC GRC. The User will receive a notification when first attempting to save if a "Primary Asset" is stored.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request](#).

3

GRC Perspective: Since *Security Risks* can arise from three perspectives—Information Security Management, Data Protection, and Business Continuity—the person handling the Risk must specify the perspective from which the Risk arose.

When the other modules are activated, the *Security Risk* is also displayed from other perspectives and can be linked. The original perspective of a *Security Risk* remains fixed.

To make it easier for the Editor to select the correct perspective, there is a filter in the background that identifies their user profile on the Asset. Depending on their permissions, the Editor can thus be shown one or more perspectives for which the *Security Risk* should be created.

4

Responsible persons: The Editor must nominate an "Editor" to conduct the evaluation of the *Security Risk* and an "Approver Risk" who is responsible for the approval of the *Security Risk*.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

If the Editor is also the Creator, they enter themselves. This attribute remains unpopulated to accommodate *Security Risks* created by other Users.

Due to a stored filter, both the Editor and the Approver must be assigned to a specific user profile on the Asset in order to be displayed to the Creator.

If the Editor selects another user, editing rights are transferred after the first save operation.

To make it clear at a glance who created the *Security Risk*, the Creator is also

displayed in this section.

5 Risk description: Next, a description of the *Security Risk* is entered, whereby information on the causes and effect may also be of interest. All users who are downstream in the *Security Risk* workflow refer to this description, so it should contain as much necessary information and data as possible.

6 Risk Catalog: In addition, an assignment must be made to a category in the "Risk Catalog."

The Risk Catalog leads to the GRC frameworks of "BSI - Elementary Threat" and "Generic Risks."

7 Save: Once the information has been entered, the Editor can save the Risk.

The Editor can then proceed to the next step, [Add & analyze Security Risk](#).

2.5.7 Add & analyze Security Risk

A *Security Risk* can be identified and created by multiple Users.

If the Creator and the Editor are different users, the Editor is informed separately about the new *Security Risk* by means of a notification. The following steps 1 & 2 refer to the steps after creation by another user.

Optional step 1: Navigating to a specific Security Risk after external creation

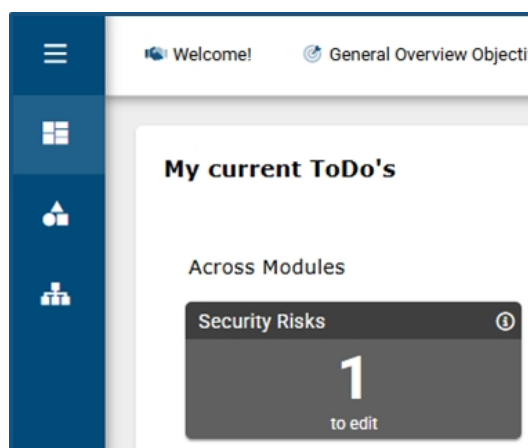
The Editor has two options for opening a *Security Risk* to be edited.

1. Open via notification

The Editor receives an E-Mail as soon as the Creator has completed all entries in the "NEW" status. The link to the specific *Security Risk* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status for which the Editor still has a task to complete.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Security Risk*. The Editor goes directly to the "Context" tab of the *Security Risk*.

Optional step 2: Reviewing the creator's entries

If the Creator and the Editor are different users, it is recommended to go to the "Context" tab in the *Security Risk* Work Item as a first step to view the Creator's detailed entries.

If the Creator's entries require clarification or further details, the Editor can leave a contribution in the "Discussion" tab. The Creator is then informed of the contribution via notification.

Step 3: Finalize assignment

The Editor responsible should regularly review the *Security Risk* to confirm that it remains current and correct.

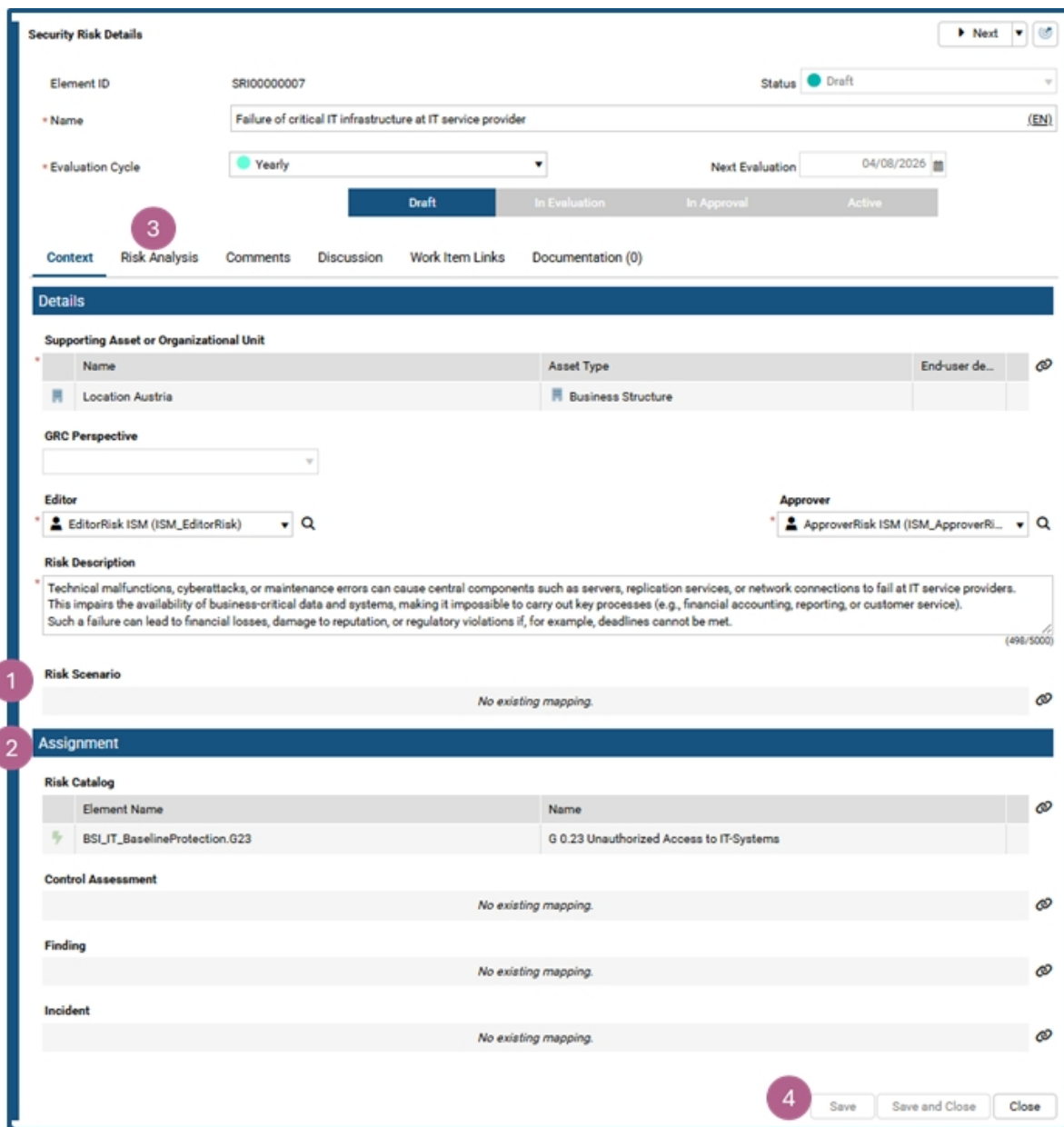
The "Next evaluation" field helps you to review this at regular intervals. Two weeks before the date is reached, the Editor automatically receives a notification reminding them of an upcoming evaluation.

On the day of the "Next Assessment," the *Security Risk* is switched from "Active" to "Evaluation" status, and the User is automatically sent another notification.

The date is automatically reset after the status change depending on the time specified in "Evaluation Cycle."

If the *Security Risk* has one of the review cycles "Every ... days," "Event-related," "Daily," or "Weekly," the system maintains the current status and the Editor receives a notification only when a status change occurs.

Step 4: Complete the entries



- Risk Scenario:** If the *Security Risk* is derived from a *Risk Scenario*, this link is automatically transferred from the *Risk Scenario* Work Item when it is created. Alternatively, the Editor can also link a *Risk Scenario* without direct derivation.

If a *Risk Scenario* is linked, an additional description field containing a *Risk Scenario* description taken from the *Risk Scenario* is displayed to the Editor under the "Risk Scenario" link.

The process is designed to link existing *Risk Scenarios* to *Security Risks*, and *Risk Scenarios* are expected to be defined in advance.

A filter has been stored for the assignment of *Risk Scenarios* so that the Editor only sees *Risk Scenarios* that have a suitable perspective and are in "Active" Status.

2 Assignment: The Editor can create links to other Work Items or Assessments.

Normally, these links are set automatically when the *Security Risk* is created from one of the Work Items or Assessments listed below.

- **Control Assessment:** The link to a specific Assessment is automatically filled in by BIC GRC if the *Security Risk* was created from a matching Assessment. If the *Security Risk* already existed before the Assessment, the "Control Assessment" can be linked afterwards.
- **Processing Activity:** "Processing Activities" should be linked by the Editor if they would be affected by the *Security Risk*.

Only processing activities with the status 'Active' are displayed to the Editor.

- **Finding:** If *Findings* lead to a *Security Risk*, they can be linked here.

Only *Findings* with the status "Treatment" or "Completed" are displayed to the Editor.

It is not intended that Control Assessments, *Findings* or *Processing Activities* from the *Security Risk* be created; instead, only a link from BIC GRC is permitted.

3 Optional step 4 – Risk Analysis

4 Status change: After all information has been entered, a status change to "Evaluation" is performed in the upper right window.

The Editor can then proceed to the next step, [Assess & evaluate Security Risk](#).

Optional - Step 5: Perform Risk Analysis

Management has the option of displaying a "Risk Analysis" tab for Users/Editors. The display is set centrally for all *Security Risks*.

Security Risk Details

Next

Element ID

SRI0000007

Status

● Draft

Name

Failure of critical IT infrastructure at IT service provider (EN)

Evaluation Cycle

● Yearly

Next Evaluation

04/08/2026

Draft

In Evaluation

In Approval

Active

Context

Risk Analysis

Comments

Discussion

Work Item Links

Documentation (0)

Risk Analysis

Possible Causes

- Technical malfunction at the service provider (e.g., hardware failure, cyberattack, power outage)
- Lack of redundancy or inadequate emergency planning on the part of the service provider
- Failure due to human error at the service provider
- Inadequate security measures or lack of infrastructure monitoring

Risk Types by Origin

Name	Catalog	End...	
Cybersecurity Risk	Risk Types		

Possible Consequences

- Critical business processes cannot be continued or can only be continued to a limited extent
- The availability of business-relevant information is not guaranteed
- Confidential data could be compromised if recovery is not secure
- Breaches of contract, damage to reputation, or financial losses due to SLA violations

Risk Types by Impact

Name	Catalog	End...	
Security Risk	Risk Types		

Affected Protection Requirements

Confidentiality

Availability

Select...

Affected stakeholders

Save

Save and Close

Close

- Possible cause** : In order to better assess and evaluate the *Security Risk*, it is sensical to carry out a Risk Analysis in advance.
The two text fields for "Possible Causes" and "Possible Consequences" allow the Editor to provide other Users with a better insight and impression.
- Risk Type by origin or Impact**: The two links to "Risk Type by origin" and "Risk Type by Impact" are intended to provide additional support to the Editor in classifying the *Security Risk*.

Only GRC Framework Items that have a tag matching the perspective are displayed.

If there is a suitable *Risk Scenario* that has filled in these two links, they are automatically transferred when the *Risk Scenario* is saved. If a link has already been created in the *Security Risk*, the existing entries for "Risk Type by origin" and "Risk Type by Impact" are preserved.

- 3 **Affected Protection Requirements:** This list attribute allows the editor to store CIA values (Confidentiality, Integrity, Availability) for the *Security Risk*.

This information is not transferred from the *Risk Scenario*.

- 4 **Affected stakeholders:** In the "Affected stakeholders" field, the Editor can enter which stakeholders they believe will be affected by this *Security Risk*.

Since this is a text field, this submission serves purely as information on the *Security Risk* and can be evaluated on dashboards, for example.

2.5.8 Assessing & evaluating Security Risks

After a *Security Risk* is identified and logged it can be supplemented and analyzed by an Editor Risk.

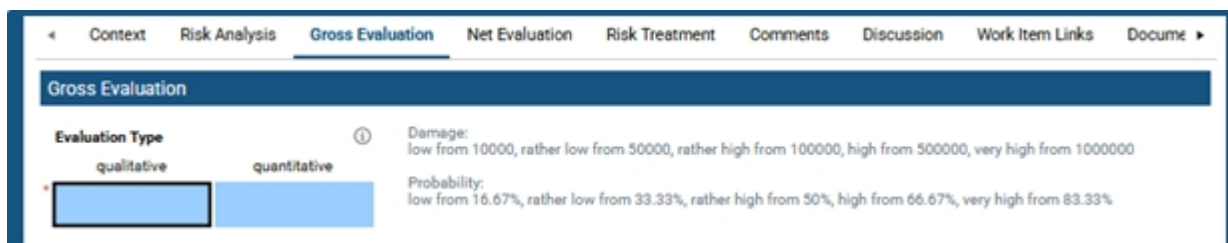
Step 1: Perform evaluation

Once the *Security Risk* has undergone the Status "Evaluation," the evaluation of the *Security Risk* can be started in the "Gross Evaluation" tab.

The Editor must select the appropriate Evaluation Method. There are two Evaluation Methods to choose from.

The following Evaluation Methods are available:

- (a) Qualitative
- (b) Quantitative



For the sake of readability, "Step 2: Perform Gross Evaluation," "Step 3: Perform Target Evaluation," and "Step 4: Perform Current Evaluation" are described depending on the Evaluation Method.

Step 2a: Perform qualitative Gross Evaluation

A qualitative risk assessment involves a **descriptive** rather than a **monetary** evaluation. In BIC GRC, this is performed as a 4x4, 5x5, or 6x6 heat map (also known as a risk matrix). The size of the heat map is determined in advance by management.

- 1 Gross Evaluation:** The Editor clicks on the heatmap to place an icon (G) in the value range where they believe the *Security Risk* lies, assuming no controls or *Measures* are in place.
- 2 Reason for the Evaluation:** The Editor must then enter a justification for this evaluation.
- 3 Save:** Once the information has been entered, the Editor can save the Risk.

Once the Editor has saved, another tab, "Net Evaluation," is displayed. The Editor must navigate to this tab for the next step.

- Once the Editor Risk has set the Target Evaluation icon (T) in the heat map, another tab, "Risk Treatment," is displayed.

- 3 **Risk Treatment:** The Editor now switches to the "Risk Treatment" tab.

The Editor then decides which treatment strategy he wants to use to achieve this Objective:

 - Avoidance: By choosing alternative solutions, attempts are made to circumvent the causes, e.g., using data protection-compliant tools.
 - Reduce: The risk is reduced by measures that influence both the causes and the effects, e.g., training employees to raise awareness of phishing and social engineering.
 - Transfer: A risk can be transferred by passing on liability or damages incurred to a third party, e.g., an insurance company.
 - Accept: When no measures are identified to efficiently or effectively avoid, reduce, or transfer a risk, the *Security Risk* is accepted.

The Editor can "accept" a *Security Risk* when it remains below the risk threshold specified by management. This threshold is displayed in the risk value bar.

If the Editor decides to "Accept," a description field becomes visible. The Editor can view existing links, and the system maintains their readability.

- 4 **Mitigating Controls:** The Editor should [derive & create](#) or link "Mitigating Controls" if they select the Treatment Strategy "Reduce" or "Transfer."

The editor can not link controls that are "Inactive" or "Obsolete".

- 5 **Mitigating Measures:** The Editor should [derive & create](#) "Mitigating Measures" when selecting the Treatment Strategy "Reduce" or "Transfer".

To map the actual impact of a measure on a *Security Risk*, the Editor must create a *Measure Evaluation*.

Links are not applicable.

Several *Measure Evaluations* can be created from the *Security Risk* for the mitigation of the *Security Risk*.

- 6 **Save:** Once the information has been entered, the Editor can save the *Security Risk*.

Once the Editor has saved, another tab, "Net Evaluation," is displayed. The Editor must navigate to this tab for the next step.

Step 4a: Perform a qualitative Current Evaluation

- 7 **Current Evaluation:** After entering the Risk Treatment, the Editor should return to the "Net Evaluation" tab and continue with the determination of the "Current Evaluation."

The Risk Editor should relate the "Current Evaluation" to the Gross Assessment and the *Measures* and *Controls* established so far. Depending on how effectively the *Measures* are already advancing toward the Target State, the icon (C) should be set in the heat map.

The Current Evaluation of the *Security Risk* is entered manually, as BIC GRC currently focuses on individual Measures and Controls.

- 8 **Reason for current evaluation:** A justification must then be entered to explain how the editor arrived at this current value.

- 9 **Status change:** After entering all the information, the status changes to "Approval" in the upper right window.

Step 2b: Perform quantitative Gross Evaluation

In the quantitative risk assessment, a monetary evaluation is performed. The evaluation is based on one specific value.

Security Risk Details ◀ Draft ▶ Next ▶

Element ID: SRI00000007 Status: Evaluation

* Name: Failure of critical IT infrastructure at IT service provider (EN)

Evaluation Cycle: Yearly Next Evaluation: 04/08/2026

Progress: Draft | **In Evaluation** | In Approval | Management Approval | Active

Risk Value: 0 to 100 (Scale with markers at 40.00, 55.00, 66.00)

☐ ERM relevant?

Context Risk Analysis **Gross Evaluation** Net Evaluation Comments Discussion Technical Attributes Work Item Links

Gross Evaluation

Evaluation Type: qualitative quantitative

1 **Probability** 0 % to 100 % (Slider) 62 %

2 **Damage** 0 to 4,000,000 (Slider) 2,900,000

3 **Reason for the Evaluation**
 * The IT service provider provides essential services for business-critical processes. A failure cannot be compensated for at short notice using the company's own resources. There is a risk of operational disruptions, data protection problems, and reputational damage. Due to the high level of dependency, both the probability of occurrence and the potential for damage are considered high. (388/5000)

4 Save Save and Close Close

1 **Probability:** Im ersten Schritt hat der Bearbeiter die Eintrittswahrscheinlichkeit zu bestimmen mit der das *Security-Risiko* auftreten kann.

2 **Damage:** A monetary value can be stored for the "Damage Potential."

The value can be set using the slider or entered manually in the number field.

The maximum value displayed in the slider is determined by management.

3 **Reason for Evaluation:** Next, a justification must be entered to explain how the editor arrived at this evaluation.

4 **Save:** Once the information has been entered, the Editor can save the Risk.

Once the Editor has saved, another tab, "Net Evaluation," is displayed. The Editor must navigate to this tab for the next step.

Step 3b: Perform quantitative Net Evaluation

Security Risk Details

Element ID: SRI00000007 Status: Evaluation 9

Name: Failure of critical IT infrastructure at IT service provider (EN)

Evaluation Cycle: Yearly Next Evaluation: 04/08/2026

Draft In Evaluation In Approval Management Approval Active

Risk Value: 0 40.00 55.00 66.00 100

☐ ERM relevant?

Context Risk Analysis Gross Evaluation **Net Evaluation** Risk Treatment Comments Discussion Technical Attributes

Net Evaluation

1 Target Probability: 0% 43%

Target Damage: 0 1,500,000

2 Reason for the Target Evaluation: The aim of the planned measure is to significantly reduce the probability of occurrence through redundancies, contracts with contingency provisions, and regular tests with the service provider. A residual risk remains due to the potential for damage if a failure does occur. (274/5000)

7 Current Probability: 0% 54%

Current Damage: 0 1,800,000

8 Reason for the Current Evaluation: Currently, there are no effective contractual or technical measures in place to ensure service availability in the event of a malfunction. There are no reliable emergency precautions or test procedures for emergencies. The high level of dependency remains unchanged. (266/5000)

Save Save and Close Close

- Once the Editor Risk has filled in the target values, another tab, "Risk Treatment," will open.

- 3 Treatment Strategy:** The Editor now switches to the "Risk Treatment" tab.

- Avoidance: By choosing alternative solutions, attempts are made to circumvent the causes, e.g., using data protection-compliant tools.
- Reduce: The risk is reduced by measures that influence both the causes and the effects, e.g., training employees to raise awareness of phishing and social engineering.
- Transfer: A risk can be transferred by passing on liability or damages incurred to a third party, e.g., an insurance company.
- Accept: When no measures are identified to efficiently or effectively avoid, reduce, or transfer a risk, the *Security Risk* is accepted.

The Editor can "accept" a *Security Risk* when it remains below the risk threshold specified by management. This threshold is displayed in the risk value bar.

If the Editor decides to "Accept," a description field becomes visible. The Editor can view existing links, and the system maintains their readability.

- 4 **Mitigating Controls:** The Editor should [derive & create](#) or link "Mitigating controls" if they select the Treatment Strategy "Reduce" or "Transfer."

The editor can not link controls that are "Inactive" or "Obsolete".

- 5 **Mitigating Measures:** The Editor should [ableiten & erstellen](#) "Mitigating Measures" when selecting the Treatment Strategy "Reduce" or "Transfer".

To map the actual impact of a *Measure* on a *Security Risk*, the Editor must create a *Measure Evaluation*.

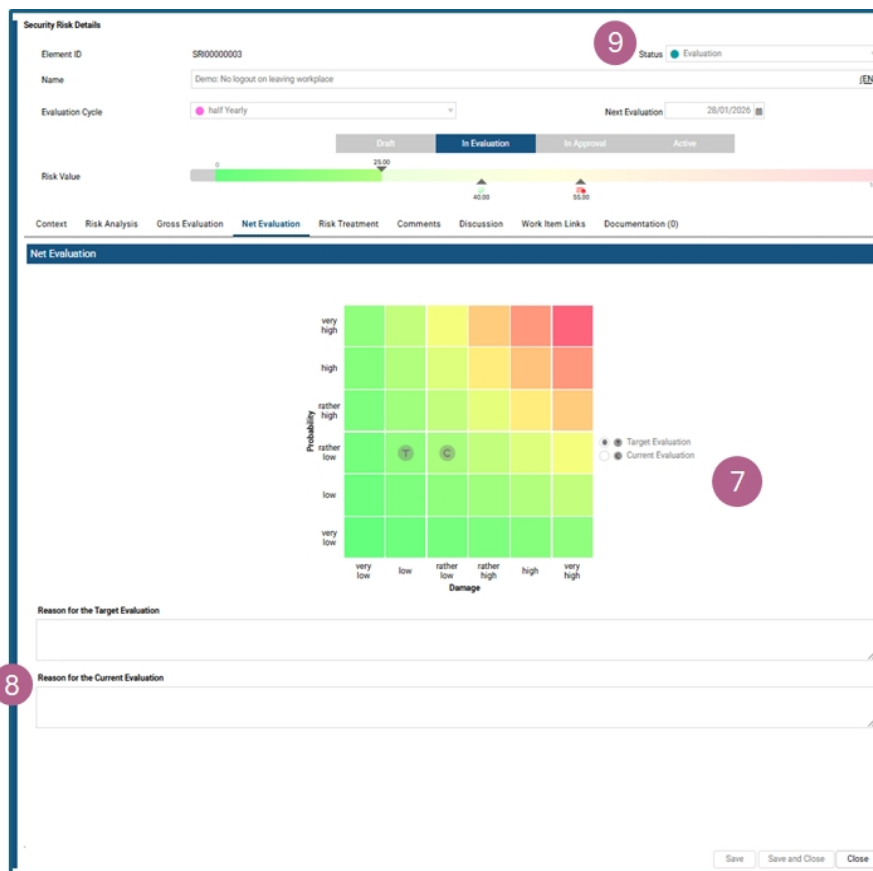
Links are not applicable.

Several *Measure Evaluations* can be created from the *Security Risk* to mitigate the *Security Risk*.

- 6 **Save:** Once the information has been entered, the Editor can save the Risk.

Once the Editor has saved, another tab, "Net Evaluation," is displayed. The Editor must navigate to this tab for the next step.

Schritt 4b: Perform Quantitative Target Evaluation



7 Current Evaluation: After Risk Treatment, the editor should return to the "Net Evaluation" tab and continue with the determination of the "Current Evaluation."

The Risk Editor should set the "Current Evaluation" in relation to the Gross Assessment and the *Measures* and *Controls* set so far. Depending on how far the *Measures* are already effective in achieving the Target State, the values for Probability of Occurrence and Damage Potential should be specified in the Current Evaluation.

8 Reason for the current evaluation: Subsequently, a justification must be entered explaining how the Editor arrived at this current value.

9 Status change: After all information has been entered, the execution of a status change to "Approval" is performed in the upper right window.

The next status is performed by [Approver Risk - review & approve Security Risk](#). The entered Approver Risk is informed of the status change by means of a notification.

After entering all necessary information, the Work Item can be saved and a status transition can be performed before closing the window.

2.5.9 Derive & create Measure Evaluation

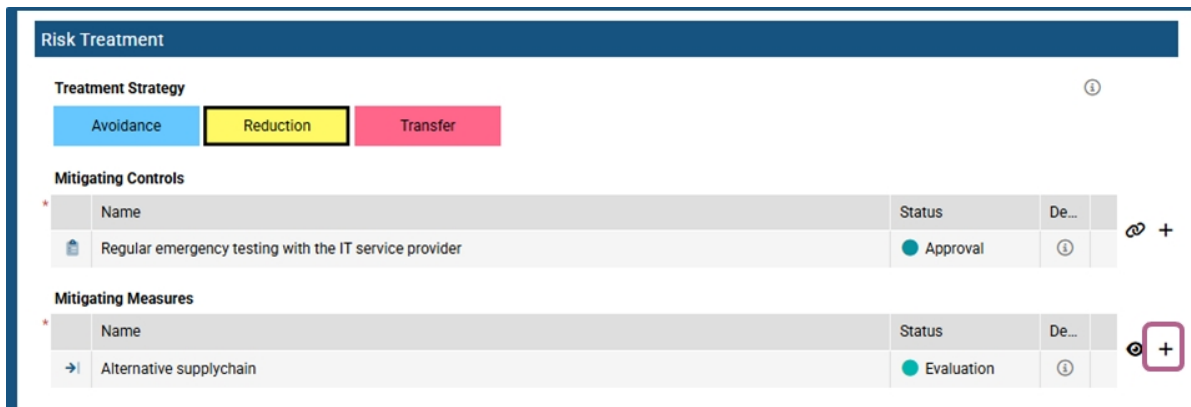
After a *Security Risk* has been created, *Measures* are used to mitigate the *Security Risk*. To efficiently utilize existing measures across multiple Risks, it is possible to use *Measure Evaluation* to establish a connection between a *Security Risk* and *Measures* that are used multiple times.

A *Measure Evaluation* determines the actual impact of a measure on a specific *Security Risk*.

Step 1: Create a Measure Evaluation

The *Measure Evaluation* can be created exclusively by the responsible Editor from the *Security Risk* Work Item. The system allows creation of a *Measure Evaluation* as long as in the Risk Treatment Section, "Accept" is not selected as the Treatment Strategy.

A new *Measure Evaluation* can be created in the "Treatment" tab in the link to the *Measure* using the icon .

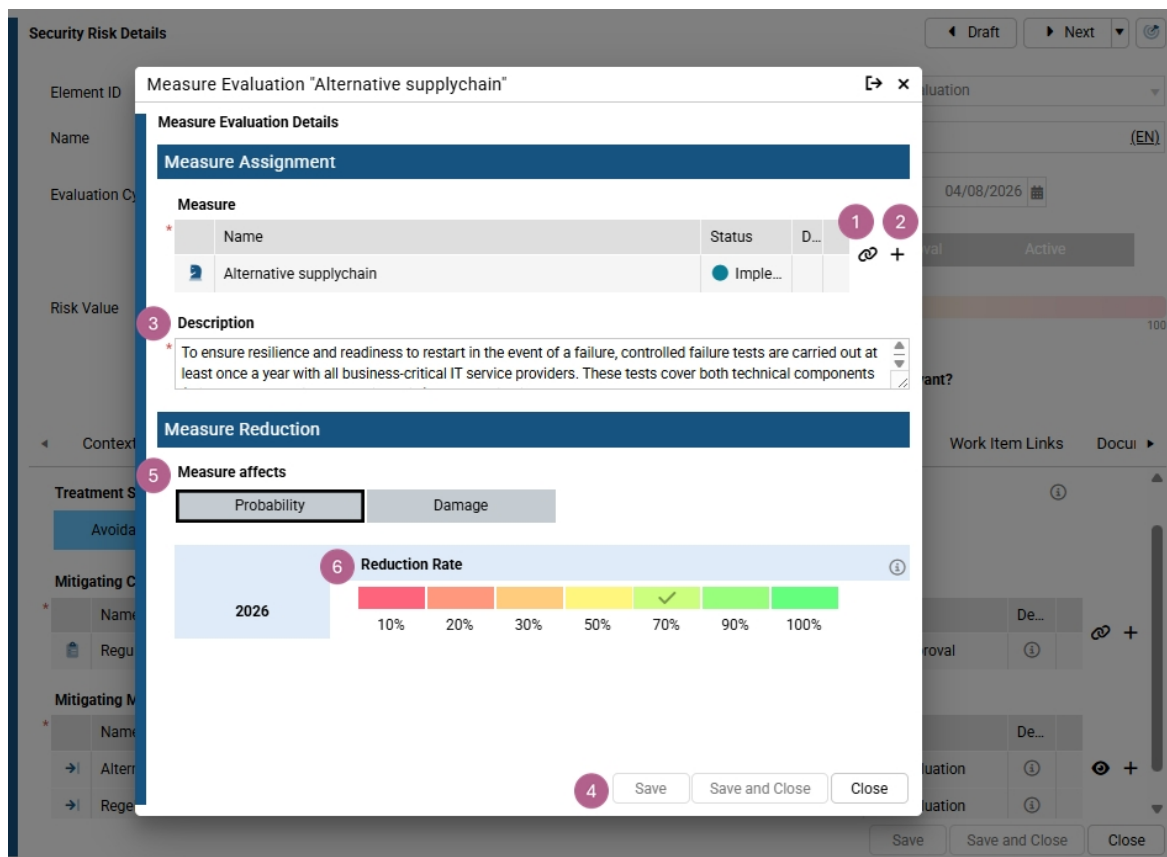


The screenshot shows the 'Risk Treatment' section of a system. It includes a 'Treatment Strategy' section with buttons for 'Avoidance', 'Reduction' (highlighted), and 'Transfer'. Below this is a 'Mitigating Controls' table with one row: 'Regular emergency testing with the IT service provider' with a status of 'Approval'. At the bottom is a 'Mitigating Measures' table with one row: 'Alternative supplychain' with a status of 'Evaluation'. To the right of the 'Alternative supplychain' row, there is a plus icon inside a square box, indicating where to click to create a new measure evaluation.

Risk Treatment			
Treatment Strategy Avoidance Reduction Transfer			
Mitigating Controls			
Name	Status	De...	
Regular emergency testing with the IT service provider	Approval		
Mitigating Measures			
Name	Status	De...	
Alternative supplychain	Evaluation		

The *Measure Evaluation* is integrated into the *Security Risk* rather than opened in a new window.

Step 2: Assign measure



Measure Evaluation "Alternative supplychain"

Measure Evaluation Details

Measure Assignment

Name	Status	D...
Alternative supplychain	Imple...	

Description

To ensure resilience and readiness to restart in the event of a failure, controlled failure tests are carried out at least once a year with all business-critical IT service providers. These tests cover both technical components

Measure Reduction

Measure affects

Probability Damage

Reduction Rate

2026

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

Save Save and Close Close

- 1 **Link Measure:** The Editor must link a Work Item of the *Measure* type , that should mitigate the specific *Security Risk*.
- 2 **Create Measure:** If a suitable *Measure* is still required, it can be created using the icon . Mehr dazu unter [Editor Risk - Define & Create Measure](#).
- 3 **Description:** Next, document why and how the *Measure* affects the *Security Risk* in the description field below.
- 4 **Save:** The *Measure Evaluation* can then be saved so that further attribute fields are displayed.

Each *Measure Evaluation* can only be linked with exactly one *Measure*.

Step 3: Document the effect of the measure

- 5 **Effect:** Once a *Measure* has been linked, the Editor can specify whether the *Measure* affects the "Probability" of Occurrence or the Amount of "Damage".
- 6 **Reduction rate:** Once the *Measure Evaluation* has been saved, a heat map relating to the reduction becomes visible. The more the specific *Measure* affects the *Security Risk*, the higher the reduction rate should be selected.

Step 4: Next steps

Once the reduction rate has been entered, the *Measure Evaluation* can be saved again and closed.

If the *Measure Evaluation* is unlinked, it is immediately removed from the system, ensuring that no "orphaned" entries remain.

When the *Security Risk* is set to "Obsolete" , the *Measure Evaluation* is also set to "Obsolete." The same behavior occurs when the *Measure* is set to "Obsolete" status.

Back to the step [Editor Risk - Assess & Evaluate Security Risk](#).

2.5.10 Identify & create Measure

A *Measure* can be created by an Editor Risk and used as part of Risk Treatment.

By creating and performing the assignment of a *Measure* to an asset in the asset hierarchy, a *Measure* can be selected and linked from multiple domains in BIC GRC. This makes measure management a material part of BIC GRC.

Step 1: Create a Measure from a Measure Evaluation

The *Measure* can be created by an Editor from a *Security Risk* or a *Measure Evaluation* by clicking on the  icon in the *Security Risk* and then in the *Measure Evaluation*.

Step 2: Enter details

Measure Details

Element ID

Draft

Name

1 Regular failure tests for business-critical IT service providers (EN)

Details

Details

2 Scope

Name	Asset Type	End-us...
Group	Business Structure	

3 GRC Perspective

Privacy Management

4 Editor

EditorMeasure

4 Approver

ApproverMeasure

5 Type of Measure

Organizational Measure

6 Priority of Measure

Very Low

Low

Rather Low

Rather High

High

Very High

7 Description of Measure

Planned and recurring execution of failure tests (blackout simulations, recovery exercises, switchover tests) for all external IT service providers classified as business-critical.
The aim is to demonstrate actual capacity to act in the event of IT failures, identify weaknesses, and remedy them in a targeted manner.

You have unsaved changes.

Save

Save and Close

Close

1 **Name:** The Editor should enter a short but meaningful name for the *Measure*.

2 **Scope:** To limit the scope of a *Measure*, it must be assigned to an asset in the Asset Hierarchy.

If a *Measure* should apply only to Location A, the scope "Location A" must be selected in the Asset link. If the *Measure* is linked again later in BIC GRC, it will be displayed only to users with permissions in Location A, and Users managing Assets in Location B will see only the *Measures* relevant to that location.

3 **GRC Perspective:** The Perspective is automatically taken from the *Measure Evaluation* and set. It is fixed after the first save operation.

4 **Responsibilities:** The Editor specifies an Editor and an Approver who will be responsible for implementing the *Measure*.

Both users can only be entered once an Asset has been assigned in ². An internal ensures both the Editor and the Approver are match a specific user profile on the Asset in order to be displayed to the creator.

The initial Creator of this *Measure* is also displayed in this section so that it is clear at a glance who created the *Measure*. If the Editor is also the Creator, they can enter themselves. This attribute remains empty until the *Measure* is created, allowing for flexibility when a *Measure* is created by another User.

5 Type of Measure: The Editor can use the type of *Measure* to specify a category for the *Measure*.

6 Priority of Measure: For a *Measure*, the Editor must specify the "Priority" with which the *Measure* is to be implemented and the "Type of Measure" it is. These two criteria can be used later for evaluation on dashboards, and they influence the workflow in this way.

7 Description of Measure: The *Measure* should be described and defined as precisely as possible in order to give users who are downstream in the workflow an overview of the task involved in the *Measure*.

Once all information has been submitted, the *Measure* can be saved.

After saving, the assigned Editor Measure is notified via notification.

The Creator can make no further changes to the *Measure* after saving. If there are any additions, these can be discussed using the "Discussion" tab.

After saving, the Work Item can be closed. The user may continue with [Derive & Create Measure Evaluation](#) or [Assess & Evaluate Security Risk](#).

2.5.11 Derive & create Control

The Editor Risk can define not only *Measures* in a *Security Risk* but also appropriate *Controls*.

For example, in the case of a *Security Risk* related to fire, it makes sense to implement the *Measure* "Place fire extinguishers" and also add the appropriate semiannual *Control* "Review fire extinguishers."

Step 1: Create Control from Security Risk

The editor can create a control directly from a *Security Risk* with the Status "Net Evaluation" by clicking on the icon "✚" in the *Security Risk*.

Step 2: Enter details

Control Details

Status: Planning

* Name 1 Regular emergency testing with the IT service provider (EN)

Assignment

Details

2 **Scope**

Name	Asset Type	End-use...
MusterKonzern AG	Business Structure	

3 **GRC Perspective**

* Privacy Management ☒ relevant for Privacy Management

4 **Editor**

* EditorControl

Approver

* ApproverControl

5 **Level of Control**

* Entity Level Control

6 **Type of control**

* Keycontrol

7 **Description of the control**

* Regular execution of planned emergency tests in collaboration with the IT service provider to verify the effectiveness of recovery procedures, escalation paths, and communication processes in case of an incident, and to identify areas for improvement.

8 You have unsaved changes. Save Close

1 **Name:** The User who is creating the *Control* should enter a short but meaningful name.

2 **Scope:** To define the scope of the *Control*, it must be assigned to an Asset in the Asset Hierarchy.

3 **GRC Perspective:** The Perspective is automatically taken from the *Security Risk* and set.

The GRC Perspective remains fixed after the first save operation.

4 **Responsible persons:** The Editor specifies an "Editor Control" and an "Approver Control" responsible for implementing the *Control*.

Due to a stored filter, both the Editor and the Approver must be assigned to a specific

user profile on the Asset in order to be displayed to the Creator.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

The Creator is also displayed in this section so that it is clear at a glance who created the *Control*. If the Editor is also the Creator, they can enter themselves. This attribute is always to be entered manually rather than automatically from the system to accommodate *Controls* created by other Users.

- 5 **Level of Control:** The Level of Control should indicate whether the *Control* is specified by management or has been created individually.
- 6 **Type of Control:** The Editor Risk can determine whether the *Control* is managed as a "Key Control" or as a "Supporting Control" if, for example, *Control Testing* has identified that additional *Measures* are needed to enhance the existing "Key Control" and fully meet a requirement.
- 7 **Description of the control:** In the description of the *Control*, the Editor Risk should specify as clearly as possible what they expect from the *Control* and what purpose it serves.
- 8 **Save:** Once all information has been entered, the *Control* can be saved.

After saving, the assigned Editor Control is notified via a notification.

After saving, the Creator can discuss any further additions in the "Discussion" tab.

After saving, the Editor can close the Work Item and continue with [Security Risk Assessment & Evaluation](#).

2.5.12 Implementation & review of Objectives

Objectives are typically achieved over a longer time horizon rather than within a short period of time.

For this reason, when creating the Work Item *Objective*, the Editor specifies a Review Cycle during which the *Objective* is reviewed again to check its relevance and progress.

Step 1: Navigate to the Objective

The Editor Risk automatically receives a reminder E-Mail from BIC GRC two weeks before the next review.

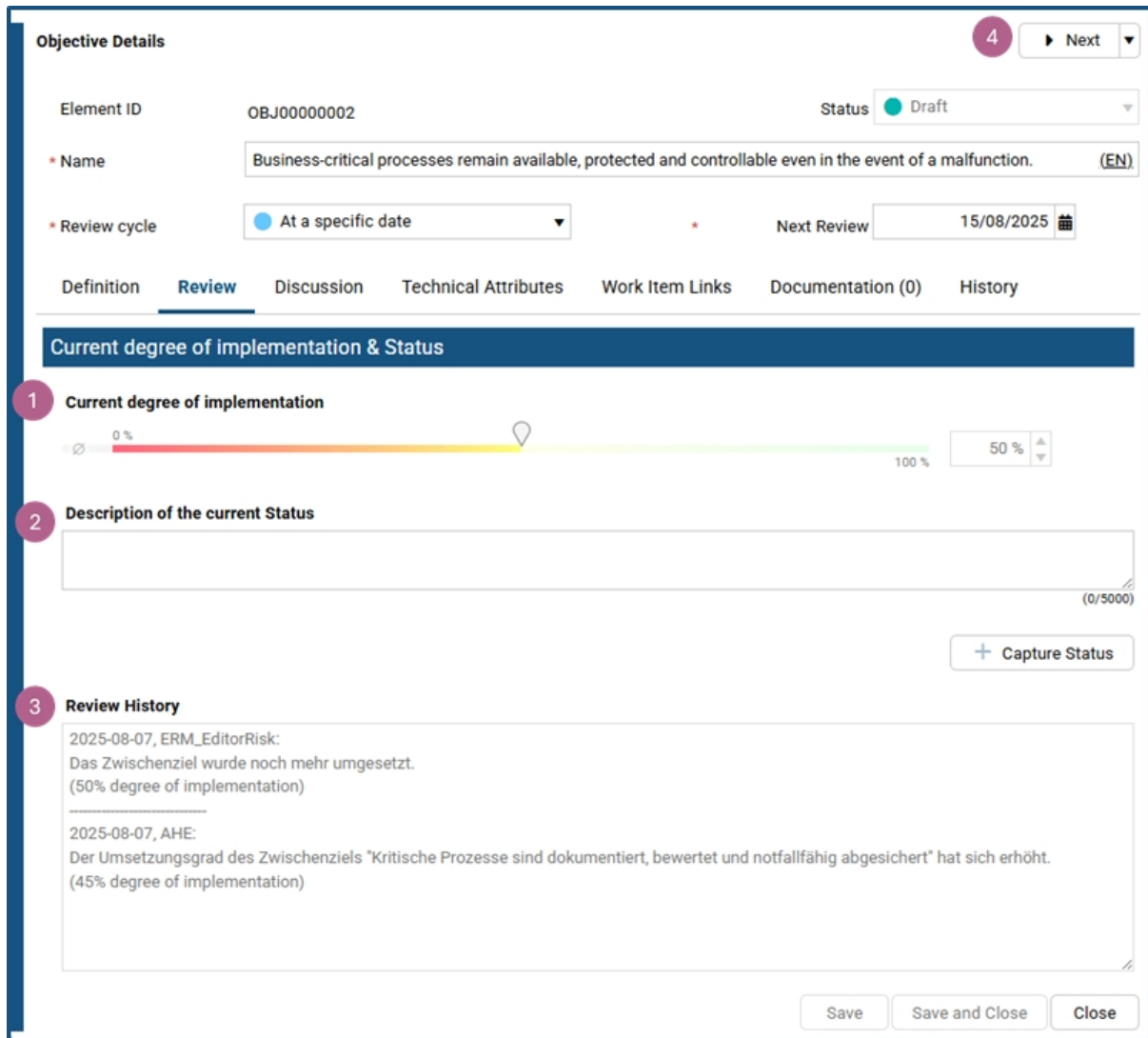
On the day the date is reached, the Status is automatically changed to "Draft" and the Editor receives another E-Mail. The link to the specific *Objective* is included in the notification.

Step 2: Evaluate Milestones

The Editor should begin the review by looking at the *Milestones*.

The Editor can edit the *Milestones* created so far and record the current Degree of Implementation of the *Milestone*.

Step 3: Perform review



Objective Details 4 ▶ Next ▼

Element ID: OBJ00000002 Status: ● Draft

* Name: Business-critical processes remain available, protected and controllable even in the event of a malfunction. (EN)

* Review cycle: ● At a specific date * Next Review: 15/08/2025

Definition **Review** Discussion Technical Attributes Work Item Links Documentation (0) History

Current degree of implementation & Status

1 **Current degree of implementation**

0 % 100 % 50 % ▲ ▼

2 **Description of the current Status**

(0/5000)

[+ Capture Status](#)

3 **Review History**

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)

[Save](#) [Save and Close](#) [Close](#)

- 1 **Current degree of implementation:** The current Degree of Implementation is automatically determined as the average of all *Milestones*.
- 2 **Description of the current status:** To better measure progress, the Editor can register the current status. Using the "Register status" button, the entered text is added to the "Review history" with the current date
- 3 **Review history:** The "Review history" is an update feed where the Editor enters the current Status of the *Objective* and other authorized persons can get an idea of the progress of the *Objective*.
- 4 **Status change:** After all information has been entered, the status is changed to "Active" in the upper right window.

2.6 Approver Risk

The *Approver Risk* user profile consists of all risk approvers who are active throughout the Company. The *Approver Risk* user profile allows for different Risk Approvers to manage an individual *Security Risk* between multiple Business Units, Processes, or Supporting Assets within the Company.

An Approver Risk has the following tasks in BIC GRC:

- [Review & approve a Security Risks](#)

The Approver Risk can also create other Work Items in BIC GRC. While this is not their primary task, we will refer to other user profiles at this point:

- [Identify & create a Threat](#)
- [Identify & create a Vulnerability](#)
- [Derive & create a Risk Scenario](#)
- [Identify & create a Security Risk](#)
- [Derive & create a Control](#)
- [Define & create an Objective](#)
- [Define & create a Milestone](#)

These processes involve simply creating and entering the most important information to initiate a designated workflow for a Work Item. As soon as the Approver Risk saves a Work Item for the first time, the right to edit it is then transferred to the assigned Editor, who is automatically notified of their assignment. The Approver Risk can add further remarks to their initial information in the "Discussion" tab.

2.6.1 Review & approve Security Risk

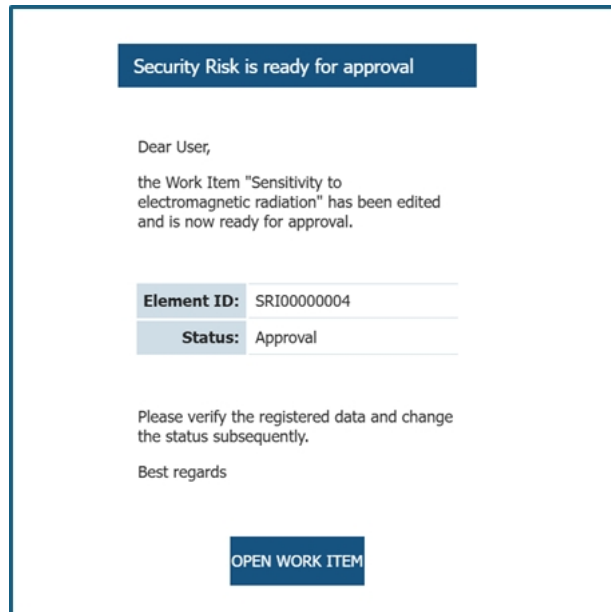
A *Security Risk* is created and evaluated by the Editor Risk. Once the evaluation has been completed and reviewed, a *Security Risk* can be passed on to the Approver Risk by changing the status to "Approval."

Step 1: Navigate to specific Security Risk

The Approver Risk has two options for opening a *Security Risk* to be approved.

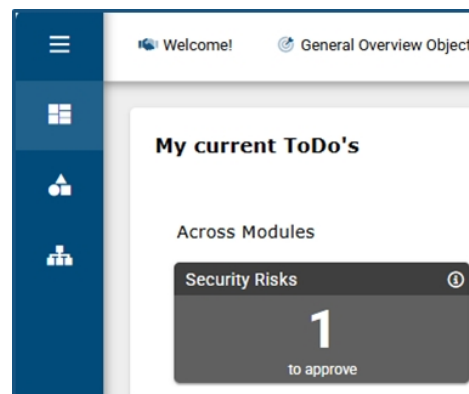
1. Open via notification

The Approver Risk receives an E-Mail as soon as the Editor Risk has completed all entries in the "Treatment" status. The link to the specific *Security Risk* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" Dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Approver Risk can approve.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Security Risk*.

Step 2: Perform review

The Approver Risk has full read access to the evaluated *Security Risk* in order to decide, based on the information entered, whether the *Security Risk* has been correctly classified, evaluated, and handled in terms of gross and net evaluation.

If further refinement is needed from the Approver's perspective, the Approver can add a Comment in the "Comment" tab and change the status to "Evaluation."

Security Risk Details

◀ Evaluation

▶ Active

Element ID

SRI00000012

Status

Approval

Name

Failure of critical IT infrastructure at IT service provider

(EN)

Evaluation Cycle

Yearly

Next Evaluation

26/08/2026

Draft

In Evaluation

In Approval

Active

Risk Value

0

33.00

40.00

55.00

100

ERM relevant?

☐

◀ Context

Risk Analysis

Gross Evaluation

Net Evaluation

Risk Treatment

Comments

Discussion

Work ▶

Comments

Comment

Enter your comment here.

(0/1000)

Add Comment

All Comments

2026-01-22, S03, BCM_ApproverRisk:

Könntest du bitte die Beschreibung noch klarer formulieren.

Save

Save and Close

Close

If the *Security Risk* is particularly high or if the *Security Risk* relates to a core process, for example, the Approver Risk can click the "ERM-relevant" checkbox in the "Approval" status.

The checkbox is only displayed if the Enterprise Risk module is also active. The ERM Executive is informed of the marking by means of a notification.

Step 3: Perform status transition execution

If the entries made by the upstream user are correct, the Approver Risk can switch the status to "Active" if Management Approval is not required.

The Creator of the *Security Risk* and Editor Risk are notified of the status change to "Active" by means of a notification.

The responsible management is notified of the status change to "Management Approval" via a notification.

After the status transition, the window can be closed.

2.7 Editor Measure

The Editor Measure is responsible for creating and implementing one or more specific *Measures* in the Company. Their task is to register, plan, implement, and document the continuous progress of the *Measure* in BIC GRC.

An Editor Measure in BIC GRC has the following tasks:

- [Define & create a Measure](#)
- [Add & edit a Measure](#)
- [Set up & plan a Measure](#)
- [Manage & implement a Measure](#)
- [Optional: Review & improve a Measure](#)
 - [Identify & create Findings](#)
 - [Review & address Findings](#)

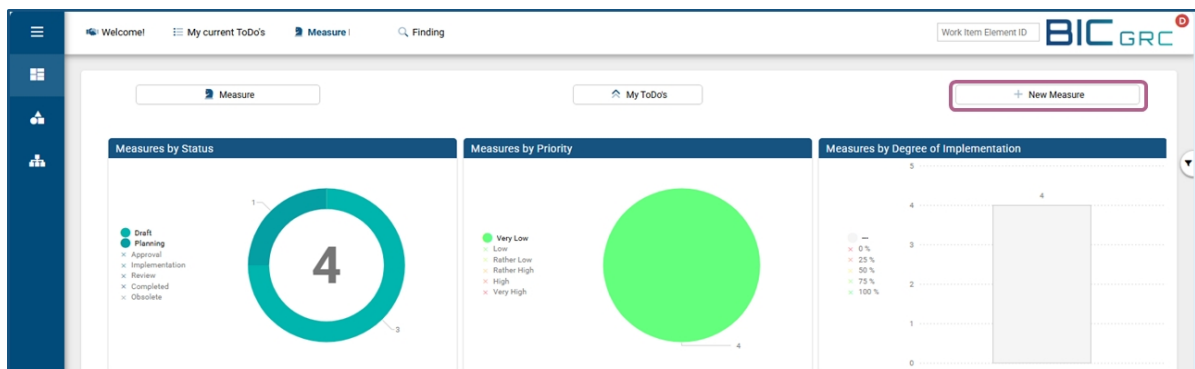
2.7.1 Define & create Measures

A *Measure* can be created by multiple user profiles from different modules and for different reasons. By creating and assigning a *Measure* to an asset in the asset hierarchy, it can be selected and linked by multiple modules in BIC GRC. This makes *Measure* management a crucial part of BIC GRC.

Step 1: Create Measure

1. Creation from Dashboard

The *Editor Measure* navigates to **Dashboards >> Measure Overview >> "New Measure."**

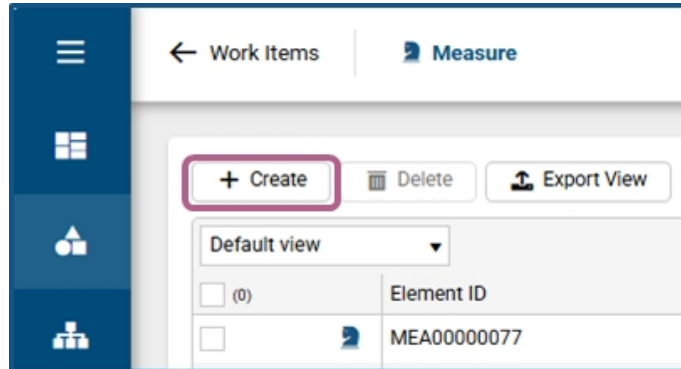


2. Creation from other Work Items

Measures can result from various Work Items, such as Risks, Findings, or Management Reviews. They are created via a corresponding link with the heading "Measure" using the icon **+** or they are linked using .

3. Creation via Work Item List

The *Editor Measure* navigates via the sidebar to **Work Items >> Measure >> "Create."**



Step 2: Enter details

Measure Details

Element ID

Draft

Name

1 Regular failure tests for business-critical IT service providers (EN)

Details

Details

2 Scope

Name	Asset Type	End-us...
Group	Business Structure	

3 GRC Perspective

Privacy Management

4 Editor

EditorMeasure

4 Approver

ApproverMeasure

5 Type of Measure

Organizational Measure

6 Priority of Measure

Very Low

Low

Rather Low

Rather High

High

Very High

7 Description of Measure

Planned and recurring execution of failure tests (blackout simulations, recovery exercises, switchover tests) for all external IT service providers classified as business-critical. The aim is to demonstrate actual capacity to act in the event of IT failures, identify weaknesses, and remedy them in a targeted manner.

You have unsaved changes.

Save

Save and Close

Close

- 1 Name:** The first step should be to enter a short but meaningful name for the *Measure*. The *Measure* is unique under the "Name" in combination with the "Element ID."
- 2 Scope:** To define the scope of the *Measure*'s display availability, it must be assigned to an asset in the asset hierarchy.

Only assets of the type "Business Structure" are permitted.

If, for example, a *Measure* should apply exclusively to Location A, the scope "Location A" must be selected in the asset link. If the *Measure* is relinked later in BIC GRC, it will be displayed only to users with permissions in Location A. Users managing Assets in Location B will see only the *Measure* relevant to that location.

- 3 **GRC Perspective:** After selecting the scope, the User is shown the list of GRC Perspectives. The Editor can select one or more GRC Perspectives for which they have creation permissions.

The number of GRC Perspectives displayed depends on the modules that have been activated.

- 4 **Responsibilities:** The Creator must specify an "Editor Measure" who is responsible for the implementation, evaluation, and implementation of the *Measure*.

Furthermore, an "Approver Measure" must be nominated to approve the *Measure*..

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

Due to a stored filter, both the Editor and the Approver must be assigned to a specific user profile on the Asset in order to be displayed to the Creator.

It is recommended that the Creator of the Work Item also serves as the "Editor Measure" of a *Measure*.

- 5 **Type of Measure:** The Editor can use the type of *Measure* to specify a category for the *Measure*.

- 6 **Priority of Measure:** For a *Measure*, you must specify the "Priority" with which the *Measure* is to be implemented.

- 7 **Description of Measure:** The *Measure* should be described and defined as precisely as possible in order to give users downstream an overview of what the *Measure* entails.

- 8 **Save:** Once all information has been submitted, the *Measure* can be saved.

If the Creator of the *Measure* is also the Editor Measure, they can continue with the next step, [Editor Measure - Add & edit Measure](#).

2.7.2 Add & edit a Measure

A *Measure* can be identified and created by multiple Users.

If the Creator and the Editor are different users, the Editor is informed separately about the new *Measure* by a notification. The following steps 1 & 2 refer to the activities after creation by a separate user.

Optional step 1: Navigating to a specific Measure after external creation

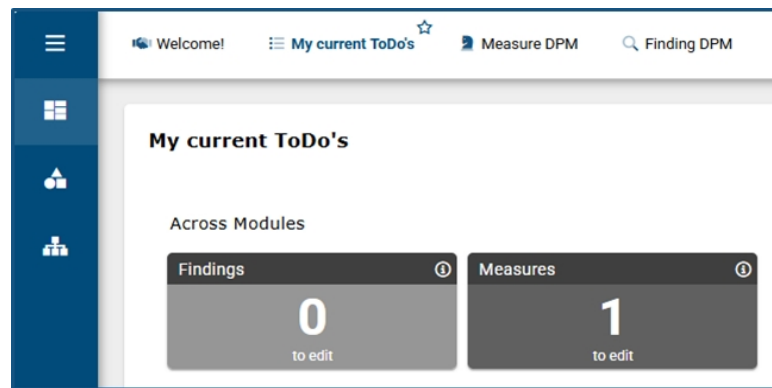
The Editor has two options for opening a *Measure* to be edited.

1. Open via notification

The Editor receives an E-Mail as soon as the Creator has completed all entries in the "NEW" status. The link to the specific *Measure* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

At the top of the "My current To-Do's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Editor can complete.

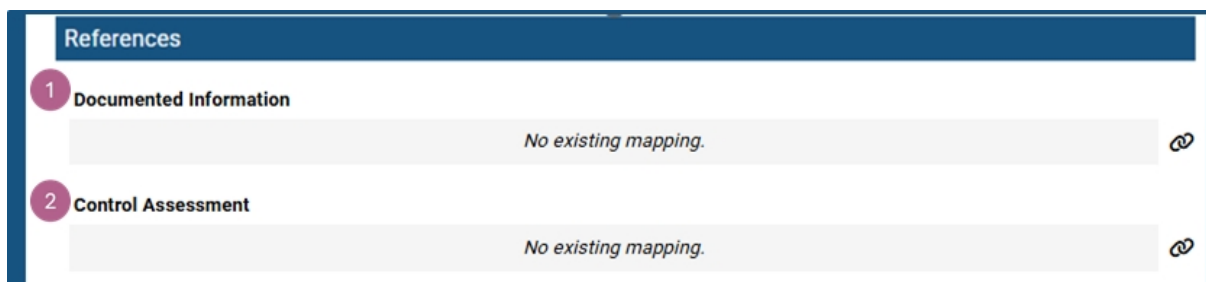


Optional step 2: Reviewing the creator's entries

If the Creator of a *Measure* and its Editor are different Users, it is recommended to review the "Details" tab in the Work Item *Measure* to ensure the Creator's detailed entries are correct.

If the Creator's entries require clarification or further details, the Editor can leave a comment in the "Discussion" tab. The Creator will then be informed of the contribution via notification.

Step 3: Add entries



- 1 **Documented Information:** The Editor Measure can store one or more pieces of *Documented Information*.

Documented Information helps improve efficiency and traceability, especially in the area of information security, but can also make a contribution to creating transparency in other modules.

- 2 **Control Assessment:** The link to a specific Assessment is automatically filled in by BIC GRC if the *Measure* was created from a suitable Assessment. If the *Measure* already existed before the Assessment, the "Control Assessment" can be linked afterwards.

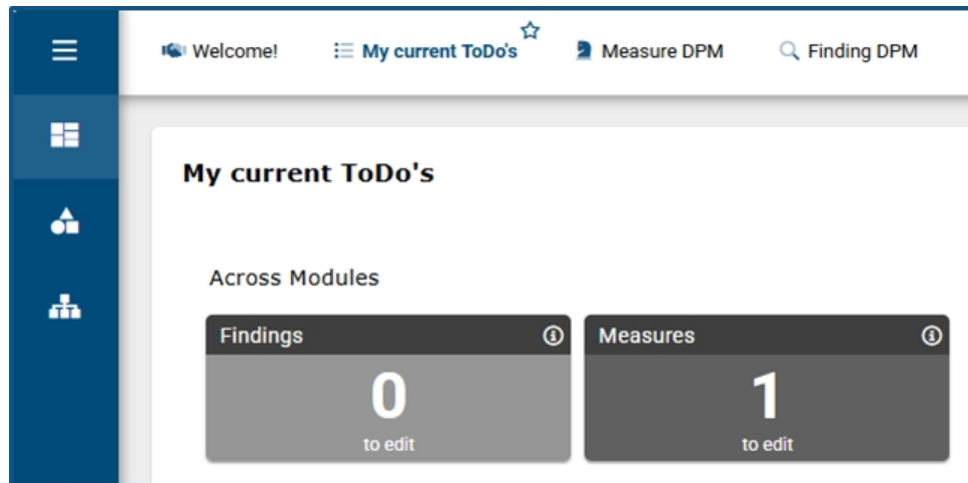
After all information has been entered, a status change to "Planning" is executed in the upper right window.

The Editor can then continue with the next step, [Set Up & plan Measure](#).

2.7.3 Set up & plan Measure

The *Editor Measure* takes on the monetary evaluation of the costs and responsibility for implementation within a scheduled period for a specific *Measure*.

The Editor can continue directly to [Add & edit Measure](#) or navigate to the *Measure* using **Dashboard >> My ToDo's**.



Step 1: Perform planning

Measure Details

5

Next

Element ID

MEA00000077

Planning

Name

Regular failure tests for business-critical IT service providers (EN)

Draft

Planning

Approval

Implementation

Review

Completed

Details

Planning

Comments

Discussion

Work Item Links

Documentation (0)

Planning

1

Planned Completion

03/02/2026

Quantification

2026

2

Initial Costs

8,000

3

Recurring Costs

0

4

Justification of Costs

The initial costs in 2025 are related to the development of a comprehensive test concept, coordination with the IT service provider, and the initial implementation of a general failure scenario, including its evaluation.

The annual recurring costs cover the performance of tests, the evaluation of results, adjustments to emergency plans, and training for relevant internal stakeholders.

(388/1200)

Save

Close

- 1 **Planned Completion:** The person responsible specifies by when the *Measure* should be completed without any foreseeable hindrance. This is crucial for the implementation of the *Measure*.
- 2 **Initial Costs:** The "Initial Costs" indicate how high the costs are in the year of implementation.
- 3 **Recurring Costs:** The "Recurring Costs" describe the costs that are expected annually following Implementation.
- 4 **Justification:** For traceability of cost information, the Editor must provide a justification on how the costs were calculated.

If, for example, there are invoices or other documentation showing how the costs of the *Measure* are composed, the "Documentation" tab can also be used to store the documents in an audit-proof manner.

- 5 **Status change:** Once all information has been entered, the status is changed to "Approval" in the upper right window.

The next status is executed by the [Approver Measure - Review & approve Measure](#). The registered *Approver Measure* is informed of the status change by means of a notification.

If further information is required later on, the *Approver Measure* can leave a comment in the "Comment" tab and reset the *Measure* to "Planning" status. The *Editor Measure* is notified of this process by means of a notification.

2.7.4 Manage & implement a Measure

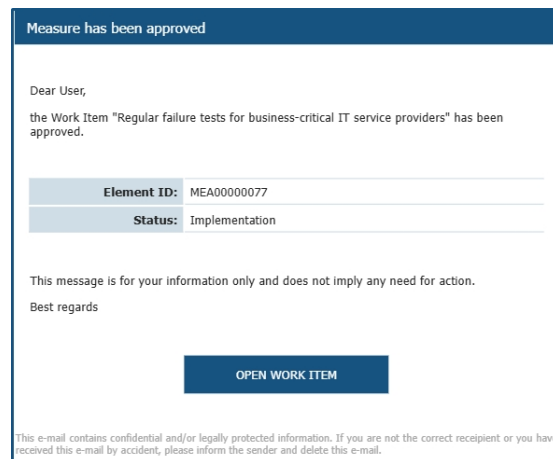
After approval, the Editor can begin implementing the *Measure*.

Step 1: Navigate to a specific Measure

The *Editor Measure* has two options for opening a *Measure* to be evaluated.

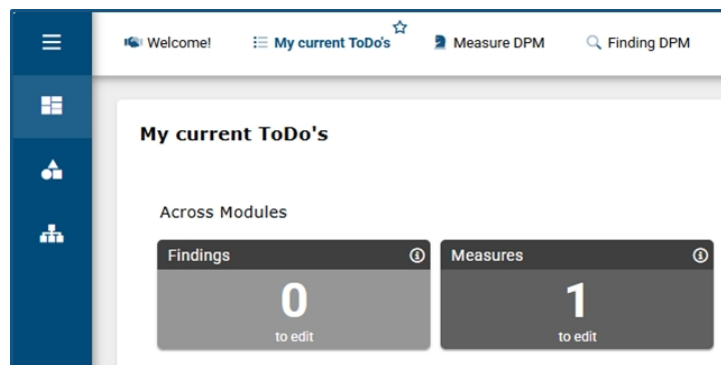
1. Open via Notification

The *Editor Measure* receives an E-Mail as soon as the Approver has approved the *Measure* and changed its status to "Implementation." The link to the specific *Measure* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

The upper part of the "My current ToDo's" dashboard contains tiles that display the number of Work Items in each Status. Clicking on a tile opens a list of all Work Items in that Status that the Editor still has to implement.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Measure*. The Editor Measure goes directly to the "Implementation" tab.

Step 2: Document implementation

Measure Details

4 Review

Element ID

MEA00000077

Implementation

Name

Regular failure tests for business-critical IT service providers

(EN)

Draft

Planning

Approval

Implementation

Review

Completed

Details

Implementation

Comments

Discussion

Work Item Links

Documentation (0)

Implementation Details

1 Degree of Implementation

0 %

25 %

50 %

75 %

100 %

☐ Degree of Implementation equals Measure Effectiveness

2 In Implementation since

03/02/2026

Delayed Completion

DD/MM/YYYY

3 Description of Implementation Steps

- Creation of a detailed test concept, including target definition and evaluation criteria
- Initial consultation with the IT service provider regarding the feasibility of the planned scenarios
- Commissioning of external support for test implementation (technical service provider)
- Scheduling of the first test run for Q4/2025

Explanation of Delays

You have unsaved changes.

Save

Close

- Degree of Implementation and Effectiveness:** The *Editor Measure* can evaluate the degree of implementation on a 5-point scale, depending on the maturity of the *Measure*. They also have the option of clicking a checkbox to indicate whether the *Measure* will take effect once it has been fully implemented or whether interim results are already effective.

For example, insurance is 100% effective once it has been signed, but if 75% of all scheduled fire extinguishers have been installed, they are already partially effective, even before reaching 100% implementation.

- Data:** The date attribute "In implementation since" is set automatically by BIC GRC when the Approver Measure changes the status of the *Measure* from "Approval" to "Implementation." The "Completion date" is the same as the "Scheduled completion date" entered by the *Editor Measure*.

If the "Completion date" has already passed and the *Measure* is still in progress, a new date attribute "Completion in case of delay" becomes visible. A new date must then be entered.

If the Completion Date is later than today's date, it is calculated from the maximum of the scheduled completion date and completion in case of delay.

- 3 **Description of the implementation steps:** The Editor must provide a detailed description to ensure the traceability of the information on the individual implementation steps.

If the scheduled "Completion date" cannot be met, the Editor must specify a new, realistic date and provide a justification for why the original date could not be met.

- 4 **Status change:** After all information has been entered, the status is changed to "Review" or "Completed" in the upper right window.

The Editor can then continue with the optional step [Optional: Editor Measure - Review & Improve Measure](#).

If the *Measure* changes to "Completed" status without review, the Approver of the Measure is notified by means of a notification.

2.7.5 Optional: Review & improve Measure

Management can insist on a review of the *Measure* by means of an additional workflow status. The Editor of the *Measure* is responsible for this after completion of the implementation.

Step 1: Navigate to the Measure

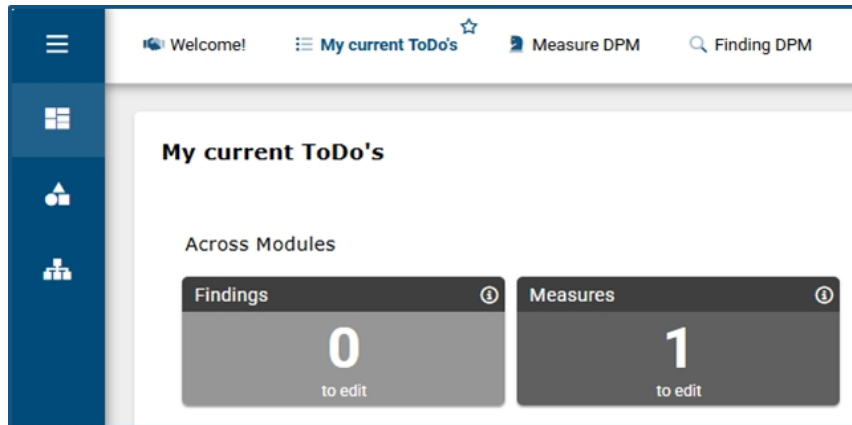
The Editor of the *Measure* has two options for editing/opening a *Measure*.

1. Direct connection to Measure implementation

The Editor Measure is already in the *Measure* because they have just completed the "Implementation" Status.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Editor has to review.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Measure*.

Step 2: Perform review

The Editor Measure can decide whether the *Measure* is appropriate and effective in the *Measure* that has been created, evaluated, and implemented.

Measure Details

Implementation

Completed

Element ID

MEA00000033

Review

Name

Regular failure tests for business-critical IT service providers

(neutral)

Draft

Planning

Approval

Implementation

Review

Completed

Details

Implementation

Testing

Comments

Discussion

Technical Attributes

Work Item Links

Documents

Testing Details

1

Date of testing

03/02/2026

2

Test Description

As part of the measure, planned failure tests were carried out in cooperation with the IT service provider. The tests included:

- Blackout simulations including server shutdown
- Restart scenarios from the emergency manual

3

Test of Design

passed

failed

Details

The measure is suitable for achieving the planned objectives. The tests cover typical scenarios, are documented in a standardised manner and are appropriately dimensioned in technical and organisational terms.

4

Test of Effectiveness

passed

failed

Details

The measure achieved the expected effect. The tests were carried out successfully and demonstrated a significant reduction in restart time and improved coordination with the IT service provider. Communication in the event of a crisis was demonstrably improved.

5

Evidence

Drop files here to upload

Testbericht

Administrator Riem

31/07/2025 11:32

6

Findings

Name	Status	D...
Documentation gap in the 2025 emergency test protocol	Registration	

7

Remark

Save

Save and Close

Close

- 1 **Date of Testing:** Here, the Editor specifies the date on which they performed the testing of the *Measure*.
- 2 **Test description:** The Editor should describe in a few words what they tested and reviewed in order to understand the basis on which the Testing was carried out.
- 3 **Test of Design:** As part of the measure testing, the Editor can determine the adequacy of the *Measure* and classify it as "Passed" or "Failed."

- 4 **Test of Effectiveness:** In addition to appropriateness, the Editor must review whether the *Measure* is effective in terms of its type and nature. The classification here is "Passed" or "Failed."

The effectiveness test is only displayed if the Test of Design was successful.

- 5 **Evidence:** At this point, documents can be linked as a link, memo, or file. All information that serves as proof should be stored here.

Files can be dragged from the desktop to the "Drag file here to upload" area.

- 6 **Finding:** The link to store a *Finding* is always visible. If the "Test of Design" or "Proof of Effectiveness" is successful, a *Finding* is optional; however, if either test is incomplete, a *Finding* must be specified. To do this, the Editor can create a new *Finding* using the icon . For more information, see [Editor Measure - Identify & Create Finding](#).

- 7 **Remark:** If there is anything else to add to the *Measure* it can be recorded here.

- 8 **Status change:** Once all information has been entered, the status is changed to "Completed" in the upper right window.

After the status change, the window can be closed.

The Approver of the *Measure* will be notified of the status change to "Completed" by means of a notification.

2.7.6 Identify & create Finding

If, while reviewing a *Measure*, the *Editor Measure* determines that either the "Test of Design" or the "Proof of Effectiveness" indicates room for improvement, the Editor Measure must create a *Finding*.

Step 1: Create Finding from Measure

A *Finding* can be created from a *Measure*. If the result of the "Test of Design" or the "Test of Effectiveness" in the *Measure* is classified as "failed," a *Finding* must be created. This is done using the  icon after the "Proof of Effectiveness" section.

The *Finding* is automatically included in the *Measure*.

Step 2: Documenting Finding

10

Registration

1

Name

*

Documentation gap in the 2025 emergency test protocol

(EN)

Details

2

GRC Perspective

P

Privacy Management

3

Editor

EditorMeasure

4

Report Date

*

31/07/2025

5

to process by

*

11/09/2025

6

Type of Finding

Observation

Recommendation

Improvement Request

Insignificant Nonconformity

Significant Nonconformity

7

Finding for these Assets:

Name	Asset Type	End-u...
Group	Business Structure	

8

Description of Finding

*

During the review of the emergency tests carried out, it was found that the complete test protocol for 2025 had not yet been stored in the central document management system. The implementation itself is documented, but the filing process was incomplete.

9

Priority of Finding

Very Low

Low

Medium

High

Critical

Save

Save and Close

Close

- Name:** A short but meaningful name for the *Finding* should be entered here.
- GRC Perspective:** The Perspective is automatically taken from the *Measure*.
- Editor:** When a *Finding* is created, the "Editor Measure" for the *Measure* is automatically set here.
- Report Date:** The Editor Measure enters when they officially reported/discovered the *Finding*. Therefore, the date can differ from the current date.

- 5 **to process by:** The date refers to the date by which the *Finding* should be resolved. It is intended as a guide for downstream users in the workflow to indicate when the *Finding* should ideally be resolved.
- 6 **Type of Finding:** The Editor of the *Measure* can classify how serious the *Finding* is in terms of the appropriateness or effectiveness of the *Measure* in the context of five levels.
- 7 **Finding for this asset:** This Asset is automatically taken from the Work Item from which it was created.
- 8 **Description offinding:** The "Description of the finding" should contain as much information and input as possible, for example, how the *Finding* was discovered. Furthermore, conclusions about cause and effect may be drawn.
- 9 **Priority of finding:** A priority can be assigned to the *Finding*, which can later be used for evaluations on dashboards, for example.
- 10 **Status change:** The Editor Measure can then switch to the "Treatment" status. For more information see [View & process Finding](#).

The Editor Measure can then return to the *Measure* and continue with the documentation of the Review of the Measure. [Editor Measure -Review & improve Measure](#).

2.7.7 Manage & handle Findings

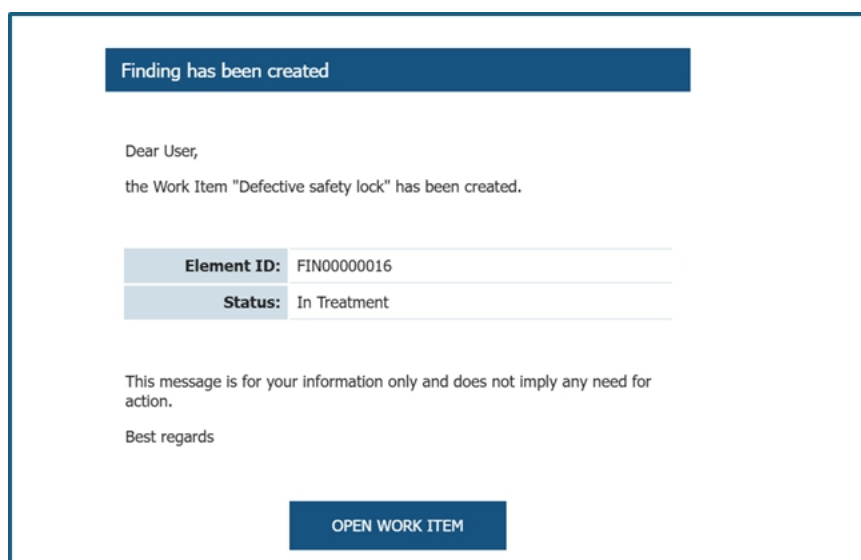
An User receives a notification when they are entered as Editor for a *Finding*. Their task is to define appropriate *Measures* in the *Finding* in order to handle the *Finding* appropriately.

Step 1: Navigating to a specific Finding after external creation

The Editor has two options for opening a *Finding*.

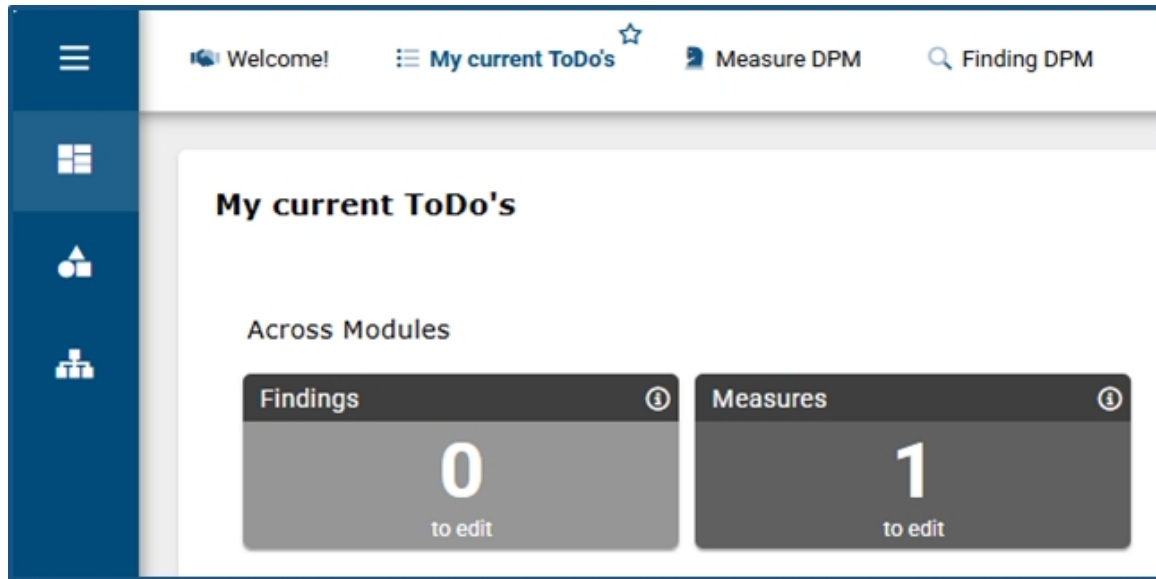
1. Open via notification

The Editor receives an E-Mail as soon as the Creator of a *Finding* has completed all entries in the "Registration" status. The link to the specific *Finding* is included in the notification.



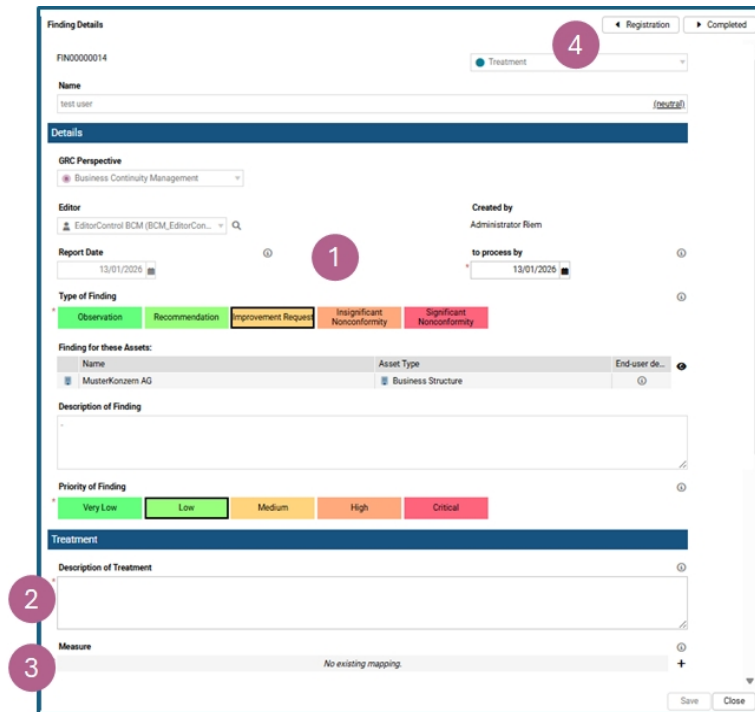
2. Open via the "My current ToDo's" Dashboard

The Editor can see their current *Findings* in the dashboard.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Finding*.

Step 2: Handle Finding



1 Check details: First, the Editor can revise the creator's assessments if necessary. This allows them to set a "to process by" date that is realistic for them. They can also reassess the

"Type of finding" and the "Priority of the finding."

2 **Description of treatment:** The Editor should then describe how they want to handle the *Finding*. This is done in writing in the first step, before specific *Measures* are created.

3 **Measure:** The *Finding* is handled by a *Measure*. For more information on creating a *Measure*, see [Editor Measure - Define & Create Measure](#) Step 2.

Only new *Measures* can be created within the *Finding* and no pre-existing *Measures* can be linked.

4 **Status change:** The Editor can then switch to the "Completed" status.

The Creator is notified of the status change via notification as a medium.

2.8 Approver Measure

Users with the Approver Measure user profile are responsible for one or more specific *Measures* in BIC GRC. Only those approvers who also have the appropriate authorization for the Asset can be stored in a *Measure*.

The Approver for Measure has the following tasks in BIC GRC:

- [Review & approve Measures](#)

In addition, they may create *Measures* and assign them to an Editor Measure after creation. For information on creating a *Measure*, see [Editor Measure - Define & Create Measure](#).

2.8.1 Review & approve Measure

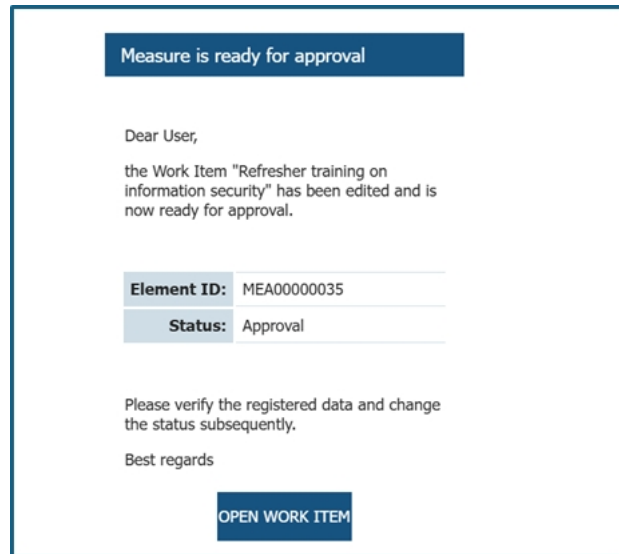
After a *Measure* has been created and planned, it must be reviewed by the Approver of the *Measure* before implementation.

Step 1: Navigating to the Measure

The *Approver Measure* has two options for opening a *Measure*.

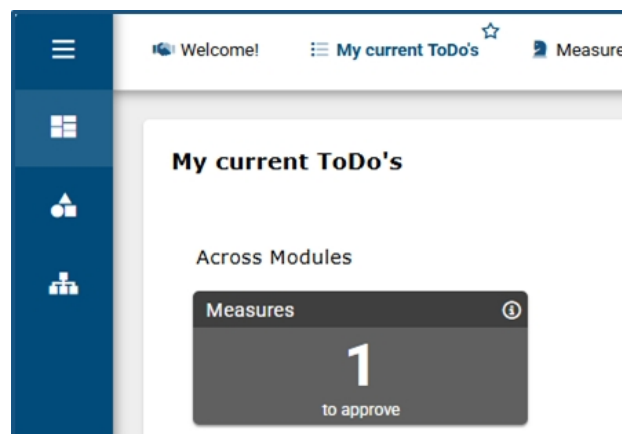
1. Open via notification

The *Approver Measure* receives an E-Mail as soon as the *Editor Measure* changes the Status of the *Measure* to "Approval." The link to the specific *Measure* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current to- dos" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Approver has to review.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Measure*.

Step 2: Perform approval

The Approver has full read access to the created and scheduled *Measure* in order to decide, based on all the information entered, whether the *Measure* has been sufficiently described and planned. If this is the case, the Approver can change the status to "Implementation."

If further refinement is needed, the Approver can leave a comment in the "Comment" tab and change the status to "Planning."

Measure Details

◀ Planning

▶ Next ▼

Element ID

MEA00000077

● Approval ▼

Name

Regular failure tests for business-critical IT service providers (EN)

Draft

Planning

Approval

Implementation

Review

Completed

Details

Planning

Comments

Discussion

Work Item Links

Documentation (0)

Comments

Comment

Enter your comment here. (0/1000)

Add Comment

All Comments

Save

Close

After saving, the assigned Editor Measure is notified by means of a notification.

2.9 Editor Control

The Editor Control is responsible for at least one *Control* in BIC GRC. They can become responsible for a *Control* through other Users or by creating it themselves.

An Editor Control has the following tasks in BIC GRC:

- [Derive & create Controls](#)
- [Edit & review Controls](#)
- [Initiate & create a Control Testing](#)
- [Review & handle Findings](#)
- [Review & approve a Control Testing](#)

The Editor Control can also create *Measures* from a *Finding* in BIC GRC. At this point, refer to the user profile "Editor Measure":

- [Define & create Measure](#)

2.9.1 Derive & create Control

In BIC GRC, different users can create a *Control*. This can be done by creating it from other Work Items (e.g., Risks) or by creating it manually (bottom-up).

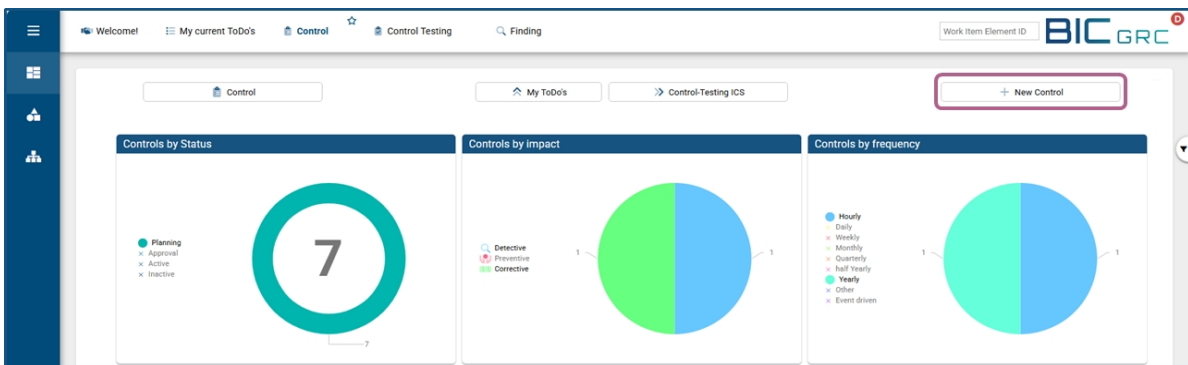
Step 1: Create Control

The Editor Control offers two options for creating a *Control*.

1. Creation via the "Control" Dashboard

The Editor Control navigates to **Dashboards >> Control Overview >> "New Control."**

A new *Control* is created using a button in the upper right corner of the window.

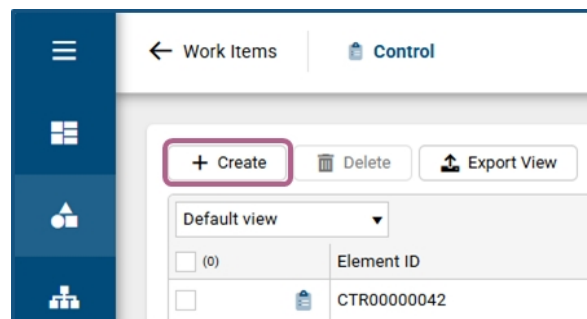


A new window will then open automatically.

2. Creation via Tile

The Editor navigates to **Work Items >> Control >> "Create."**

A new window then opens automatically.



Step 2: Enter details

Control Details

Status: Planning

* Name: 1 Regular emergency testing with the IT service provider (EN)

Assignment

Details

2 **Scope**

Name	Asset Type	End-use...	
MusterKonzern AG	Business Structure		

3 **GRC Perspective**

* Privacy Management ☒ relevant for Privacy Management

4 **Editor**

* EditorControl

Approver

* ApproverControl

5 **Level of Control**

* Entity Level Control

6 **Type of control**

* Keycontrol

7 **Description of the control**

* Regular execution of planned emergency tests in collaboration with the IT service provider to verify the effectiveness of recovery procedures, escalation paths, and communication processes in case of an incident, and to identify areas for improvement.

8 You have unsaved changes. Save Close

1 **Name:** The first step should be to enter a short but meaningful name for the *Control*.

2 **Scope:** The scope specifies the area or process in which the *Control* should be applied.

In the background, a filter limits the scope for Assets of the Types "Business Unit" and "Primary Asset."

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request..](#)

3 **GRC Perspective:** After selecting the scope, the User is shown the list of GRC Perspectives. The Editor can select one or more GRC Perspectives for which they have creation permissions.

The number of GRC Perspectives displayed depends on the activated modules.

If the Data Protection module is active, a "relevant for Privacy" checkbox is displayed next to the GRC Perspective.

- 4 **Responsible persons:** A user must be stored in the "Editor" attribute and, in addition, an "Approver" who is responsible for the approval of the *Control*.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

- 5 **Level of Control:** The "Control Level" determines whether a *Control* is requested by management (top-down) or whether it is a bottom-up control.

- 6 **Type of control:** It can be determined whether the control is performed as a "Key Control" for a process or as a "Supporting Control" if, for example, Control Testing has identified that the existing "Key Control" is not adequate on itself.

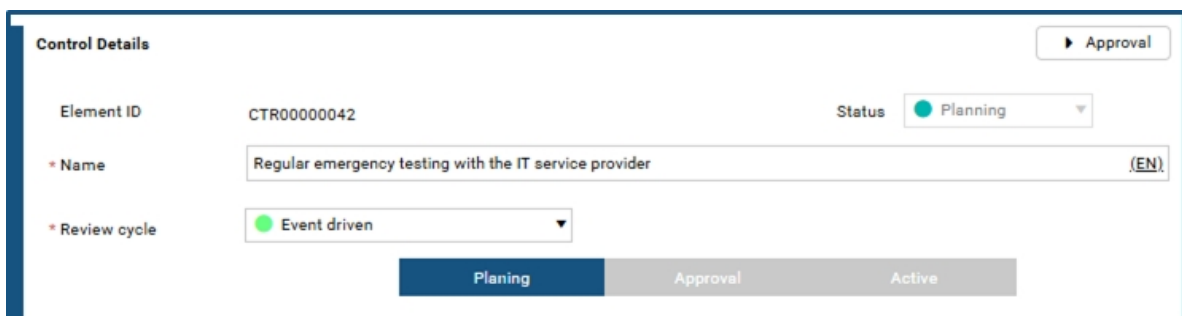
- 7 **description of the control:** This description should contain as much information and input as possible so that the Control Executer is then fully informed about what their task is during the *Control Execution*.

- 8 **Save:** Once the information has been entered, the user can save it.

Otherwise, the assigned Editor Control will be notified of the status change after the save process by means of a notification.

Step 3: Finalize assignment

The Editor should regularly review the *Control* to ensure that it remains up to date and correct. The "Next review" field helps you to review this at regular intervals. Two weeks before the date is reached, the Editor automatically receives a notification reminding them of an upcoming reassessment. On the day of the "Next Evaluation," the *Control* is switched from "Active" to "Planning" Status, and the User is automatically sent another notification.



The screenshot shows the "Control Details" form. It includes the following fields and controls:

- Element ID:** CTR00000042
- Status:** A dropdown menu currently set to "Planning" with a teal circle icon.
- Name:** A text field containing "Regular emergency testing with the IT service provider" and a language selector "(EN)".
- Review cycle:** A dropdown menu currently set to "Event driven" with a green circle icon.
- Buttons:** At the bottom, there are three buttons: "Planing" (dark blue), "Approval" (grey), and "Active" (grey).
- Approval button:** A button with a right-pointing arrow and the text "Approval" is located in the top right corner.

The date is automatically reset after the status change depending on the time specified in the "Review Cycle."

If the *Control* has one of the review cycles "Every ... days," "Event-related," "Daily," or "Weekly," the status will not automatically be set back to "Approval". The Editor receives a notification only when manually triggered.

If the Creator of the check is also the Editor Control, they can continue with the next step, [Editor Control - Add & Edit Control](#).

2.9.2 Edit & review Control

A *Control* can be identified and created by multiple users.

If the Creator and the Editor are different users, the Editor is informed separately about the new *Control* by means of a notification. The following steps 1 & 2 refer to the steps after creation by another User.

Optional step 1: Navigating to a specific Control after external creation

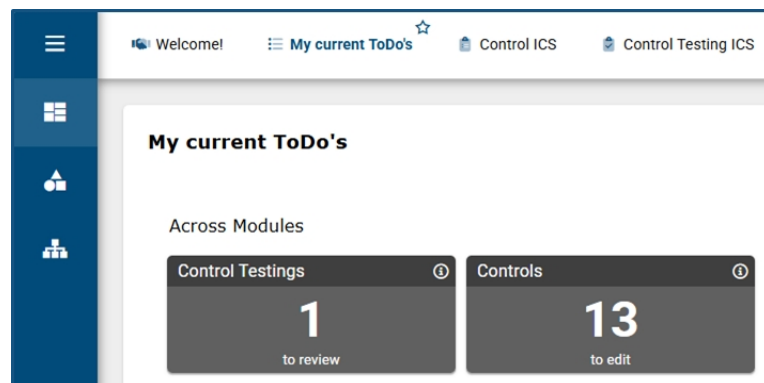
The Editor has two options for opening a *Control* to be edited.

1. Open via notification

The Editor receives an E-Mail as soon as the Creator has completed all entries in the "NEW" status. The link to the specific *Control* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Editor can still complete.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Control*. The Editor goes directly to the "Assignment" tab of the *Control*.

Optional step 2: Reviewing the Creator's entries

If the Creator and the Editor are different users, it is recommended to go to the "Assignment" tab as the first step in the Work Item *Control* to view the Creator's detailed entries.

If the Creator's entries require clarification or further details, the Editor can leave a contribution in the "Discussion" tab. The Creator is then informed of the contribution via notification.

Step 3: Add to Control

Control Details

Element ID

CTR00000042

Status

Planning

Name

Regular emergency testing with the IT service provider

Review cycle

Event driven

Planning

Approval

Active

Assignment

Control Execution

Control Testing

Comments

Discussion

Work Item Links

Documentation (0)

1 Control Objectives

Name	Catalog	E...	
Business Continuity and Emergency Planning	Control Objectives		
Operational Efficiency and Effectiveness	Control Objectives		

2 Control Frequency

Monthly

2 Control Testing Frequency

Yearly

4 Impact of Control

Detective

5 Outsourcing

outsourced within company

3 Control Automation

Manual

5 Is control outsourced

☒

5 Control assigned to

Name	Asset Type	End-use...	
4wheels Automotive Magyarország Kft	Business Structure		

Save

Close

- Control Objective:** In the "Control Objective" field, one or more suitable objectives from a GRC framework can be linked to which the *Control* is based upon.

The GRC Framework contains a number of examples, such as "Access Control," which should be supplemented by management. If, for example, the control is subject to the Control Objective "Access Control," then the objective of the control should be that, with a well-functioning *Control*, only authorized persons have access to a system.

- Frequencies:** Two types of frequencies can be stored in the *Control*:
 - Control Frequency: At what intervals should the *Control* be performed?

The frequency is also used later for *Control Execution*.

- **Control Testing Frequency:** At what intervals should the *Control* be reviewed for appropriateness and effectiveness?

The frequency is also used later for *Control Testing*.

- 3 **Control Automation:** The three most common options, "Manual," "Semi-automatic," or "Automatic," are displayed in this attribute field.

Depending on the selection, a link to "IT System used" is also displayed to the Editor for "Semi-automatic" or "Automatic." This link must explicitly be filled if "Automatic" is selected.

- 4 **Impact of the Control:** A *Control* can be preventive or detective. The appropriate choice must be specified here.

- 5 **Outsourcing:** If the *Control* is executed outside the Process/Business Unit, you can specify here where the *Control* is outsourced. The *Control* can be executed within the Company or outside the Company.

If the *Control* is outsourced within the company, a link to the asset hierarchy in BIC GRC appears when the corresponding "Outsourcing" option is selected. The Editor Control can then select the responsible unit using the  icon. In the background, a filter filters for Assets of the Type "Business Unit."

If the outsourcing is external to the Company, a link to a supplier directory is displayed. Here, too, a corresponding link must be made using the icon .

- 6 **References:** In addition to the above, the following assignments can also be made:

- **Control Catalog:** The "Control Catalog" leads to the Control Catalog(s) of
 - ISO 27701:2019
- **Documented Information:** The Editor Control can store one or more pieces of *Documented Information*.

Documented Information supports efficiency and traceability, particularly in the area of information security, but can also make a contribution to transparency in other modules.

- **Assessment:** The link to a specific assessment is automatically filled in by BIC GRC if the *Control* was created from a suitable assessment. If the *Control* already existed before the assessment, the "Assessment" can be linked afterwards.

References

Control Catalogs

Element Name	Name	
ISO270022022.ISO27002_2022.05.30	5.30 ICT readiness for business continuity	
BSIRequirementsGrundschutz.BSI.PB.DER.04.A09_H	DER.4.A9 Integration of emergency management into organi...	

Documented Informations

No existing mapping.

Assessment

No existing mapping.

Save

Close

Step 4: Store Control Executors & Testers

In the two tabs "Control Execution" (optional) and "Control Testing," the Editor must enter the appropriate Users before a status change is made.

Control Details

Element ID

CTR00000042

Status

Planning

Name

Regular emergency testing with the IT service provider

(EN)

Review cycle

Event driven

Planing

Approval

Active

Assignment

Control Execution

Control Testing

Comments

Discussion

Work Item Links

Document:

Control Execution

1 Control Executer

ControlExecuter

Last Control Execution

Next Control Execution

Control Execution

No existing mapping.

Save

Close

1

Control Executer:

For *Control Execution*, a responsible Control Executer can be specified in the second tab "Control Execution" using the icon .

The Editor can enter exactly one User as the Control Executer. The Editor can focus on this specific task, as other attribute fields in this tab are currently not available for editing.

The attributes in this tab behave as follows:

- **Last Control Execution** : This is set automatically after the status of the *Control Execution* changes from "Progress" to "Completed."

The attribute is Read Only and is automatically managed by the system.

- **Next Control Execution**: Set automatically after a date is entered in "Last Control Execution" for the first time. The "Next Control Execution" date is then calculated by adding the "Last Control Execution" date and the control frequency from the "Assignment" tab.

The attribute is Read Only and is automatically maintained.

- **Control Execution**: Only a user with the appropriate user profile can create a *Control Execution*. For more information, see [Control Executer - Control Executer - Create & execute Control Execution](#).

Control Details ► Approval

Element ID: CTR00000042 Status: Planning

* Name: Regular emergency testing with the IT service provider (EN)

* Review cycle: Event driven

Planing Approval Active

◀ Assignment Control Execution **Control Testing** Comments Discussion Work Item Links Documents ▶

Control Testing

2 **Designated Tester**

* Tester GEN (Tester) Q

3 **Last Control Testing** i **Next Control Testing**

4 **Test Description** i

* As part of the control testing, it is verified whether emergency tests with the IT service provider are conducted regularly, documented properly, and executed with sufficient scope and quality. The review includes:

- Test planning (e.g., frequency, scenarios)
- Involvement of the service provider

5 **Evidence**

No documents available.

6 **Control Testing**

No existing mapping.

7 Save Close

2 **Designated Tester:** To assign a Tester, the Editor switches to the third tab, "Control Testing." As in the "Control Execution" tab, the Editor uses the Q icon to assign a Tester responsible for the *Control*.

3 **Control Testing Data:** As in the Control Execution, two data attributes are displayed in the "Control Testing" tab.

- **Last Control Testing:** This is set automatically after the status of the *Control Testing* changes from "Execution" to "Review."

The attribute is Read Only and is automatically managed by the system.

- **Next Control Testing:** Set automatically after a date is entered in "Last Control Testing" for the first time. The "Next Control Testing" date is then calculated as the sum of the "Last Control Testing" date and the Control Testing frequency from the "Assignment" tab.

The attribute is Read Only and is automatically managed.

- 4 **Test description:** In the test description, the Editor must specify how the *Control* can be validated.

For example, they can specify the activity the Tester can use to perform the *Control Testing* or suggest the size of the Random Sample to be selected.

- 5 **Evidence:** In addition to the description, a document can also be attached to the Control.

Files can be dragged from the desktop to the "Drag file here to upload" area.

An exemplary file to link would be a template of a checklist for checking the *Control*.

- 6 **Control Testing:** *Control Testing* can be created exclusively by an Editor Control. For more information, see [Editor Control - Initiate & create Control Testing](#).

- 7 **Status change:** After all information has been entered, a status change to "Approval" is performed in the upper right window.

After saving, the entered *Approver Control* is notified by means of a notification.

2.9.3 Initiating & creating Control Testing

During the documentation phase of a *Control*, the Editor Control can nominate a suitable Tester in the third tab, "Control Testing." Once the *Control* has been approved and is in "Active" status, *Control Testing* can be started.

The Editor Control starts *Control Testing* manually. To do this at regular intervals, a scheduler supports the Editor Control by reminding them one day before the "Next Control Testing" is due.

Step 1: Navigate to Control

The Editor Control automatically receives an E-Mail as soon as the date for "Next Control Testing" has been reached. The link to the specific *Control* is included in the notification.

Step 2: Create Control Testing

The *Control Testing* is created from the *Control* by the Editor creating a new *Control Testing* using the  icon.

Control Testing is designed to be performed uniquely for each *Control*.

Step 3: Enter details

Control Testing Details

Element ID Execution

* Name **1** Regular emergency testing with the IT service provider (EN)

Test Execution

Details

2 GRC Perspective
Privacy Management

3 Tester Tester GEN (Tester) **3** Editor EditorControl ERM (ERM_EditorCont...

4 testing for:

Name	Asset Type	End-u...
MusterKonzern AG	Business Structure	

You have unsaved changes. Save Close

- 1 Name:** The first step is to automatically transfer the "Name" from the *Control* to the *Control Testing*, so the editor can rely on the pre-populated value.

When the status changes, the "Name" is supplemented with the date of the "Time of Test Execution."

- 2 GRC Perspective:** The perspective is automatically transferred from the *Control* and set. It remains unchanged after the first save operation.
- 3 Responsibilities:** Furthermore, when creating the *Control Testing*, the responsible persons defined in the *Control* are automatically transferred.
- 4 Testing for::** Furthermore, the Control Asset is automatically transferred.

After saving, the registered Tester is notified via notification.

The window can then be closed.

2.9.4 Manage & handle Findings

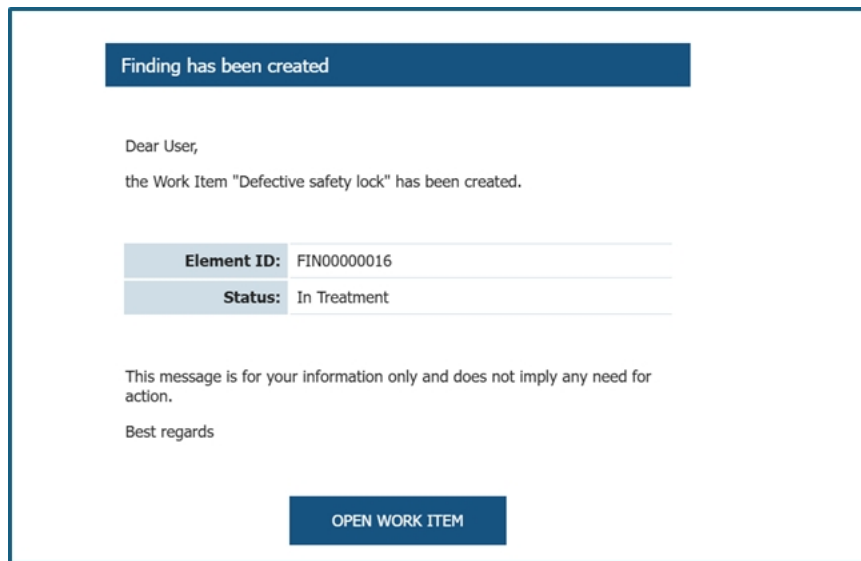
An User receives a notification when they are entered as Editor for a *Finding*. Their task is to define appropriate *Measures* in the *Finding* in order to handle the *Finding* appropriately.

Step 1: Navigating to a specific Finding after external creation

The Editor has two options for opening a *Finding*.

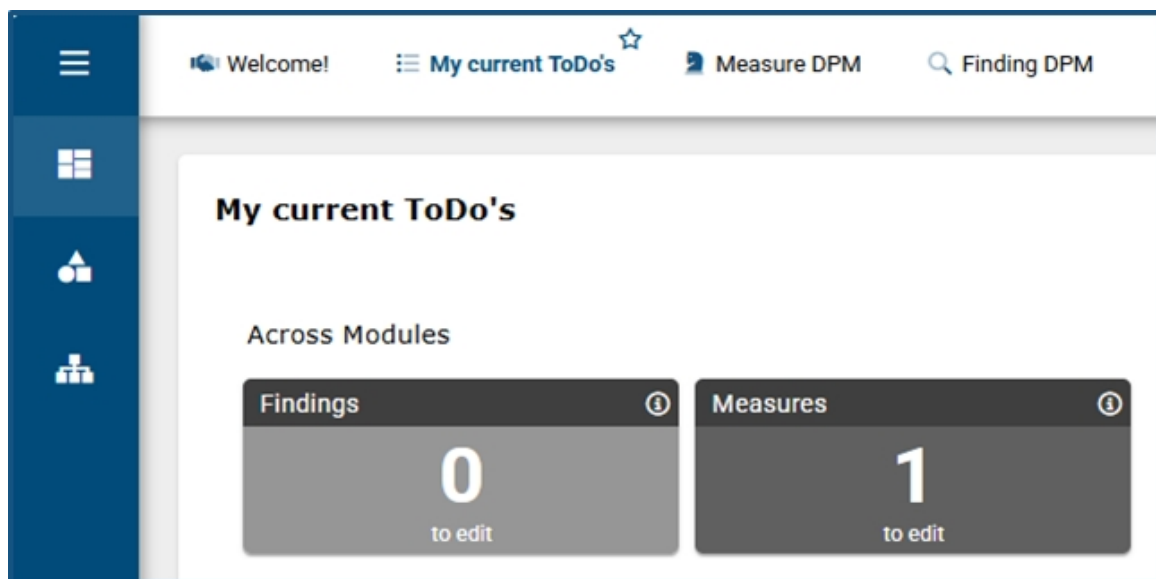
1. Open via notification

The Editor receives an E-Mail as soon as the Creator of a *Finding* has completed all entries in the "Registration" status. The link to the specific *Finding* is included in the notification.



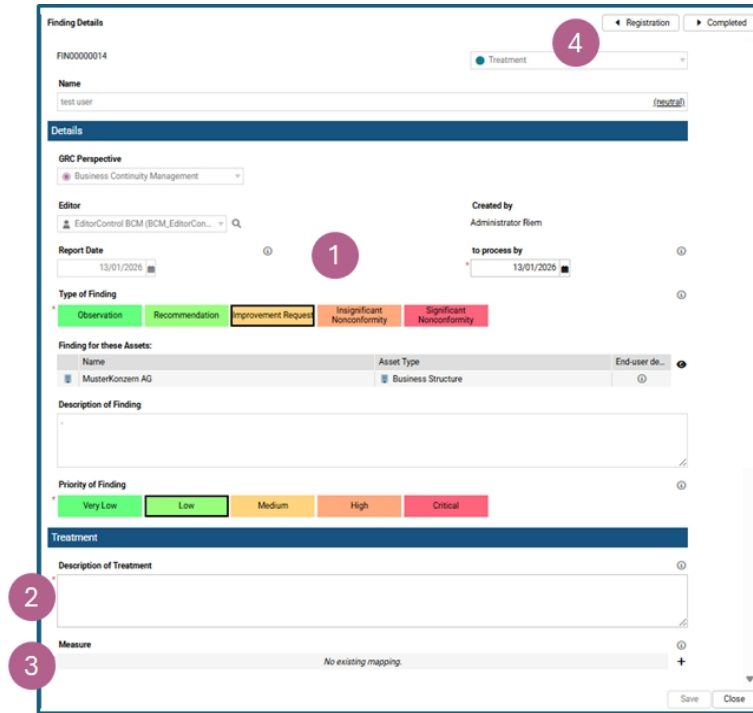
2. Open via the "My current ToDo's" Dashboard

The Editor can see their current *Findings* in the dashboard.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Finding*.

Step 2: Handle Finding



- 1 **Check details:** First, the Editor can revise the creator's assessments if necessary. This allows them to set a "to process by" date that is realistic for them. They can also reassess the "Type of finding" and the "Priority of the finding."
- 2 **Description of treatment:** The Editor should then describe how they want to handle the *Finding*. This is done in writing in the first step, before specific *Measures* are created.
- 3 **Measure:** The *Finding* is handled by a *Measure*. For more information on creating a *Measure*, see [Editor Measure - Define & Create Measure](#) Step 2.

Only new *Measures* can be created within the *Finding* and no pre-existing *Measures* can be linked.

- 4 **Status change:** The Editor can then switch to the "Completed" status.

The Creator is notified of the status change via notification as a medium.

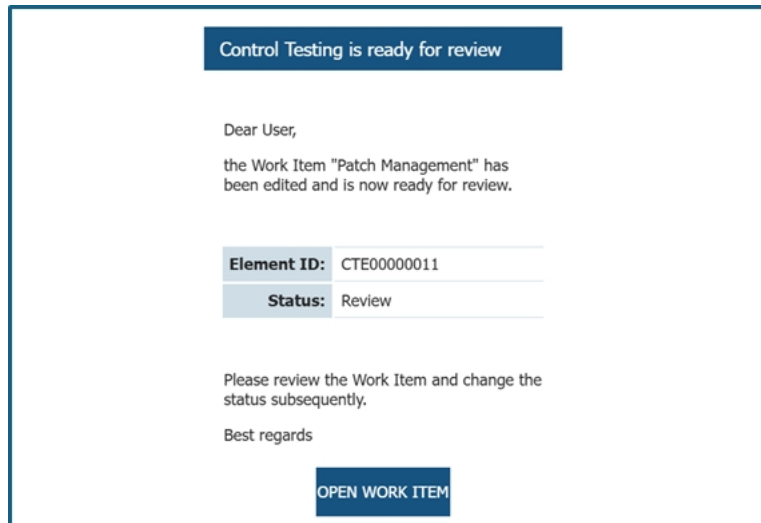
2.9.5 Review & approve Control Testing

Control Testing is created by the Editor Control and documented by the Tester. Once the test results are completed *Control Testing* can be forwarded to the Editor Control by changing the status to "Review."

Step 1: Navigate to Control Testing

The Editor Control has two options for opening a *Control* to be approved.

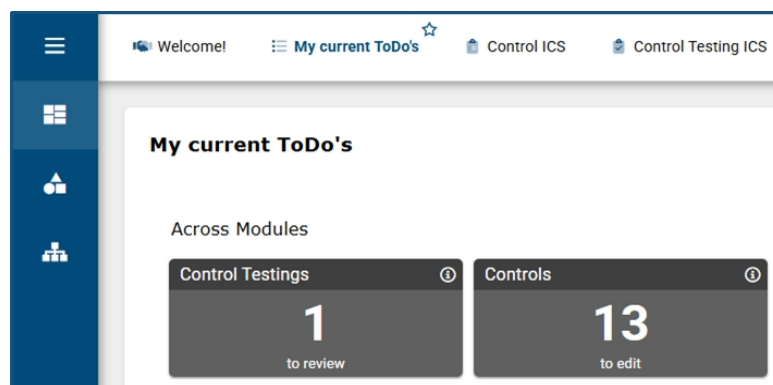
1. Open via notification



The Editor Control receives an E-Mail as soon as the Tester has completed all entries in the "Execution" status. The link to the specific *Control Testing* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the *Editor Control* still has to review.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for *Control Testing*.

Step 2: Perform review

The Editor Control has full read access in the *Control Testing* to decide, based on the information entered, whether the *Control Testing* was successful or not. There are two status transitions available: "Test passed" and "Test not passed."

If either the "Test of Design" or the "Test of Effectiveness" has not been successful, the Editor Control can change the status to "Test not Successful." Alternatively, the Editor Control can leave a Comment in the "Comment" tab and change the status to "Execution." The Tester is notified by means of a notification.

Step 3: Perform status transition execution

If the entries made by the upstream user are correct and the test result is positive, the Editor can change the status to "Test passed."

After saving, the Tester is notified via notification.

After the status transition, the window can be closed.

2.10 Approver Control

The *Approver Control* in BIC GRC is responsible for the approval of at least one *Control* assigned to their Asset.

- [Review & release a Control](#)

They can also create *Controls* in BIC GRC. However, as their primary responsibility lies elsewhere, only the "Editor Control" user profile is referred to here:

- [Derive & create Control](#)

2.10.1 Review & approve Control

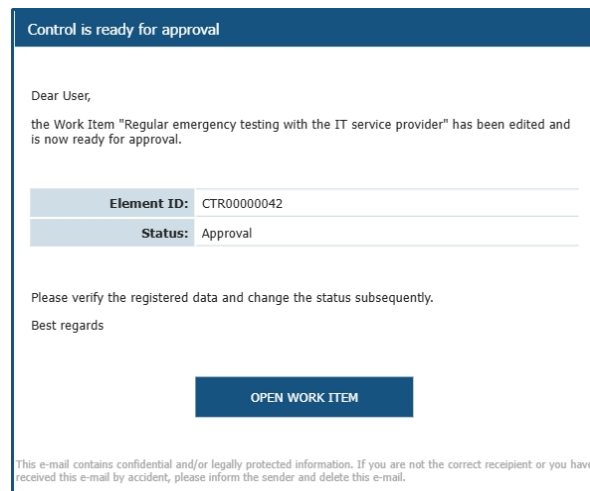
A Control is created and documented by the *Editor Control*. Once all information has been entered and reviewed, a *Control* can be passed on to the *Approver Control* by changing its status to "Approved."

Step 1: Navigate to Control

The *Approver Control* has two options for opening a *Control* to be approved.

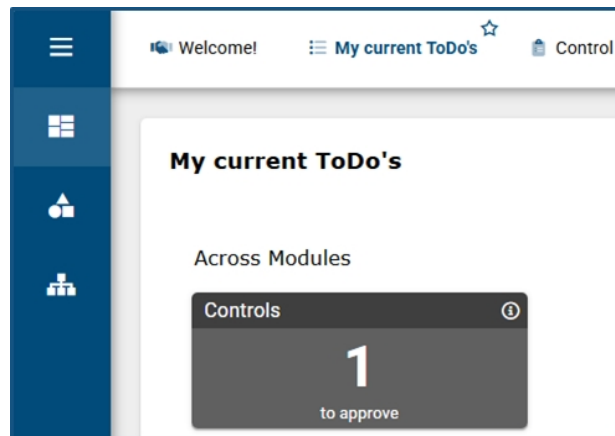
1. Open via notification

The *Approver Control* receives an E-Mail as soon as the *Editor Control* has completed all entries in the "Planning" status. The link to the specific *Control* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Approver Control can still approve.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Control*.

Step 2: Perform review

The Approver Control has full read access to the *Control* in order to decide, based on the information entered, whether the *Control* is suitable for improving the process. If further improvements are needed, the Approver Control can leave a comment in the "Comment" tab and change the status to "Planning."

Control Details

Element ID

CTR00000042

Status

Approval

Name

Regular emergency testing with the IT service provider

(EN)

Review cycle

Event driven

Planing

Approval

Active

Assignment

Control Execution

Control Testing

Comments

Discussion

Work Item Links

Document

Comments

Comment

Enter your comment here.

(0/1000)

Add Comment

All Comments

2026-01-22, S02, ERM_ApproverControl:

Wir müssen einen bald einen neuen Kontrolldurchführer nominieren.

Save

Close

Step 3: Execution of the status change

If the entries made by the upstream User are correct, the Approver Control can change the status to "Active."

After saving, the Editor is notified by means of a notification.

After the status transition, the window can be closed.

2.11 Control Executer

The Control Executer is responsible for performing a *Control* on a specific Asset. The task of the Control Executer in BIC GRC is to confirm the execution and, if necessary, to deposit the associated documents.

2.11.1 Create & perform Control Execution

During the documentation phase of a *Control*, the *Editor Control* nominates a suitable Control Executer in the second tab, "Control Execution." Once the control has been approved and is in "Active" status, *Control Execution* can be started.

Step 1: Navigate to the Control

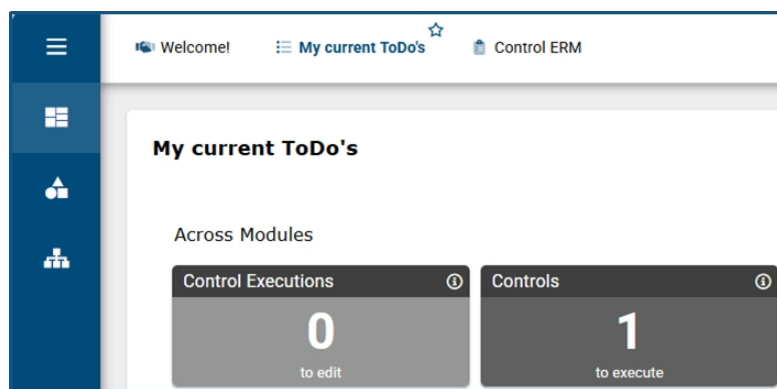
The Control Executer has two options for opening a *Control*.

1. Open via notification

The *Control Executer* receives an E-Mail as soon as the Approver has changed the status to "Active," or an automatic notification is sent by a scheduler. The link to the specific *Control* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

The "My current ToDo's" dashboard contains tiles that display the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status for which the *Control Executer* still has to perform an Execution (open via *Control*) or can continue.

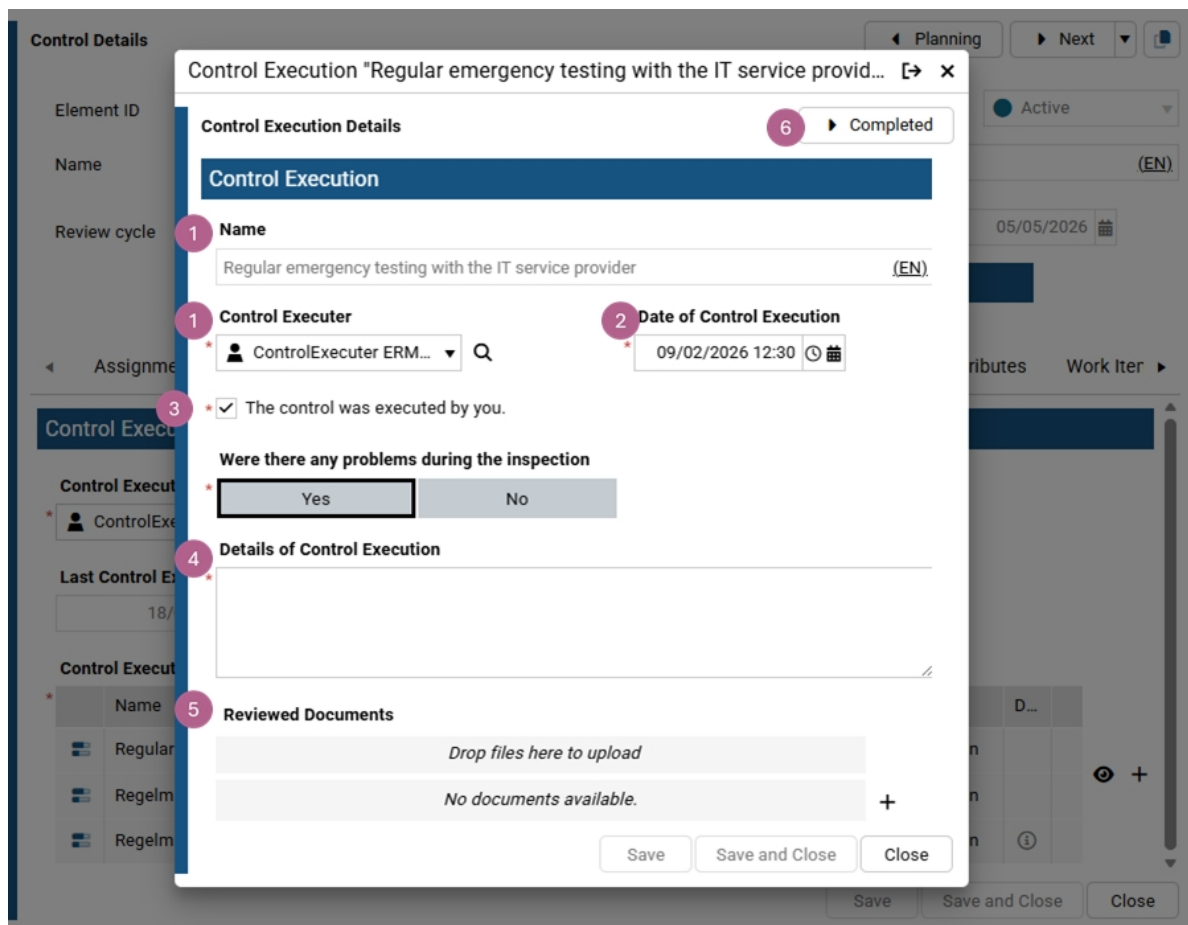


Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Control*. The Control Executer is directly led to the "Control Execution" tab of the *Control*.

Step 2: Reviewing the entries made by the Editor Control

Firstly, it is recommended to switch to the "Assignment" tab to view the detailed entries made by the Editor Control and draw conclusions about the specifications for the *Control Execution*.

Step 3: Create Control Execution



- 1 **Name and Executer:** As a first step, the "Name" and the user field "Control Executer" are automatically filled in by BIC GRC, so the *Control Executer* does not manually have to them.
- 2 **Date of Control Execution:** The Control Executer enters the date individually. They can also enter the exact time if necessary.

This date is used for the "Last Control Execution" attribute field in the *Control*.

The date of the *Control Execution* must be the current day or in the past so that the *Control Execution* can later be changed to "Completed" status. See also point 6 below.

- 3 **Indication of execution:** The Control Executer must use this checkbox to explicitly confirm that they have performed the *Control*. After ticking this box and initially saving, additional attribute fields are displayed.
- 4 **Details of the control execution:** If there were any special circumstances during the *Control Execution*, or if other details are relevant, these can be described here.
- 5 **Reviewed Documents:** The Control Executer may also attach documents that have either been reviewed during or were used to assist in performing the *Control*.

Files can be dragged from the desktop to the "Drag file here to upload" area.

An exemplary file would be a signed checklist of all executed steps. This can be stored here.

6

Status change: Once all information has been entered, the status is changed to "Completed" in the upper right window.

If any challenges arose during the *Control Execution*, the person responsible for the *Control* will be notified via notification.

The system currently focuses on efficient execution rather than a review of the *Control Execution* in BIC GRC. The Editor is notified when the *Control Execution* has been completed.

2.12 Tester

The Tester is responsible for reviewing *Controls* in BIC GRC at regular intervals to ensure that they are appropriate and effective. Testers may be any qualified persons inside or outside the Company, such as internal auditors or external auditors. Only one Tester can be nominated per *Control*. In addition to documenting the *Control Testing*, the Tester must also identify *Findings* in order to improve the *Control*.

A Tester in BIC GRC has the following tasks:

- [Perform & evaluate a Control Testing](#)
- [Identify & create Findings](#)

2.12.1 Perform & evaluate Control Testing

During the documentation phase of a *Control*, the *Editor Control* can nominate a suitable *Tester* in the third tab, "Control Testing." Once the *Control* has been approved and is in "Active" status, *Control Testing* can be started by the *Editor Control*.

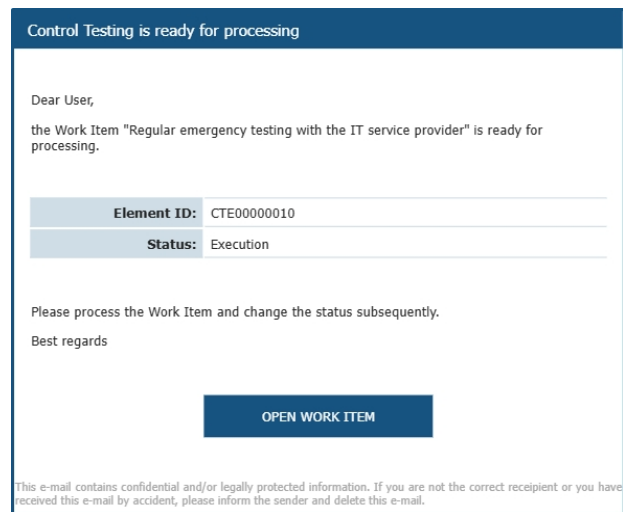
The *Control Testing* is created by the Editor Control and, after the first save operation, is transferred to the Tester via notification proof.

Step 1: Navigate to Control

The *Tester* has two options for opening a *Control*.

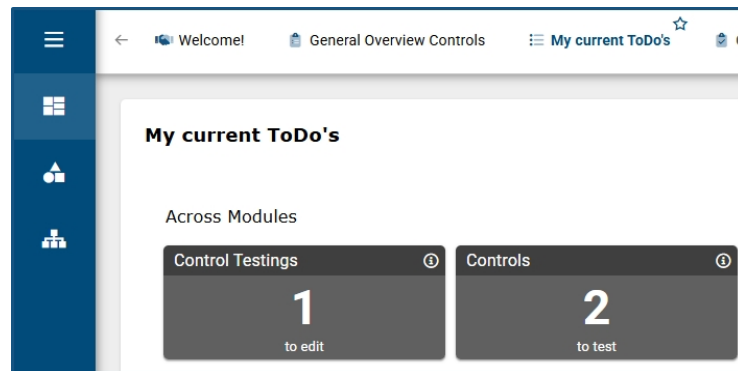
1. Open via notification

The *Tester* receives an E-Mail as soon as the Editor has created a *Control Testing* and saved it for the first time. The link to the specific *Control Testing* is included in the notification.



2. Open via the "My current ToDo's" dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status for which the *Tester* has to perform *Control Testing*.



Step 2: Enter details

Some information has already been entered when the Editor Control was created.

Control Testing Details

Element ID

CTE00000010

Execution

Name

Regular emergency testing with the IT service provider

Test Execution

Review

Completed

Test Execution

Comments

Discussion

Work Item Links

Documentation (0)

1 Date of Testing

03/02/2026

2 Chosen Sample Size

33

3 Total Population and Sample Unit Description

The total population comprises all annually planned emergency tests with business-critical IT service providers in the period 2020–2025. The emergency test on 15 June 2025 with the main service provider 'ITCore GmbH' was selected for testing. This covers over 80% of the critical processes affected.

4 Verified period

From

03/02/2026

To

03/02/2026

5 Test of Design

Passed

Failed

Details Test of Design

The tested control meets the defined expectation according to the control description: The emergency test was carried out in full in accordance with the agreed procedure (blackout simulation, restoration, communication channels, supporting documentation). All affected processes were appropriately included.

6 Test of Effectiveness

Passed

Failed

Details Test of Effectiveness

The test showed that the defined emergency response plan works. Recovery times were within the target values, and communication with relevant stakeholders was structured. The result confirms the effectiveness of the measures implemented.

7 Evidence

Drop files here to upload

No documents available.

8 Link Findings

Name	Status	De...
Incomplete documentation of emergency testing with IT service provider	Registration	

9 Remark

10

Save

Close

- Date of Testing:** The current date on which the *Control Testing* was performed should be entered here. When the first save occurs without a date being entered, the date is automatically filled in with the current date.
- Selected sample size:** The actual size of the random sample selected by the *Tester* must be entered in this attribute field. The number may differ from the suggestion made by the *Editor Control* and can be adjusted as needed.
- Total population and sample unit description:** Here, the *Tester* can provide a description of how they selected the random sample.

For example, they can specify how the random samples were selected and whether there are any other special features of the random sample that need to be taken into account.

- 4 **Verified period:** Finally, a period must be specified that the *Tester* will audit as part of their testing activities.

For Example: If the control or its execution is reviewed and checked from November to December, the date entered should be 11/1 to 12/31.

- 5 **Test of Design:** As part of the *Control Testing*, the *Tester* can determine the adequacy of the *Control* and classify it as "passed" or "failed."

For example, it must be questioned whether the *Control* is appropriate to mitigate a specific risk.

- 6 **Test of Effectiveness:** In addition to appropriateness, the *Tester* must review whether the *Control* is effective in terms of its type and nature. The classification here is "Passed" or "Failed."

- 7 **Evidence:** At this point, documents can be linked. Any information that can be used as evidence can be stored.

- 8 **Link findings:** The link to store a *Finding* is always visible. If the "Test of Design" or "proof of effectiveness" has passed, a *Finding* can be specified. To do this, the *Tester* can use the icon . For more information, see [Tester - Identify & create Finding](#).

- 9 **Remark:** At this point, you can add a supplementary comment about the Testing. This is information that is not relevant anywhere else but is relevant to the Context of the Testing.

- 10 **Save:** After all information has been entered, it may be saved. Then, a status change may be performed by the *Tester*.

2.12.2 Identify & create Finding

If, while reviewing a *Control Testing*, the Editor determines that either the "Test of Design" or the "Proof of Effectiveness" indicates room for improvement, the Editor must create a *Finding*.

Step 1: Create Finding from Control Testing

A *Finding* can be created from a *Control Testing*. If the result of the "Test of Design" or the "Test of Effectiveness" in the *Control Testing* is classified as "failed," a *Finding* must be created. This is done using the  icon after the "Proof of Effectiveness" section.

The *Finding* is automatically included in the *Control Testing*.

- 5 **To process by:** The date refers to the date by which the *Finding* should be resolved. It is intended as a guide for downstream users in the workflow to indicate when the *Finding* should ideally be resolved.
- 6 **Type of Finding:** The Editor of the *Control Testing* can classify how serious the *Finding* is in terms of the appropriateness or effectiveness of the *Control Testing* in the context of five levels.
- 7 **Finding for this asset:** The asset is automatically taken from the Work Item from which it was created.
- 8 **Description of the finding:** The "Description of the finding" should contain as much information and input as possible, for example, how the *Finding* was discovered. Furthermore, conclusions about cause and effect may be drawn.
- 9 **Priority of the Finding:** A priority can be assigned to the *Finding*, which can later be used for evaluations on dashboards, for example.
- 10 **Status change:** The Editor Measure can then switch to the "Treatment" status. For more information on the status change, see [View & process Finding](#).

After the status change, the window can be closed.

The Tester can then return to *Control Testing* and continue with the documentation of *Control Testing*. [Tester - Perform & evaluate Control Testing](#)

2.13 Editor Domain Specific

An "Editor Domain Specific" is a user who performs all tasks (creation, documentation, etc.) for a specific domain not within the context of Risk, Measure and Control. These domains have separate editors dedicated to them.

This user profile therefore requires that all Users assigned *Editor Domain Specific* possess a specific set of knowledge for their domain in order to be able to perform the tasks properly.

The "Editor Domain Specific" will be abbreviated as *Editor DS* in the following chapters.

The Editor DS has the following preparatory task:

- [Define & create a Category of Personal Data](#)

An Editor in BIC GRC has the following tasks:

- [Determine & create Processing Activity](#)
- [Define & create Data Subject Data](#)
- [Define & create Data Processing Agreement](#)
- [Determine & create Transfer Impact Assessment](#)
- [Determine & create Privacy Impact Assessment](#)

- [Define & create Privacy Request](#)
- [Review & edit Privacy Requests](#)
- [Define & create Management Review](#)
- [Perform & review Management Review](#)
- [Identify & create Findings](#)

The *Editor DS* can also create additional Work Items in BIC GRC. While this is beyond their primary responsibility, we will refer to other user profiles at this point:

- [Define & create Objectives](#)
- [Define & create Milestone](#)
- [Derive & create Control](#)
- [Define & create Measure](#)

2.13.1 Define & Create Category of Personal Data

Certain *Create Category of Personal Data* are more sensitive than others and therefore require particularly high levels of protection. For this reason, the Data Protection Editor should create these categories before other users begin working in the Data Protection module.

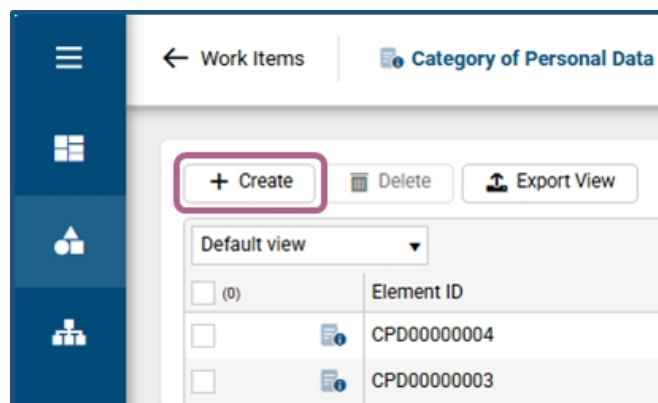
Step 1: Create Category of Personal Data

The EditorDS can create *Create Category of Personal Data* in several places in BIC GRC.

1. Creation via tile

The Editor navigates to **Work Items >> Category of Personal Data >> "Create"** via the sidebar.

A new window will then open automatically.



2. Creation from the "Data Subject Data" Work Item

A *Create Category of Personal Data* can be created by the Responsible Editor from the Work Item "Processing Activity."

To create it, a new *Create Category of Personal Data* Work Item is created in the "Categorization" tab using the icon **+**.

Step 2: Enter details

Category of Personal Data Details

Obsolete

Status

Active

1

Name of the Category

Marketing and communication data from customers and prospects

(EN)

2

contains Special Categories of Personal Data

3

Data Types

Name	E...	
Address		
First name		
Phone number		
Email address		
Last name		

4

Additional Data Types

As part of marketing and communication activities, additional information on thematic interests, responses to marketing measures, and times of contact may also be processed.

(295/5000)

6

Assignment Informational Asset

Name	Asset Type	End-user...	
Kundenstammdaten	Primary Asset		

5

Save

Close

1 **Category name:** The first step should be to enter a short but meaningful name for the *Create Category of Personal Data*. This "name" in combination with the "Element ID" makes the *Create Category of Personal Data* unique.

2 **Contains special data:** The "Contains special data" checkbox indicates whether this category contains sensitive data within the meaning of Art. 9 GDPR. If this is the case, the Editor must click this checkbox.

3 **Data type:** They can use the icon  as a medium to select one or more suitable data types from a GRC Framework.

4 **Additional Data Types:** In the text field, the Editor can register "Additional Data Types" in addition to those mentioned above.

These include, for example, "Last name," "First name," "date of birth," etc.

5 **Save:** Once all the necessary information has been entered, the Work Item can be saved for the first time. Step 6 must then be performed before the Work Item is saved again and the window is closed manually.

6 **Assignment of information asset:** The Editor DS can select an asset from the asset hierarchy in which the data is processed.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request](#).

The status of the *Create Category of Personal Data* is "Active" after the first save operation. The Editor may continue to make changes in the "Active" status in exceptional cases.

2.13.2 Determine & create Processing Activity

As part of their duties, the Editor must register, evaluate, and handle *Processing Activities* in BIC GRC.

According to Art. 30 GDPR, every company must maintain a record of all *Processing Activities* —i.e., structured documentation of where and how Personal Data is processed.

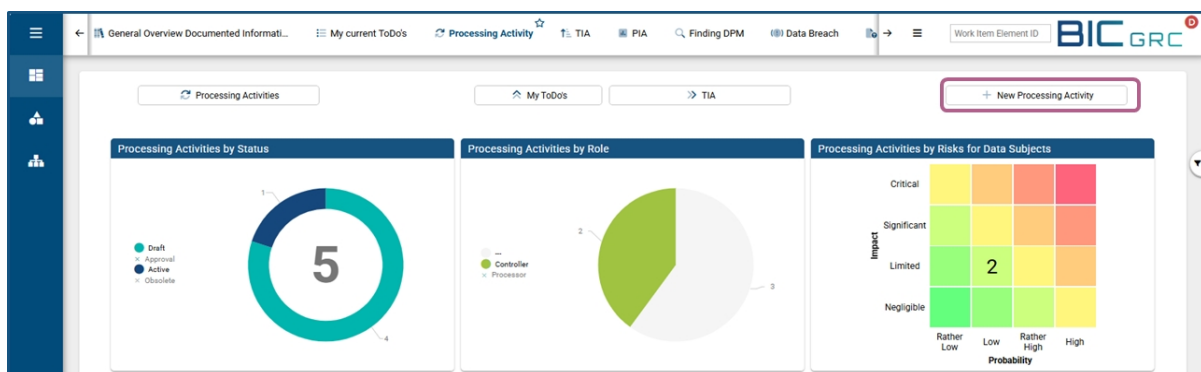
Step 1: Create Processing Activity

The Editor DS can create *Processing Activities* in several places in BIC GRC.

1. Create via the "Processing Activity" Dashboard

The Editor navigates via the sidebar to **Dashboards >> Processing Activity >> "New Processing Activity."**

A new *Processing Activity* is created using a button in the upper right corner of the window.

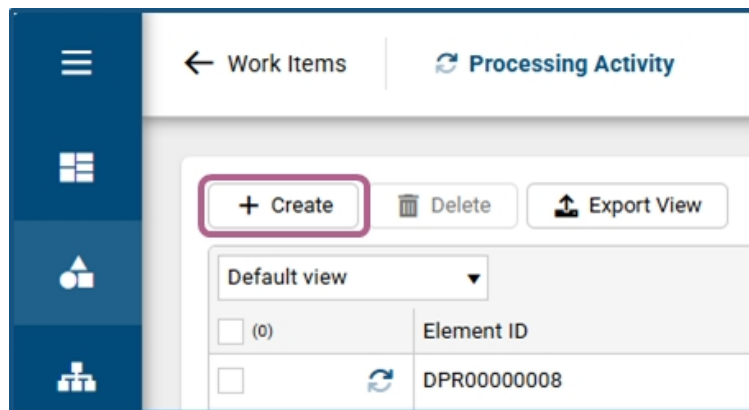


A new window then opens automatically.

2. Creation via tile

The Editor navigates to **Work Items >> Processing Activity >> "Create"** via the sidebar.

A new window then opens automatically.



Step 2: Define details

Processing Activity Details

Status Draft

1

* Name

Customer and prospect communication in marketing (neutral)

Context

Context

2

Legal Entity

Name	Asset Type	End-us...	
4wheels Automotive Leasing GmbH	Business Structure		

3

You have unsaved changes.

Save

Close

1 Name: The first step should be to enter a short but meaningful name for the *Processing Activity*. This "name" in combination with the "Element ID" makes the *Processing Activity* unique.

2 Legal Entity: A "Legal Entity" must be assigned to the *Processing Activity*.

Only one Business Unit with the tag "Company" can be assigned to the scope of application.

3 Save process: Once the necessary information has been entered, the *Processing Activity* can be saved for the first time.

Step 3: Enter Additional Information

Processing Activity Details Next

Element ID: DPR00000012 Status: Draft

* Name: Customer and prospect communication in marketing (neutral)

1 * Evaluation Cycle: half Yearly Next Evaluation: 05/08/2026

Draft Approval Active

Context LIA Risks & TOMs Check PIA Comments Discussion Work Item Links Documentation (0)

Context

Legal Entity

Name	Asset Type	End-user ...
4wheels Automotive Leasing GmbH	Business Structure	

2 **Editor** EditorDomainSpecific DPM (DPM_E_)

2 **Data Protection Officer** ApproverDomainSpecific DPM (DP_)

Created by
EditorDomainSpecific DPM

3 **Further Contacts**
Please record further contact persons or organizations relevant to the Processing Activity here.
(0/5000)

4 **Affected Processes**

Name	Asset Type	End-user...
Process 4	Primary Asset	

5 **Data Subject Data**

Name	Status	Category of D...
Customer data and prospect data (marketing)	Active	Prospects ...

6 **Groups of Processing Activities**

Name	Catalog	E...
Customer Data	Groups of Proces...	

Save Close

- 1 **Evaluation Cycle:** The Editor must enter an "Evaluation Cycle." The Evaluation Cycle specifies how often a *Processing Activity* is switched back to "Draft" status in order to evaluate the *Processing Activity* at regular intervals.

The attribute field "Next evaluation on" is set automatically by BIC GRC and is Read Only.

- 2 **Editor:** The Editor is automatically stored in the "Processor" field and can still be changed. An "Approver" who is responsible for approving the *Processing Activity* must be stored by the Editor.

This User is searched for and linked using the icon or suggested by entering the User's name in the attribute.

Only users who have the "Processor DS" user profile are suggested to the Processor DS.

- 3 **Further contacts:** The Editor can also document additional contacts in writing if they are not Users in BIC GRC.

These persons can be documented for reference, and access to the Work Item is managed centrally.

- 4 **Affected processes:** The Editor DS must assign the business processes in which Personal Data is processed. The Editor is permitted to link only processes.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request..](#)

- 5 **Data Subject Data:** The Editor DS must create a new Work Item of the type *Data Subject Data* using the icon . For more information on creating the Work Item, see [Editor DS - Define & Create Data Subject Data.](#)

- 6 **Groups of Processing Activities:** In addition, an Assignment to a higher-level grouping or Category of Processing Activities must be made. To do this, the Editor links to a suitable GRC Framework element using the icon  to a suitable GRC Framework Item.

Processing Activity Details

Next

Element ID

DPR00000012

Status

Draft

Name

Customer and prospect communication in marketing

(neutral)

Evaluation Cycle

half Yearly

Next Evaluation

05/08/2026

Draft

Approval

Active

Context

LIA

Risks & TOMs

Check PIA

Comments

Discussion

Work Item Links

Documentation (0)

7

Description of the Processing Activity

As part of this processing activity, personal data of customers and interested parties is processed for the purpose of carrying out marketing and communication measures.

The processing includes, in particular, the planning, implementation, and evaluation of marketing campaigns, as well as direct communication with

(371/5000)

Purpose of Processing

The purpose of processing is to plan, implement, and evaluate marketing and communication measures aimed at customers and interested parties.

This includes, in particular, providing information about products, services, and offers, as well as maintaining customer relationships via various communication channels.

(314/5000)

Statement of the Data Protection Officer

The data protection officer was involved in the design and documentation of the processing activity.

From a data protection perspective, there are currently no fundamental objections to the processing activity being carried out in the manner described, provided that the planned technical and organizational measures are implemented and regularly reviewed.

(357/5000)

Description of the Legal Basis

The processing of personal data is based on Art. 6 (1) lit. f GDPR (legitimate interest) and, where necessary, on Art. 6 (1) lit. a GDPR (consent of the data subject).

The legitimate interest consists in the implementation of marketing and communication measures for customer loyalty and sales promotion.

(394/5000)

Save

Close

7 Description: The Editor DS must enter descriptions and information in several text fields. These include:

- Description of the Processing Activity: A brief, understandable Summary of the type of data processing.
- Purpose of Processing: Specifies the specific objective for which the Personal Data is being processed.
- Opinion of the Data Protection Officer: To be completed by the Data Protection Officer.
- Description of the Legal Basis: Specification of the legal basis for data processing in accordance with Art. 6 or, if applicable, Art. 9 GDPR.

GBTEC Austria GmbH

136/226

Processing Activity Details Next 🔍

Element ID: DPR0000012 Status: Draft

* Name: Customer and prospect communication in marketing (neutral)

* Evaluation Cycle: half Yearly Next Evaluation: 05/08/2026

Draft Approval Active

Context LIA Risks & TOMs Check PIA Comments Discussion Work Item Links Documentation (0)

8 Responsible Business Unit

Name	Asset Type	End-user ...
Marketing	Business Structure	

9 Functional Contact

Head of Marketing (17/500)

10 Start of Processing

02/02/2026

11 Data is processed as

Controller

12 File Reference

DPM-VT-MARKETING-001 (20/100)

13 Processing Activity as Controller

Joint Controllers

Element Name	Name
Customer.cus00	Example Customer

Own Processors

No existing mapping.

Data Processing Agreement

Name	Status
DPA - Customer and prospect communication in marketing	Approval

14 Data Transfer

☒ Data Transmission to Third Countries

Transfer Impact Assessment

Name	Status	Type of guarant...
TIA - Customer and prospect communication in marketing	Draft	Adequacy d...

15 Save Close

- 8 Responsible Business Unit:** Using the icon , the Editor must select a Business Unit that is responsible for processing the data.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request.](#)

- 9 Functional contact:** The Editor DS must specify the name or role of the person who is technically responsible for processing, if there is a suitable person.

10 Start of processing: By using a medium to enter the date, you can specify when the processing of the data actually began.

11 Data is processed as: It must be specified whether the data is processed as a Controller or as a Processor.

Depending on the selection under "Data is processed as," a different section is displayed to the Editor.

- Controller: Enter "Joint Controllers" and "Processors." Once a "Processor" has been entered, a Work Item Data Processing Agreement can be created.
- Processor: "Controller" must be stored so that additional information can be transferred from the GRC framework. Here, too, a Processor is required and a Work Item Data Processing Agreement must be created.

For more information on creation, see [Editor_DS - Define & create Data Processing Agreement](#).

For the link to "Joint Controllers," "Processors," and "Controllers," please note that the appropriate tags must have been assigned in the corresponding GRC Framework.

12 File Reference: By means of a "File Reference," the Editor can ensure that an internal reference number is specified for administration or linking to files, processes, or documents—for Audits, for example.

13 Processing Activity as Controller: This section specifies the role of the organization in this processing activity – solely responsible, jointly responsible, or involving Processors?

- Joint Controllers: This Processing Activity is carried out jointly with at least one other Organization.
- Own Processors: Organizations that process Personal Data exclusively on the instructions of the Controller must be recorded here.

The links to be provided lead to the GRC Framework "Customers," "Suppliers," and "Partners & Authorities."

- Data Processing Agreement: An individual *Data Processing Agreement* can be created. For more information on how to create one, see [Editor_DS - Define & Create Data Processing Agreement](#).

14 Data transfer: If the data has also been transferred to third countries, this is indicated by clicking the checkbox. If the checkbox has been clicked, a new link appears below it. The Editor DS creates a new Work Item of the type *Transfer Impact Assessment* using the icon



. For more information on creating the Work Item, see [Editor_DS - Datentransfer-Determine & create Transfer Impact Assessment](#).

15 Saving process: After entering the necessary information, the *Processing Activity* can be saved again before continuing with the "Legitimate Interest Assessment" LIA.

Step 4: Document the Legitimate Interest Assessment

To continue processing the *Processing Activity*, the Editor DS must switch to the "LIA" tab.

Processing Activity Details

Element ID

DPR00000012

Status

Draft

* Name

Customer and prospect communication in marketing

(neutral)

* Evaluation Cycle

half Yearly

Next Evaluation

05/08/2026

Draft

Approval

Active

Context

LIA

Risks & TOMs

Check PIA

Comments

Discussion

Work Item Links

Documentation (0)

1

Legitimate Interest Assessment

☒ The processing activity is absolutely necessary.

☒ This is the least intrusive way to achieve the wanted result.

☒ A balancing-test was conducted and I am confident, that the individual's interests do not override those legitimate interests.

☒ The Data Subjects data will be used in a way they can reasonably expect.

☐ Regarding childrens data, extra care will be taken to ensure that their interests are protected.

☒ An opt-out is offered.

☒ Information about legitimate interests is included in our privacy information.

2

Further Considerations

Personal data is processed within the scope of standard marketing and communication measures aimed at customers and interested parties.

The scope, type, and purpose of the processing are limited to what is necessary and are proportionate to the legitimate interests of the company.

The interests and rights of the data subjects are taken into account through transparent information, clear purpose limitation, and the possibility of objection at any time.

(558/5000)

3

Save

Close

- Legitimate Interest Assessment:** The Editor must perform a "Legitimate Interest Assessment." Questions have been prepared for this purpose, which the Data Protection Officer can confirm to the best of their knowledge and belief by clicking on the respective checkbox.
- Further Considerations:** After the Assessment, the Editor can enter additional notes on the Assessment in the text field.
- Saving process:** After entering the necessary information, the *Processing Activity* can be saved again before continuing with the specification of potential risks.

Step 5: Evaluation of risks

To continue processing the *Processing Activity*, the Editor must switch to the "Risks & TOMs" tab.

GBTEC Austria GmbH

139/226

Processing Activity Details

Next

Element ID

DPR0000012

Status

Draft

Name

Customer and prospect communication in marketing

(neutral)

Evaluation Cycle

half Yearly

Next Evaluation

05/08/2026

Draft

Approval

Active

Context

LIA

Risks & TOMs

Check PIA

Comments

Discussion

Work Item Links

Documentation (0)

Risks for Data Subjects

Impact

Critical

Significant

Limited

Negligible

Low

Rather Low

Rather High

High

Probability

Gross Risk

Net Risk

1

Reason for Gross Risk Evaluation

As part of marketing and communication activities, personal data of customers and interested parties is processed regularly and on a large scale. Due to the number of systems, processes, and people involved, there is a fundamentally increased risk of data protection violations, such as unauthorized access, incorrect transmission of information, or unauthorized contact.

(372/5000)

Reason for Net Risk Evaluation

The technical and organizational measures implemented significantly reduce the risk to the rights and freedoms of the individuals concerned. In particular, access restrictions, clear role and authorization concepts, documented processes for exercising the rights of data subjects, and transparent data protection information reduce the likelihood of relevant data breaches occurring.

(384/5000)

Measures & Controls

Technical & Organizational Measures

No existing mapping.

Controls

Name

Status

D...

Review of deletion periods for marketing data

Planning

Save

Close

- Gross & Net Risk:** First, the Editor enters a Gross Evaluation for the risk from the Processing Activity. They can then perform a Net Evaluation.
- Reason for Risk Evaluation:** The Editor DS must specify how they arrived at both the gross and net risk assessments. There are two different text fields available for this purpose, which they must fill in.
- Measures:** The Editor should link or [Derive & Create Measure](#).

If the Editor DS wants to link a *Measure*, only *Measures* selected as "Technical

GBTEC Austria GmbH

140/226

Measure" or "Organizational Measure" will be displayed.

4

Controls: The Editor should link or [Derive & Create Control](#).

If there are general *Measures* and *Controls* for the Data Protection module on the Asset, these are automatically assigned by BIC GRC.

5

Saving process: After the necessary information has been entered, the *Processing Activity* can be saved again before continuing.

Step 6: Check mandatory privacy impact assessment

To continue processing the *Processing Activity*, the Editor DS must switch to the "PIA review" tab.

Processing Activity Details

Element ID

DPR00000012

Status

Draft

Name

Customer and prospect communication in marketing

(neutral)

Evaluation Cycle

half Yearly

Next Evaluation

05/08/2026

Draft

Approval

Active

Context

LIA

Risks & TOMs

Check PIA

Comments

Discussion

Work Item Links

Documentation (0)

Check for mandatory Privacy Impact Assessment

1 Is there a White- or Blacklist?

—

4 Identifier

Please state the identifier for the exception.

(0/500)

5

☐ Does the automatic processing activity perform evaluation and scoring, including forecasts and profiling?
 ☐ Does the processing activity give rise to the possibility of systematic surveillance of individuals in publicly accessible areas?
 ☐ Does the processing activity involve the use of innovative technologies or novel organisational solutions?
 ☐ Does the processing activity involve the processing of special categories of personal data?
 ☐ Does the processing activity involve the processing of data of highly personal nature?
 ☐ Does the processing activity involve processing large (large scale) amounts of data?
 ☐ Does the processing activity directly compare or merge/combine data sets?
 ☐ Does the processing activity involve processing data of vulnerable data subjects?
 ☐ Are data subjects prevented from exercising a right or using a service or a contract?

6 A Privacy Impact Assessment is not necessarily required!

7 Decision PIA

PIA will be conducted

PIA will not be conducted

Privacy Impact Assessment

No existing mapping.

8

You have unsaved changes.

Save

Close

- 1 **White list or black list:** First, the Editor DS must specify whether the *Processing Activity* falls within the scope of the white list or black list for the Privacy Impact Assessment.

The blacklist is the officially published blacklist (risk processing) and the whitelist is the exempted processing.

- 2 **Country:** The Editor DS is shown a predefined selection of "countries" in which the competent data protection supervisory authority has compiled the list.
- 3 **Authority:** In addition, the Editor can specify the competent supervisory authority and related details in writing.

- 4 **Identifier:** Under the identifier, the Editor DS must document the exact name or number of the PIA-relevant Submission on the list.

Examples: "Blacklist submission no. 4: Extensive surveillance of publicly accessible areas" or "Whitelist item 7: Processing of Contact Details for appointment scheduling."

- 5 **Risk criteria:** The review is based on various questions regarding the risk criteria. The Editor indicates what applies by clicking a checkbox.

These questions are based on recommendations from the Article 29 Data Protection Working Party / EDPB, which represent typical indicators of a "presumed high risk."

- 6 **Recommendation:** Depending on the selection of "white list or black list" and the entries for the risk criteria, a recommendation is given by means of a label. The recommendation indicates whether BIC GRC recommends creating a Work Item for a Privacy Impact Assessment.

- 7 **Decision:** The Editor DS can follow this recommendation or make an alternative decision. The decision must be specified in the "PIA decision" attribute.

Depending on the selection, if the decision is "PIA will be performed," a new *Privacy Impact Assessment* Work Item must be created. For more information on creation, see [Editor DS - Determine & Create Privacy Impact Assessment](#).

- 8 **Saving process:** After the necessary information has been entered, the *Processing Activity* can be saved again before continuing with the specification of potential risks.

Once the relevant data and information has been entered in all tabs, the Editor DS can be moved to the next status, "Approval." The Data Protection Officer receives notification of the status change via a medium.

2.13.3 Define & create Data Subject Data

Data Subject Data must be created by a Editor DS from a *Processing Activity*.

Step 1: Create Data Subject Data

The *Data Subject Data* can be created exclusively by the responsible Editor from the *Processing Activity* Work Item.

To create it, a new *Data Subject Data* Work Item is created in the "Context" tab.

Step 2: Categorize Data Subject Data

Data Subject Data Details

Status ● Draft

* Name 1 Customer data and prospect data (marketing) (neutral)

Categorization

Assignment

2 **Category of Data Subjects**

Name	Category	E...	
 Prospects	Normal pr...		

3 **Category of personal Data**

Name of the Category	Additional Data Types	Last Modi...	
 Marketing and communication data from customers and prospects	As part of marketing and co...	02/02/20...	 +

4 ⚠ You have unsaved changes. Save Close

1 **Name:** The first step should be to enter a short but meaningful name for the *Data Subject Data*. This "name" in combination with the "Element ID" makes the *Data Subject Data* unique.

2 **Category of Data Subjects:** The Editor DS must select the "Categories of Data Subjects" from the appropriate GRC framework.

The GRC Framework can be expanded by authorized Users in BIC GRC.

3 **Category of personal Data:** The Editor DS should then specify the "Category of Personal Data." This is a Work Item that they can create or link to.

For more information on creation, see [Editor DS - Define & Create Category of Personal Data](#).

4 **Save:** Once all information has been entered, the *Data Subject Data* Work Item can be saved for the first time.

Step 3: Enter further details

Data Subject Data Details Next

Element ID: DSD00000008 Status: Draft

* Name: Customer data and prospect data (marketing) (neutral)

[Categorization](#)
[Storage & Transfer](#)
[Discussion](#)
[Work Item Links](#)
[Documentation \(0\)](#)

Assignment

Category of Data Subjects

Name	Category	E...	
Prospects	Normal pro...		

Category of personal Data

Name of the Category	Additional Data Types	Last Modifi...	
Marketing and communication data from customers and prospects	As part of marketing and comm...	02/02/202...	

Legal Basis of Data Processing

1 **Legal Basis**

* Consent of Data Subject X Legitimate Interest of the Controller X

Select...

2 **Concretization Legal Basis**

Personal data is processed for the purpose of marketing communication with customers and interested parties.
This is based on the company's legitimate interest in maintaining customer relationships and providing information about products and services.

Please consider conducting a Legitimate Interest Assessment!

Origin of Data

3 **Source**

* Data Subject X

Select...

4 **IT Systems**

Name	Asset Type	End-user...	
CRM Tool	Supporting Asset		

5 Save Close

- 1 **Legal Basis:** The Editor must select a "Legal Basis" from a predefined list. This involves selecting the appropriate legal permission standard in accordance with Art. 6 (or Art. 9 for special data) GDPR on which the data processing is based.

If "Other" is selected, the Editor can manually enter a Legal Basis in the text field that appears.

- 2 **Concretization of the Legal Basis:** After a "Legal Basis" has been selected, an explanation of the Legal Basis can be added.

This can be helpful in particularly complex legal relationships or when providing evidence to Authorities and auditors.

3

Source: The "origin of the data" can come from different sources:

- Data Subject
- Third Party: If the data originates from Third Parties, details can be documented manually in a separate text field.
- Internal: The Editor is provided with a link

4

IT Systems: Finally, an assignment can be made to the technical systems, applications, or databases in which the data concerned is processed or stored.

Only "Supporting Assets" with the tag "hardware," "software," or "network" can be stored.

5

Save: Once all information has been entered, the *Data Subject Data* Work Item can be saved.

Step 4: Enter storage information

Once all the entries from the previous steps have been completed, you can continue in the "Storage & Transfer" tab.

If the option "Other" is selected, the Editor DS can manually specify a Legal Basis in the text field that appears.

5 Controls: To ensure that the Deletion Concept is implemented, for example, a control can be stored voluntarily. For more information on creating *Controls*, see [Editor Control - Derive & Create Control](#).

6 Transfer Type: The Editor can specify either "Internal data transfer" and/or "External data transfer" or "None."

If one of the first two or both are selected, an additional link must be filled in for each. For "Internal Recipients," the link leads to assets with the tag "Business area," while for "External Recipients," it leads to "Customers," "Suppliers," and "Partners & Authorities."

7 Status change: Once all information has been entered, a status change to "Active" is executed in the upper right window.

After the status change, the Editor DS can continue with the documentation in the Work Item [Processing Activity - step 3](#).

2.13.4 Define & create Data Processing Agreement

The *Data Processing Agreement* is a contractual document that must be completed in accordance with Art. 28 GDPR when an Editor commissions an external service provider to process Personal Data on its behalf.

Step 1: Create the Data Processing Agreement

The *Data Processing Agreement* can only be created by the responsible Editor using the *Processing Activity* Work Item.

To create it, click on the icon  in the "Context" tab to create a new *Data Processing Agreement*.

Step 2: Describe the Data Processing Agreement

Data Processing Agreement Details

Status Draft

Contractual Details

Data Processing Agreement

1
Subject of the Contract

The subject matter of this data processing agreement is the processing of personal data on behalf of the controller within the scope of customer and prospect communication in marketing.
The contractor provides IT-supported services for the provision, operation, and maintenance of systems used for marketing and communication purposes, in particular CRM and marketing automation systems.

2
Contractual Partner

Element Name	Name
 Supplier.sup00	Example Supplier

3
Further details on Contractual Partner

The contractual partner shall process personal data exclusively on the documented instructions of the controller. Processing shall be carried out within the scope of the contractually agreed services and in compliance with the agreed technical and organizational measures in accordance with Art. 32 GDPR.

Further details on Subcontractors

The use of subcontractors is regulated by contract and only takes place after prior notification or approval by the responsible party. Subcontractors are contractually obliged to comply with equivalent data protection and security requirements.

4
Valid from 02/02/2026
Valid to 27/02/2026

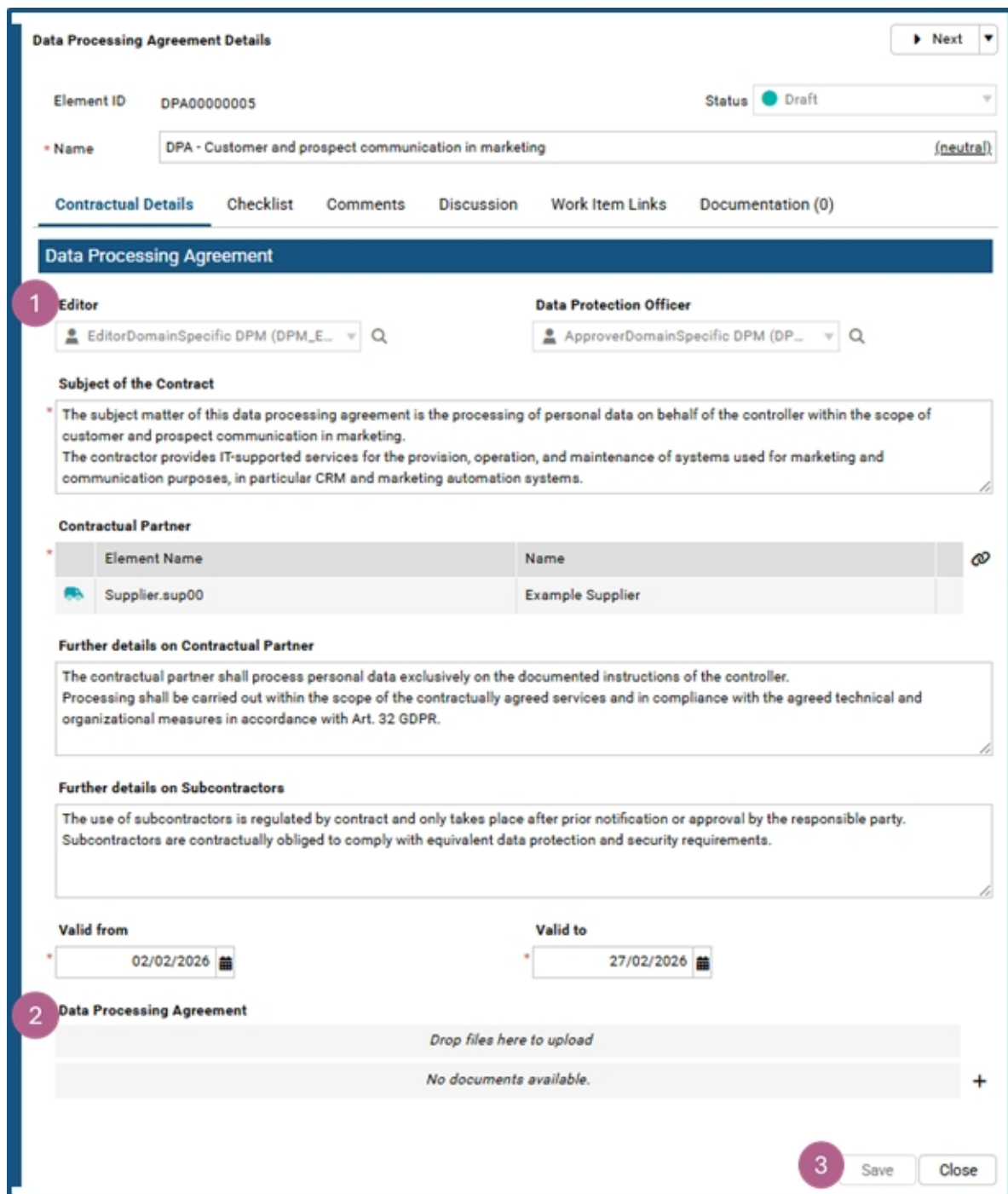
5
You have unsaved changes.
Save Close

- 1 **Subject matter of the contract:** The Editor DS must then record in writing what the subject matter of the contract is within the scope of the *Data Processing Agreement*.

Example: "Sending newsletters for 24 months."

- 2 **Contractual partner:** The Editor DS can select the appropriate "contractual partner" from three different GRC Frameworks if they have set the appropriate tag in the GRC Framework.
- 3 **Additional Information:** They can then store additional information about the contractual partner as well as information about associated subcontractors.
- 4 **Period:** Finally, the Editor must specify the period during which the *Data Processing Agreement* is valid.
- 5 **Save:** Once all the information has been entered, the *Data Processing Agreement* can be saved.

Step 3: Supplement the Data Processing Agreement



Data Processing Agreement Details Next

Element ID: DPA00000005 Status: Draft

Name: DPA - Customer and prospect communication in marketing (neutral)

Contractual Details Checklist Comments Discussion Work Item Links Documentation (0)

Data Processing Agreement

1 **Editor** Data Protection Officer

EditorDomainSpecific DPM (DPM_E... Search ApproverDomainSpecific DPM (DP... Search

Subject of the Contract

The subject matter of this data processing agreement is the processing of personal data on behalf of the controller within the scope of customer and prospect communication in marketing. The contractor provides IT-supported services for the provision, operation, and maintenance of systems used for marketing and communication purposes, in particular CRM and marketing automation systems.

Contractual Partner

Element Name	Name
Supplier.sup00	Example Supplier

Further details on Contractual Partner

The contractual partner shall process personal data exclusively on the documented instructions of the controller. Processing shall be carried out within the scope of the contractually agreed services and in compliance with the agreed technical and organizational measures in accordance with Art. 32 GDPR.

Further details on Subcontractors

The use of subcontractors is regulated by contract and only takes place after prior notification or approval by the responsible party. Subcontractors are contractually obliged to comply with equivalent data protection and security requirements.

Valid from: 02/02/2026 Valid to: 27/02/2026

2 **Data Processing Agreement**

Drop files here to upload

No documents available.

3 Save Close

1 **Editor:** The Creator is automatically transferred to the “Editor” user field and the “Data Protection Officer” is filled in with the (single) Approver DS in the Data Protection module. Neither of these can be changed after the save process.

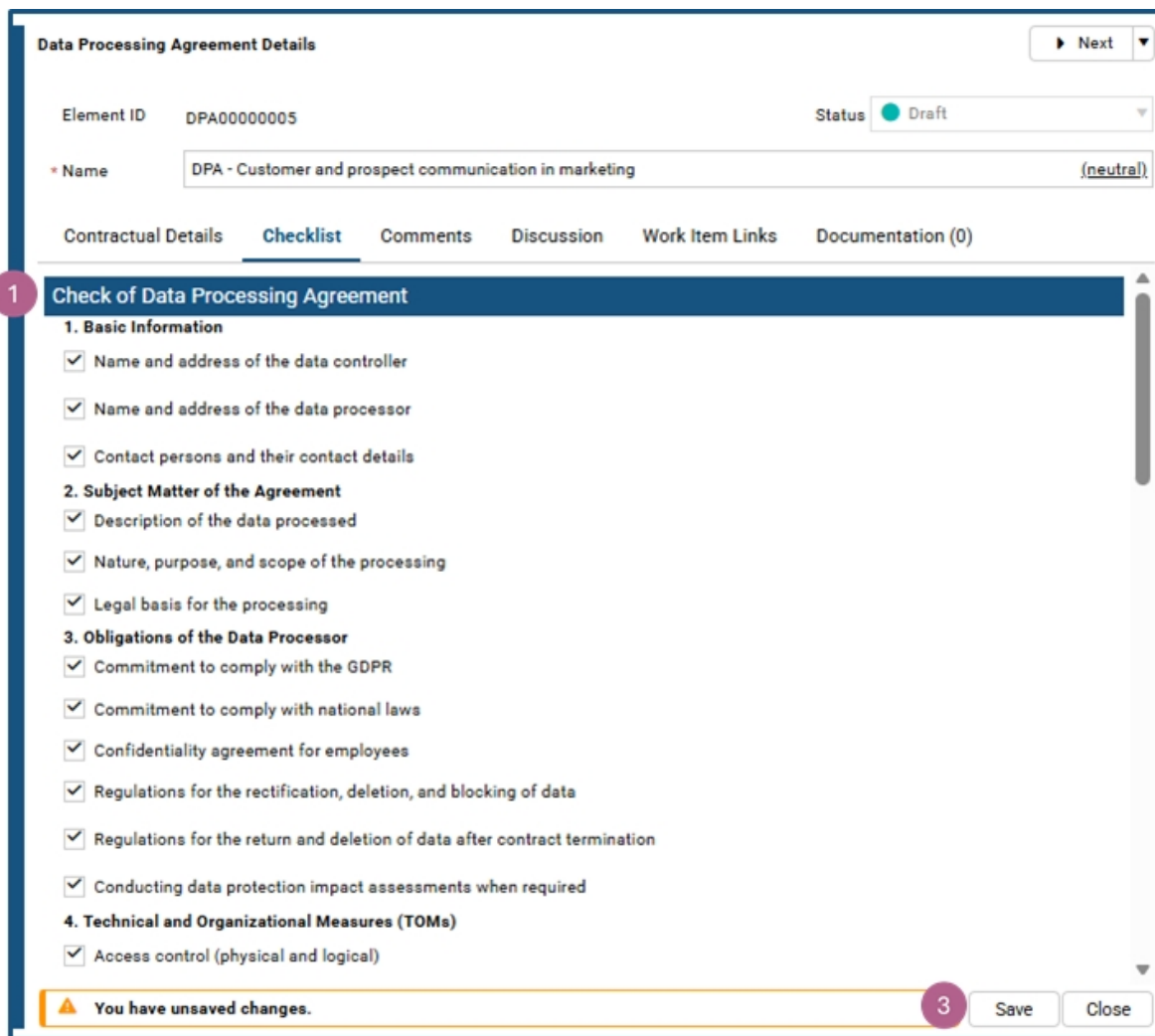
2 **Data Processing Agreement:** The “Data Processing Agreement” document can be stored in the Work Item.

If it is a file, it can be dragged from the desktop to the “Drag file here to upload” area, for example. The file is then linked in the attribute field.

- 3 **Save:** Once all information has been entered, the *Data Processing Agreement* can be saved.

Step 4: Go through the checklist

After submitting the document for the *Data Processing Agreement*, you can proceed to the “Checklist” tab.



The screenshot shows the 'Data Processing Agreement Details' form with the 'Checklist' tab selected. The form includes fields for 'Element ID' (DPA00000005), 'Status' (Draft), and 'Name' (DPA - Customer and prospect communication in marketing). The checklist is divided into four sections: 1. Basic Information, 2. Subject Matter of the Agreement, 3. Obligations of the Data Processor, and 4. Technical and Organizational Measures (TOMs). Each section contains several items with checkboxes, all of which are currently checked. A warning bar at the bottom indicates 'You have unsaved changes.' and there are 'Save' and 'Close' buttons.

- 1 **Check of Data Processing Agreement:** The Editor has access to a list that can be used to review the contract data processing relationship. The list contains topic blocks that can be confirmed by clicking on a checkbox.
- 2 **Additional provisions and comments:** If the Editor needs to add further notes or provisions that are not included in the list, these can be added manually in the text field.
- 3 **Status change:** Once all information has been entered, a status change to “Approval” is carried out in the upper right window.

The Data Protection Officer is notified of the status change by means of a notification.

2.13.5 Determine & create Transfer Impact Assessment

Transfer Impact Assessment must be created by a Editor DS when data has been transferred abroad.

Step 1: Create Transfer Impact Assessment

The *Transfer Impact Assessment* is created by the responsible Editor using the Work Item Processing Activity.

Data Transfer

☒ Data Transmission to Third Countries

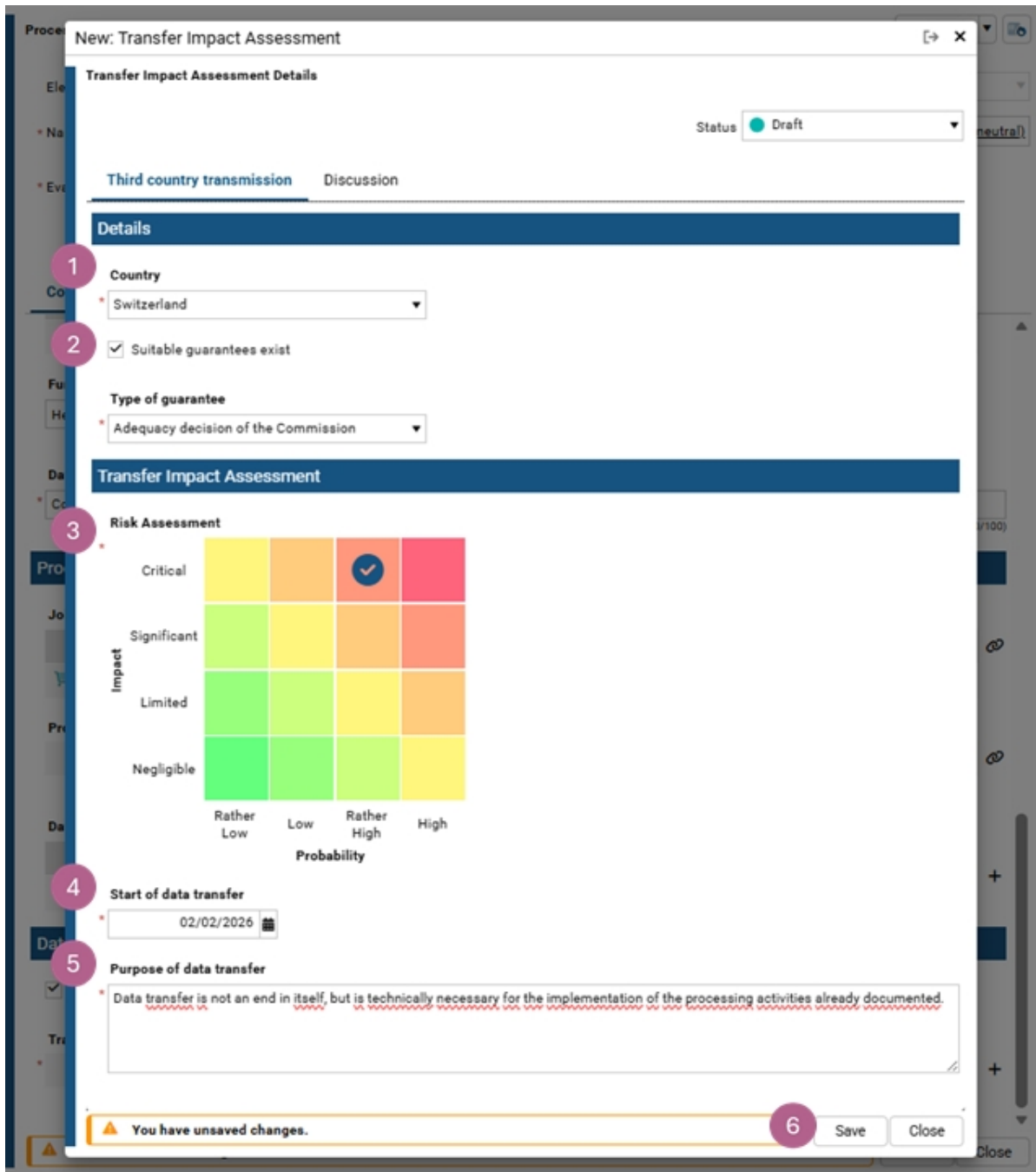
Transfer Impact Assessment

Name	Status	Type of guarant...
TIA - Customer and prospect communication in marketing	Draft	Adequacy d...

+

To create it, click the icon  in the "Context" tab to create a new *Transfer Impact Assessment*.

Step 2: Describe the Transfer Impact Assessment



The screenshot shows a web form titled "New: Transfer Impact Assessment". The form is divided into sections: "Transfer Impact Assessment Details", "Third country transmission", and "Discussion". The "Status" is set to "Draft".

1 Country: A dropdown menu showing "Switzerland".

2: A checkbox labeled "Suitable guarantees exist" is checked. Below it, a dropdown menu for "Type of guarantee" shows "Adequacy decision of the Commission".

3 Risk Assessment: A 4x4 grid with "Impact" on the y-axis (Critical, Significant, Limited, Negligible) and "Probability" on the x-axis (Rather Low, Low, Rather High, High). The cell for "Critical" and "Rather High" is highlighted in red and contains a blue checkmark.

4 Start of data transfer: A date field showing "02/02/2026".

5 Purpose of data transfer: A text area containing the text: "Data transfer is not an end in itself, but is technically necessary for the implementation of the processing activities already documented."

6: A "Save" button and a "Close" button at the bottom right. A warning message "You have unsaved changes." is displayed at the bottom left.

- 1 Country**: The Editor must specify the country to which the data was transferred. If the appropriate country is not in the list, select "Other" and an additional text field will appear in which the Editor can manually enter a country.
- 2 Guarantees**: The Editor DS should indicate if "Guarantees" are in place by clicking the checkbox. If the checkbox is clicked, an additional selection for "Type of guarantee" will appear.

Supplementary protective measures ("guarantees") are required, particularly for data transfers to third countries (outside the EEA), to ensure an appropriate level of data

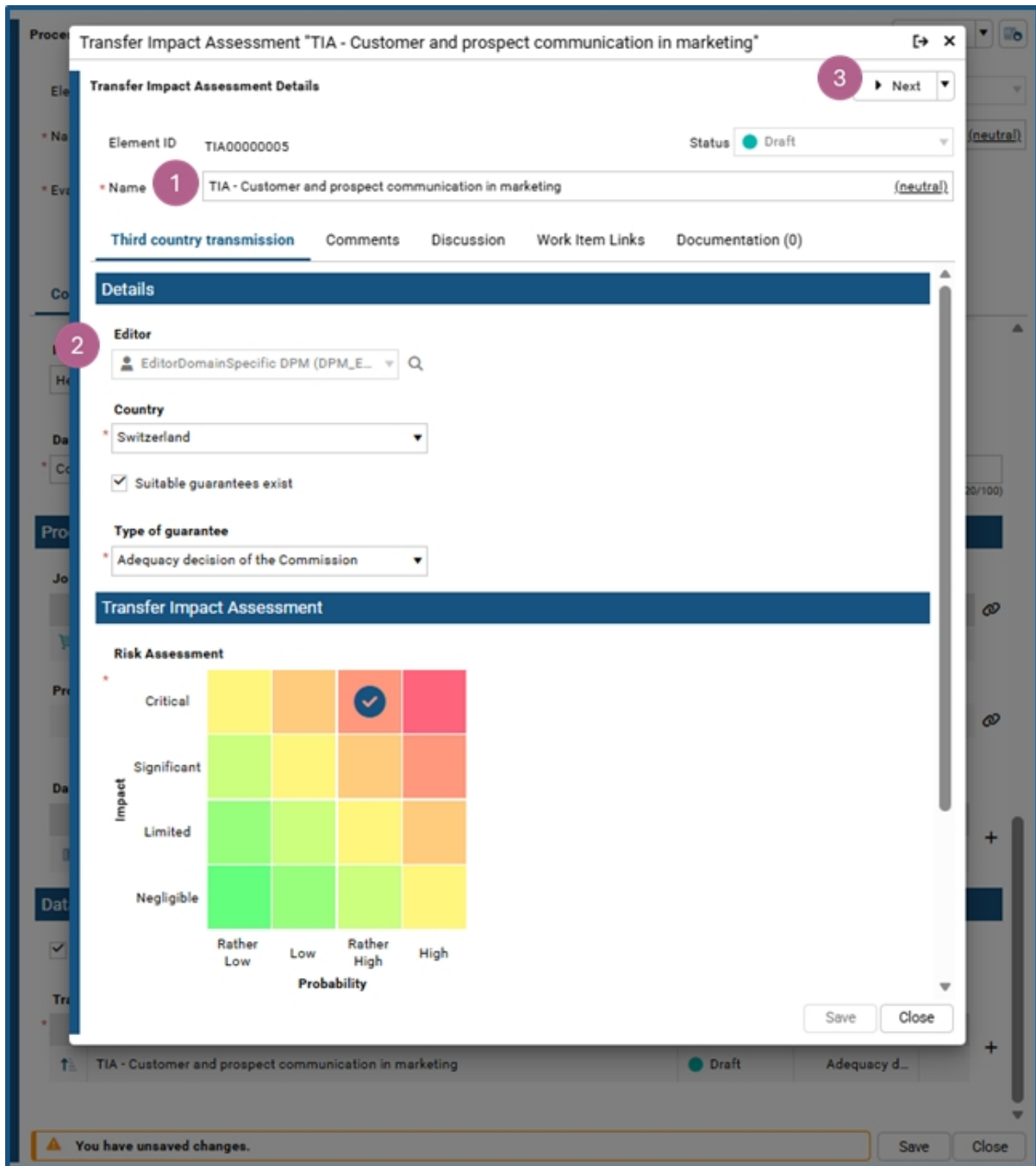
protection for Data Subjects.

- 3 **Transfer Impact Assessment:** The Editor must carry out a risk assessment. This is a simple evaluation in a standard 4x4 heat map.
- 4 **Start date of data transfer:** The date on which the data transfer began must be specified.
- 5 **Purpose of data transfer:** The purpose of the data transfer must then be specified.

Example: The purpose of "video surveillance of workplaces."

- 6 **Save:** Once all the information has been entered, the *Transfer Impact Assessment* can be saved for the first time.

Step 3: Finalize the Transfer Impact Assessment



Transfer Impact Assessment "TIA - Customer and prospect communication in marketing"

Transfer Impact Assessment Details

Element ID: TIA00000005 Status: Draft

Name: TIA - Customer and prospect communication in marketing (neutral)

Third country transmission Comments Discussion Work Item Links Documentation (0)

Details

Editor: EditorDomainSpecific DPM (DPM_E...)

Country: Switzerland

☒ Suitable guarantees exist

Type of guarantee: Adequacy decision of the Commission

Transfer Impact Assessment

Risk Assessment

Critical			✓	
Significant				
Limited				
Negligible				
	Rather Low	Low	Rather High	High
	Probability			

Save Close

TIA - Customer and prospect communication in marketing Draft Adequacy d...

You have unsaved changes. Save Close

1 **Name:** The "Name" is set automatically by BIC GRC and is a combination of the abbreviation of the Work Item Type "TIA" and the "Name" of the associated Work Item *Processing Activity*.

2 **Editor:** In addition to the "Name," the "Editor" is also automatically set to the current User after the save process.

The "Editor" is now Read Only.

3 **Status change:** After all information has been entered, a status transition to "Completed" is executed in the upper right window.

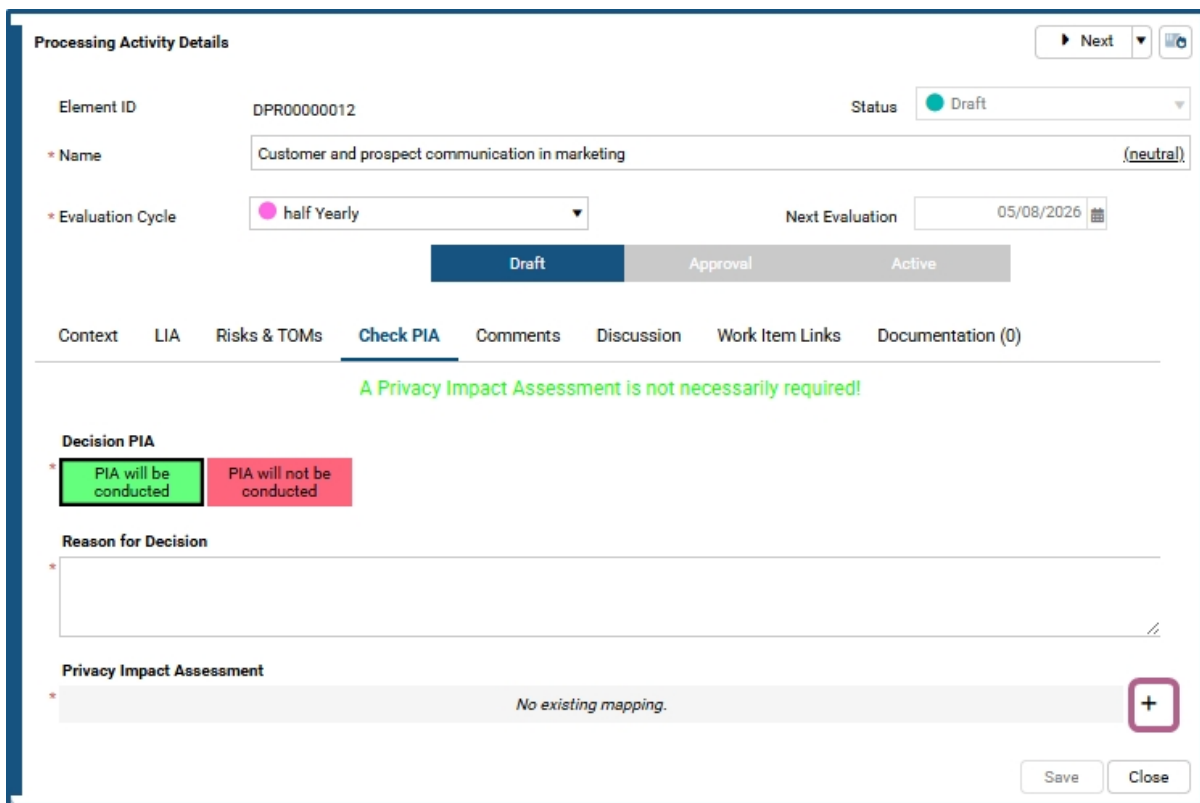
Approval is not required.

2.13.6 Determine & create Privacy Impact Assessment

Privacy Impact Assessments are a mandatory review procedure under Art. 35 GDPR that must be carried out if scheduled data processing is likely to pose a high risk to the rights and freedoms of natural persons.

Step 1: Create a Privacy Impact Assessment

The *Privacy Impact Assessment* can be created exclusively by the responsible Editor from the *Processing Activity Work Item*.



Processing Activity Details

Element ID: DPR00000012 Status: Draft

* Name: Customer and prospect communication in marketing (neutral)

* Evaluation Cycle: half Yearly Next Evaluation: 05/08/2026

Draft Approval Active

Context LIA Risks & TOMs **Check PIA** Comments Discussion Work Item Links Documentation (0)

A Privacy Impact Assessment is not necessarily required!

Decision PIA

* PIA will be conducted PIA will not be conducted

Reason for Decision

*

Privacy Impact Assessment

* No existing mapping. +

Save Close

To create it, a new *Privacy Impact Assessment* is created in the "PIA review" tab.

Step 2: Describe the Privacy Impact Assessment

Privacy Impact Assessment Details

Status ● Draft

Description

Description

1 **Description**

* The data protection impact assessment relates to the processing activity "customer and prospect communication in marketing."
As part of this processing, personal data of customers and prospects is processed for the purpose of carrying out marketing and communication measures. Processing is based on legitimate interests and, where necessary, on the consent of the data subjects.

2 You have unsaved changes. Save Close

- 1 **Description:** The Editor must describe the impact and risk to the rights and freedoms of individuals.
- 2 **Save:** Once all information has been entered, the *Privacy Impact Assessment* can be saved for the first time.

Step 3: Finalize the Privacy Impact Assessment

Privacy Impact Assessment Details Next

Element ID: PIA00000007 Status: Draft

* Name **1** PIA - Customer and prospect communication in marketing (neutral)

◀ **Description** Legal Assessment Risk Analysis Comments Discussion Work Item Links Documer ▶

Description

2 Editor EditorDomainSpecific DPM (DPM_E...) **2** Data Protection Officer ApproverDomainSpecific DPM (DP...

3 Further Contributors Enter search text

Description

* The data protection impact assessment relates to the processing activity "customer and prospect communication in marketing." As part of this processing, personal data of customers and prospects is processed for the purpose of carrying out marketing and communication measures. Processing is based on legitimate interests and, where necessary, on the consent of the data subjects.

4 ☒ Was the advice of the DPO sought?

5 ☐ Were the views of data subjects or their representatives sought, where appropriate?

6 Save Close

1 Name: The "Name" is set automatically by BIC GRC and is a combination of the abbreviation of the Work Item Type "PIA" and the "Name" of the associated Work Item *Processing Activity*.

2 Responsible: In addition to the "Name," the "Editor" and "Data Protection Officer" is also automatically set with the current User or the sole Approver after the save process.

The "Editor" is now Read Only.

3 Further Contributors: Using the icon , the Editor DS can designate further "Contributors" in BIC GRC.

4 Data Protection Officer involved?: If the Data Protection Officer has been involved, this checkbox can be clicked.

5 Views Obtained: Furthermore, a checkbox can be used as a medium to indicate whether the views of Data Subjects or representatives of Data Subjects have been obtained.

6 Save: Once all information has been entered, the *Privacy Impact Assessment* can be saved.

Step 4: Perform legal evaluation

Once the description of the *Privacy Impact Assessment* has been completed, the Editor can switch to the "Legal Evaluation" tab.

Privacy Impact Assessment Details Next

Element ID: PIA00000007 Status: Draft

* Name: PIA - Customer and prospect communication in marketing (neutral)

◀ Description **Legal Assessment** Risk Analysis Comments Discussion Work Item Links Documents ▶

1 Assessment of Proportionality & Necessity

☐ There is a legislation, contract or economical necessity to process personal data

☐ There are no other possibility besides a processing and no milder means exist that fulfill the same purpose

☐ It is necessary to use personal data and it is not possible to use metadata to fulfill the same purpose

☒ There is only personal data processed that is absolutely necessary and a data reduction is not possible

Explanation - Data reduction data subjects

*

☐ There are only data categories processed that are absolutely necessary

☐ The reason to process the data has been clearly defined and there is a valid legal basis

☐ The storage duration of processed data has been defined and involves only necessary data

☐ The access on processed data by staff is restricted and absolutely necessary

2 Annotations Proportionality & Necessity

Please summarize the assessment in a few words.

Assessment of legislative and contract requirements, measure assessment

☐ Legislative and contract risks for this processing are identified and are fulfilled

3 You have unsaved changes. Save Close

- 1 Evaluation:** The Data Protection Officer performs an evaluation based on "Proportionality & Necessity" and "Legal and Contractual Requirements." A number of questions are available to assist them in this evaluation.

If a question applies and the Editor clicks the checkbox for this reason, a text field appears below the question where an explanation must be entered.

- 2 Notes:** After the Editor has clicked the appropriate checkboxes, they should leave a short note at the end of the questions summarizing the respective evaluation in a few words.

- 3 **Save:** Once all the information has been entered, the *Privacy Impact Assessment* can be saved for the first time.

Step 5: Perform Risk Analysis

Once the legal evaluation has been performed, the Editor can switch to the "Risk Analysis" tab.

Privacy Impact Assessment Details

Next

Element ID

PIA00000007

Status

Draft

Name

PIA - Customer and prospect communication in marketing

(neutral)

Description

Legal Assessment

Risk Analysis

Comments

Discussion

Work Item Links

Docume

1 Confidentiality

Critical				
Significant				G
Limited			N	
Negligible				
	Low	Rather Low	Rather High	High

G

 Gross Evaluation

N

 Net Evaluation

Potential Threats

Potential Impacts

1 Integrity

Save

Close

- 1 **Evaluation:** Following the legal assessment, a Risk Analysis should be performed. This involves the following overarching topics

- Confidentiality
- Integrity
- Availability
- Data Minimization
- Non-chaining

- Transparency for Data Subjects
- Intervenability

Perform your own evaluation based on gross and net. In addition, the Editor must also indicate in writing the potential impacts and risks of each evaluation.

2 **Measures:** The Editor should link or [derive & create Measure](#).

If the Editor DS wants to link a *Measure*, only *Measures* that have been specified as "Technical Measure" or "Organizational Measure" are displayed.

3 **Controls:** The Editor should link or [derive & create](#) Controls.

4 **Consultation?:** If the Risk Analysis identifies that there is a greater risk for Data Subjects, then a consultation with the data protection authority should be held.

If this checkbox is selected, the Editor must also specify the Date of Consultation and the results in writing.

5 **Status change:** Once all information has been entered, a status change to "Completed" is executed in the upper right window.

Approval is unnecessary.

Privacy Impact Assessment Details

5

Next

Element ID

PIA00000007

Status

Draft

Name

PIA - Customer and prospect communication in marketing

(neutral)

Description

Legal Assessment

Risk Analysis

Comments

Discussion

Work Item Links

Docume

Technical & Organisational Measures

2 Measure

Name	Status	D...	
Role-based and permission-based access control for marketing and CRM systems	Draft	i	+ -

3 Controls

Name	Status	D...	
Regular review of marketing data processing	Planning		+ -

4

☐ Prior Consultation with the Data Protection Authority is necessary

You have unsaved changes.

Save

Close

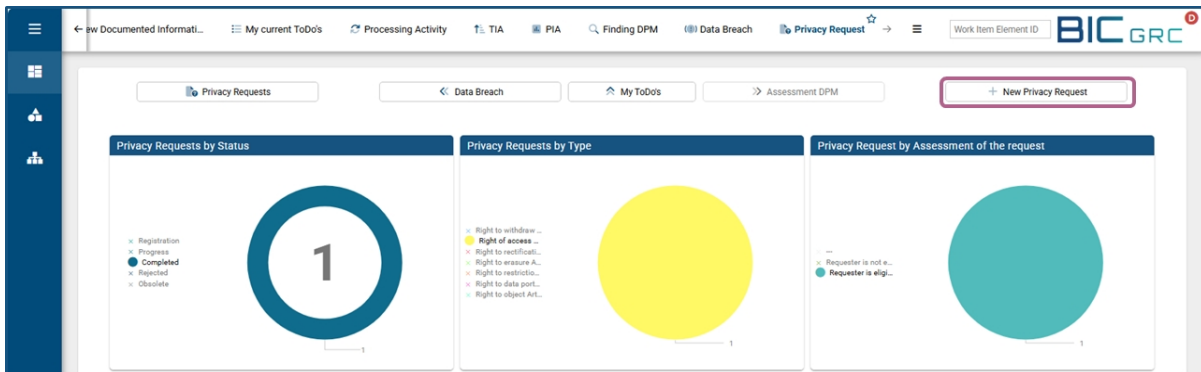
2.13.7 Define & create Privacy Request

A *Privacy Request* should be registered by an Editor in BIC GRC if a Data Subject (e.g., Customer, Employee, Supplier) asserts their rights under the GDPR. Registration of the request in BIC GRC helps to ensure that it is processed in a traceable, legally compliant, and timely manner.

Step 1: Create Privacy Request

1. Creation from dashboard

The Editor navigates via the sidebar to **Dashboards >> Privacy Request >> "New Privacy Request."**

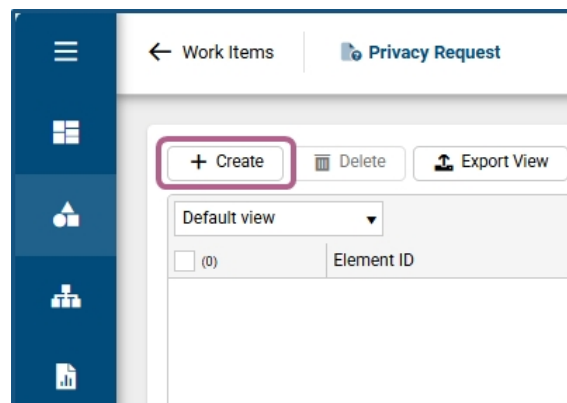


A new window will then open automatically.

2. Creation via tile

The Editor navigates via the sidebar to **Work Items >> Privacy Request >> "Create"**.

A new window will then open automatically.



Step 2: Enter details

Privacy Request Details

Status Registration

* Name 1 Request for information on marketing data (neutral)

Review of the request

Incoming request

2

Type of request

Right of access Art 15 GDPR

Select...

3

Date of request

26/02/2026

4

Description of request

A data subject requests information about which personal data is processed about them in the context of marketing and communication measures.

In addition, information is requested about the purposes of the processing, the categories of data processed, and the storage period.

(276/5000)

5

Relevant processing activities

Name	Status	D...
Kunden- und Interessentenkommunikation im Marketing	Active	

You have unsaved changes.

6

Save

Close

1 Name: The first step is to enter a short but meaningful name for the *Privacy Request*. The *Privacy Request* is unique under the "Name" in combination with the "Element ID."

2 Type of request: The Editor is presented with a list of Data Subject Rights under the GDPR.

For example, if the type "Rectification pursuant to Art. 16 GDPR" is selected, the Data Subject wishes to have incorrect data corrected.

3 Date of Request: After classification, a date must be set for when the request was received. This date is important for calculating the deadline in accordance with the GDPR.

4 Description of the request: This text field can be used by the Editor to provide a detailed description of the content or a justification for the processing steps.

Example: "Name change after marriage."

5 Relevant Processing Activities: The Editor should use the icon  to perform the Assignment for a relevant *Processing Activity*.

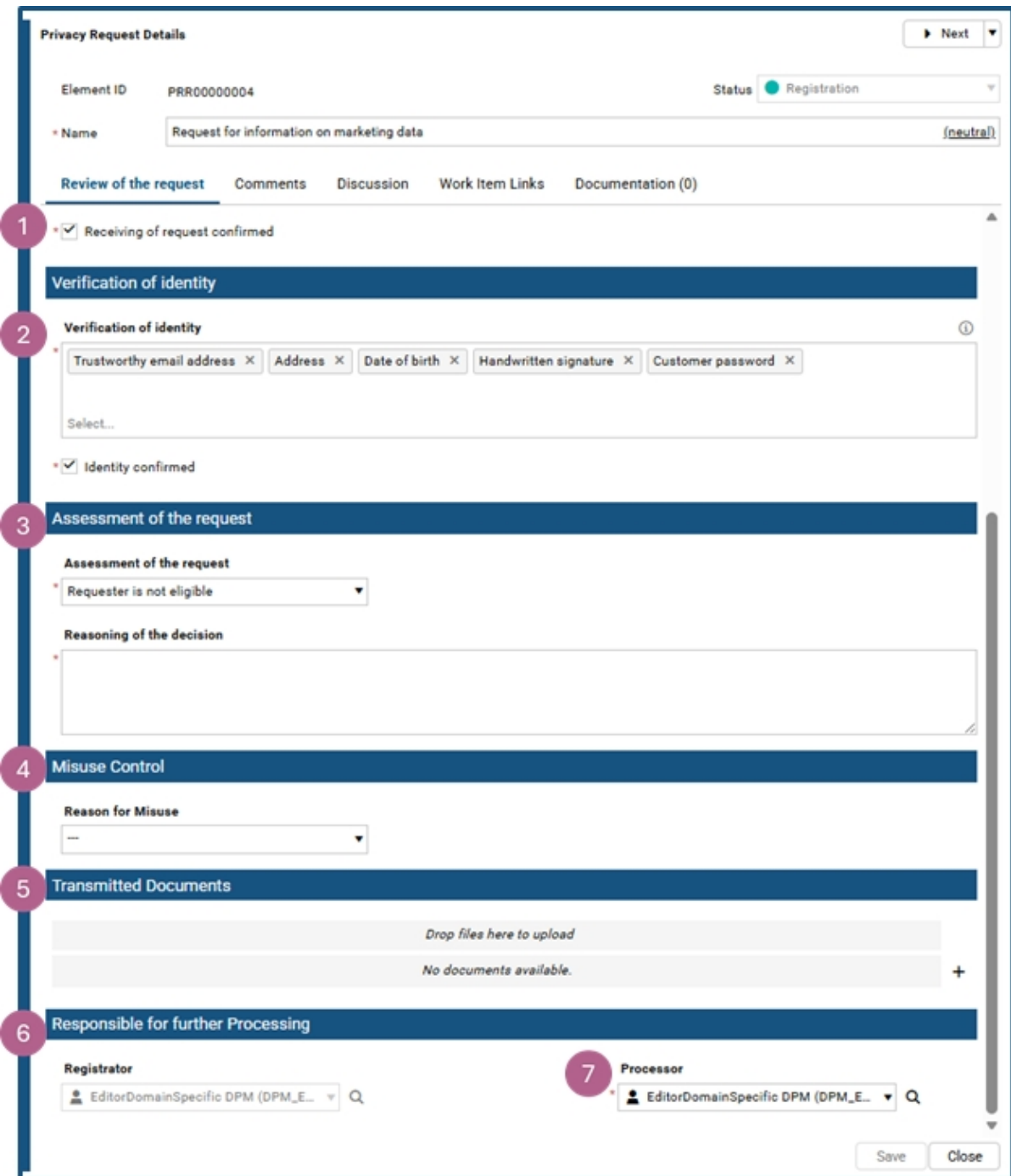
When selecting *Processing Activities*, only those Work Items that are in "Active" Status are suggested to the Editor.

GBTEC Austria GmbH

163/226

- 6 **Save:** Once the information has been entered, the Editor can save it for the first time.

Step 3: Add further details



The screenshot shows the 'Privacy Request Details' form. At the top, there's a 'Next' button. Below it, the 'Element ID' is 'PRR00000004' and the 'Status' is 'Registration'. The 'Name' field contains 'Request for information on marketing data' with a '(neutral)' tag. Below this are tabs for 'Review of the request', 'Comments', 'Discussion', 'Work Item Links', and 'Documentation (0)'. The form is divided into several sections, each with a numbered annotation:

- 1** **Receiving of request confirmed:** A checkbox that is checked.
- 2** **Verification of identity:** A section with a title bar. Below it, there's a 'Verification of identity' section with a list of options: 'Trustworthy email address', 'Address', 'Date of birth', 'Handwritten signature', and 'Customer password'. A 'Select...' dropdown is below these. Below the dropdown, there's a checked checkbox for 'Identity confirmed'.
- 3** **Assessment of the request:** A section with a title bar. Below it, there's an 'Assessment of the request' dropdown menu showing 'Requester is not eligible'. Below that is a 'Reasoning of the decision' text area.
- 4** **Misuse Control:** A section with a title bar. Below it, there's a 'Reason for Misuse' dropdown menu.
- 5** **Transmitted Documents:** A section with a title bar. Below it, there's a 'Drop files here to upload' area and a 'No documents available.' message with a '+' button.
- 6** **Responsible for further Processing:** A section with a title bar. Below it, there are two dropdown menus: 'Registrator' and 'Processor'. Both are set to 'EditorDomainSpecific DPM (DPM_E...'. There are search icons next to each dropdown.
- 7** **Processor:** This annotation points to the 'Processor' dropdown menu.

At the bottom right, there are 'Save' and 'Close' buttons.

- 1 **Request receipt:** After the first save operation, the "Request receipt confirmed" checkbox must be clicked to confirm that an official request has been received before the *Privacy Request* is investigated.
- 2 **Identity Review:** The Editor must document the medium used to review the identity. To do this, they can select the appropriate option from a list.

Confirmation is then required that the verification was successful and that the request may be processed further. This is confirmed by clicking the checkbox.

- 3 **Review of entitlement:** As each request requires evaluation, it must be reviewed whether this request will be followed up.

Regardless of the outcome of the decision, it must be described manually in a separate text field.

- 4 **Reason for Misuse:** The Editor can document if a request is classified as abusive.

According to Art. 12 (5) GDPR, the GDPR may accept requests or charge fees only if they are: 1) clearly well-founded, 2) reasonable (occasional, non-repetitive, non-systematic), or 3) lawful.

If misuse is identified, an appropriate measure can be selected from a list and specified in the Measure Rationale text field.

- 5 **Transmitted documents:** At this point, the Editor can store all documents that have been transmitted in connection with this request.

Example: Copy of ID for identity verification or response letter/reason for approval

If it is a file, it can be dragged from the desktop to the "Drag file here to upload" area, for example. The file is then linked in the attribute field.

- 6 **Responsible:** The Creator of the Work Item is automatically entered in the user attribute "Creator" and remains unchanged. Furthermore, an "Editor" must be nominated to follow up on the *Privacy Request*.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

Using a stored filter, Editors DS or Approvers DS can be selected to process the Work Item.

- 7 **Status transition:** Once the information has been entered, the Editor can save it and perform a status transition.

The stored Editor is informed of the status transition by means of a notification.

For more information on the next step, see [Editor DS - Review & edit Privacy Requests](#).

2.13.8 Review & edit Privacy Requests

A *Privacy Request* can be identified & created by Users Editor DS.

If the Creator and the Editor are different users, the Editor will be notified separately about the new *Privacy Request*. The following steps 1 & 2 refer to the steps after creation by another User.

Optional step 1: Navigate to specific Privacy Request after external creation

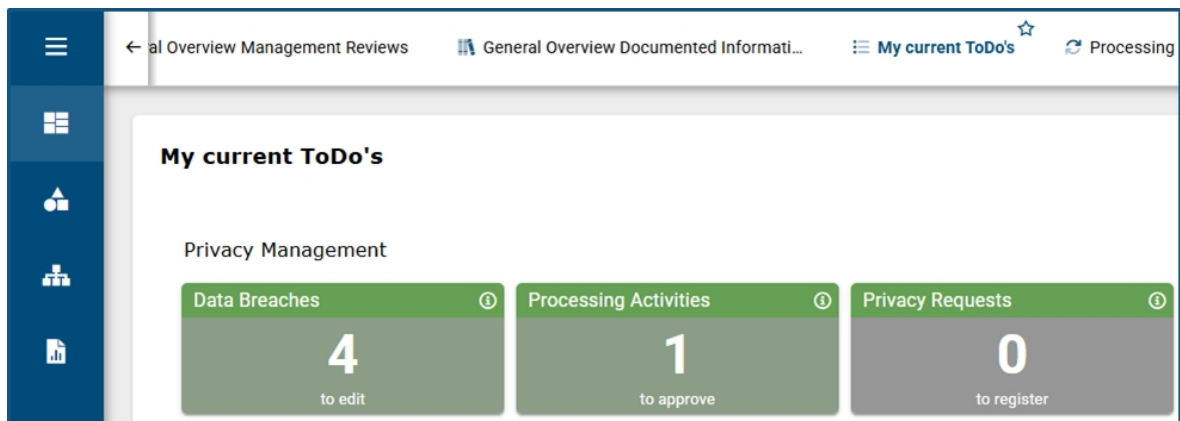
The Editor has two options for opening a *Privacy Request* to be edited.

1. Open via notification

The Editor receives an E-Mail as soon as the Creator has completed all entries in the "Registration" status. The link to the specific *Privacy Request* is included in the notification.

2. Open via the "My ToDo's" dashboard

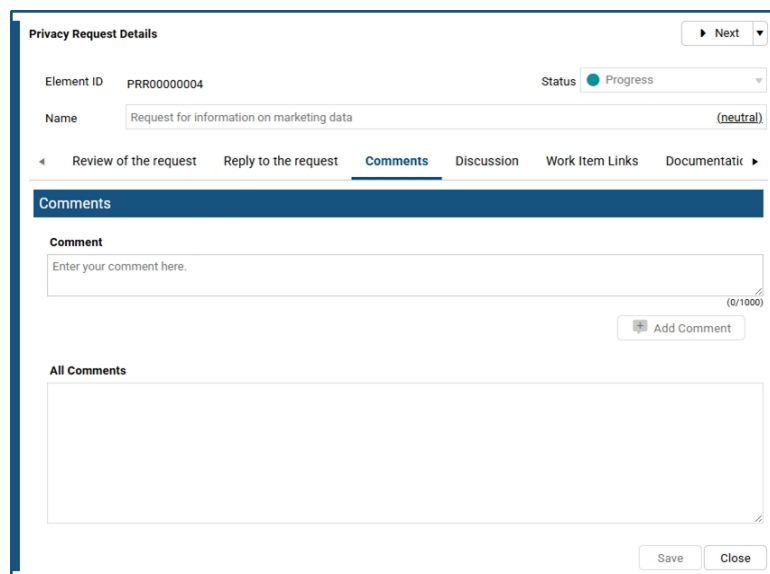
At the top of the "My ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on a tile opens a list of all Work Items in that Status for which the Editor DS can provide a response.



Optional step 2: Reviewing the creator's entries

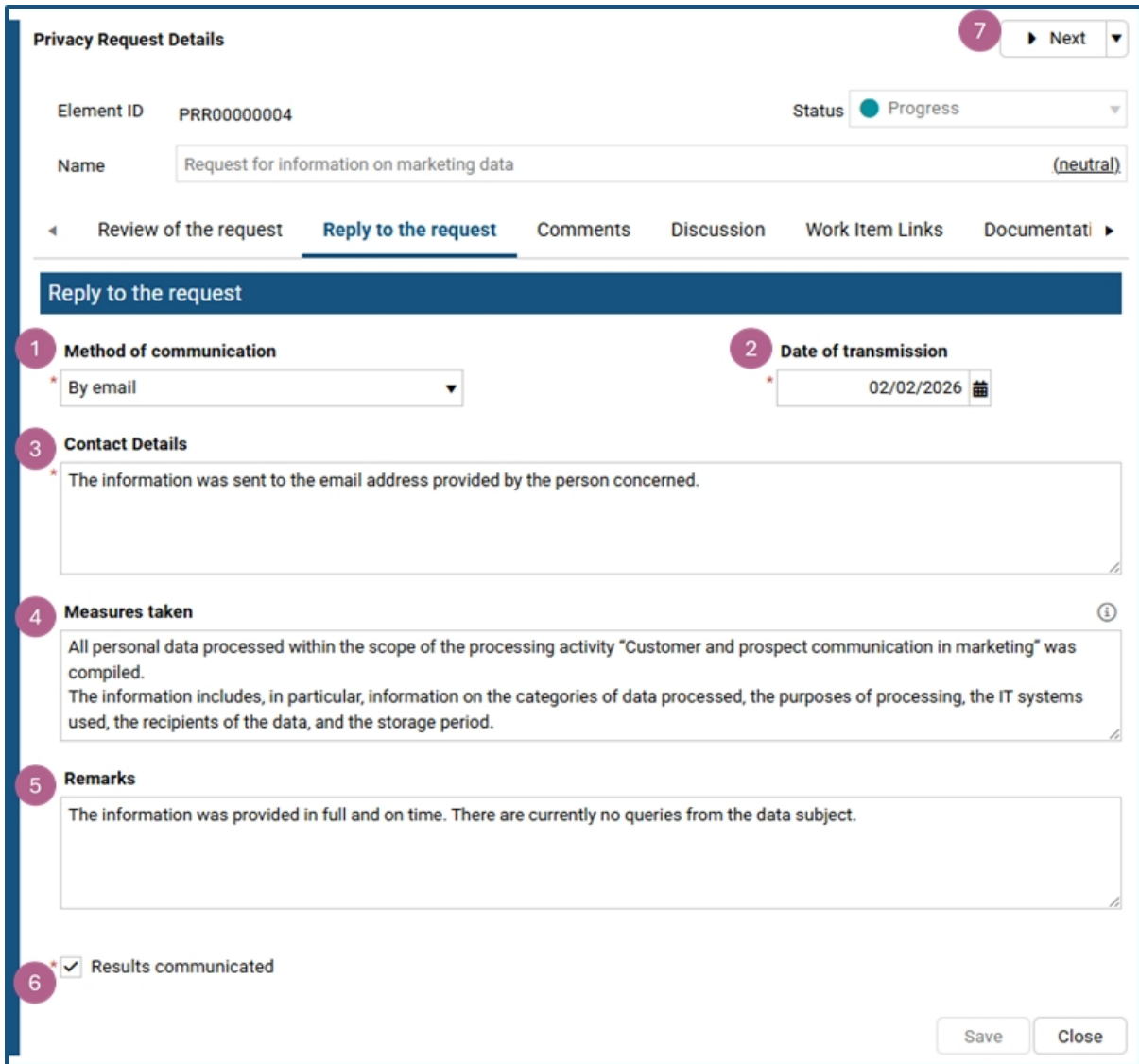
If the Creator and the Editor are different users, it is recommended that you first go to the "Review of the Request" tab in the *Privacy Request* Work Item to view the Creator's detailed entries.

If the Creator's entries require clarification or further details, the Editor can leave a contribution in the "Discussion" tab. The Creator will then be notified of the contribution via a notification.



Step 3: Complete the Privacy Request

Should the entries be correct, the Editor can switch to the "Respond to Request" tab and begin processing.



- 1 **Method of communication:** The Editor specifies the communication channel through which the response was sent to the Data Subject.
- 2 **Date of Transmission:** The Editor must then specify when the transmission was made by post or E-Mail.
- 3 **Contact Details:** The Recipient's Contact Details must be provided.

Either an E-Mail Address or a postal address should be provided.
- 4 **Measures taken:** A detailed description of the specific steps taken for the implementation of the request must be provided.
- 5 **Remarks:** Here, the Editor can leave further notes relevant to the request.

Example: "Additional telephone inquiry made" or "Special feature: Translator involved."

6 Results communicated: The Editor must provide separate confirmation that the response has actually been sent, regardless of the channel. They do this by clicking the checkbox.

7 Status change: Once all information has been entered, the status is changed to "Completed" or, if applicable, "Rejected" in the upper right window.

The Work Item can then be closed.

2.13.9 Define & create Management Review

In BIC GRC, an Editor can define *Management Reviews* in different contexts.

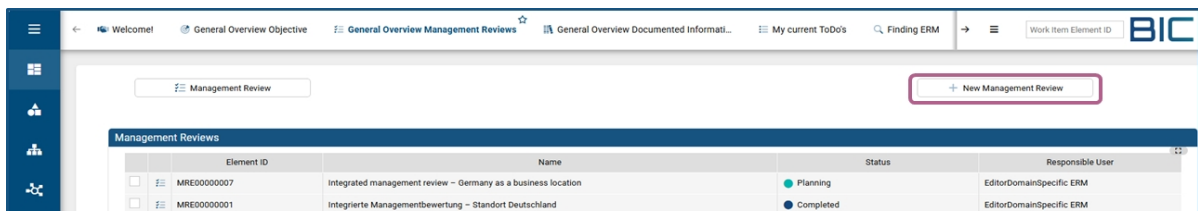
A *Management Review* should be executed at least once a year to comply with most standards. Additional reviews are recommended for special occasions.

Step 1: Create Management Review

The *Editor DS* can create *Management Reviews* in several places in BIC GRC.

1. Creation via the "Management Review Overview" dashboard

The Editor navigates to **Dashboards >> Management Review Overview >> "New Management Review."**

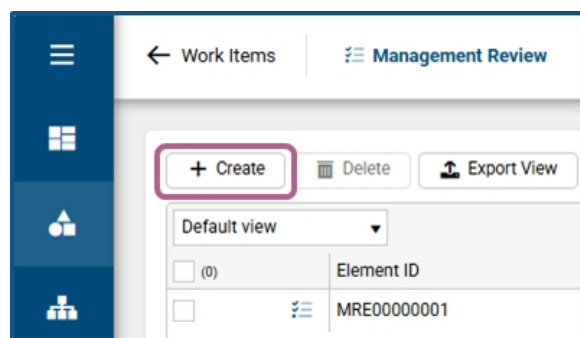


A new window then opens automatically.

2. Creation via Work Item List

The Editor navigates via the sidebar to **Work Items >> Management Review >> "Create."**

A new window then opens automatically.



Step 2: Define details

Management Review Details

Status: Planning

* Name **1** Integrated management review – Germany as a business location (EN)

Planning

2 Scope

Name	Asset Type	End-user ...
Location Germany	Business Structure	

3 Purpose and Goals

The aim of this management review is to comprehensively assess the effectiveness and efficiency of the management systems and control mechanisms implemented at the German site.

4 GRC Perspectives

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

Select...

Discussion Topics

5 Information Security Management

Name	En...
What trends, deviations, or insights have been identified through monitoring, measurement, audits, or performance reviews?	
Do current procedures or controls need to be adapted due to internal findings or new external requirements?	

5 Business Continuity Management

Name	En...
What are the potential consequences of planned organizational or process changes?	

6 You have unsaved changes. Save Save and Close Close

1 Name: A short but meaningful name for the *Management Review* is added here.

2 Scope: The *Management Review* must be assigned to an Asset.

The Scope only filters for Assets with the Asset Type "Business Structure".

3 Purpose and Goals: The *Management Review* should be documented and described in as much detail as possible so that other perspectives can also understand its context.

4 GRC Perspective: The Editor can select one or more GRC perspectives.

The number of GRC Perspectives displayed depends on the modules that have been activated.

- 5 **Management Review questions:** After the *Editor DS* has selected GRC Perspectives, links are displayed below depending on the selected perspective. These links lead to a GRC framework "Management Review questions."

The *Editor DS* sees only those "Management Review Questions" that have the appropriate tag in the GRC Framework for the link heading.

- 6 **Save:** After entering the necessary information, the *Management Review* can be saved.

After saving the first time, the user creating the *Management Review* is automatically entered as the "Editor."

Step 3: Enter Additional Information

Management Review Details

Next

Element ID

MRE00000007

Status

Planning

Name

Integrated management review – Germany as a business location

(EN)

Planning

Scheduled

Execution

Review

Management Approval

Completed

Planning

Comments

Discussion

Work Item Links

Documentation (0)

Planning

1 Processor

EditorDomainSpecific ERM (ERM_E...

Q

1 Approving Executive

Executive ERM (ERM_Executive)

Q

2 Date Management Review

10/02/2026

Scope

Name	Asset Type	End-user ...	
Location Germany	Business Structure		

Purpose and Goals

The aim of this management review is to comprehensively assess the effectiveness and efficiency of the management systems and control mechanisms implemented at the German site.

GRC Perspectives

Information Security Management

Business Continuity Management

Privacy Management

Enterprise Risk Management

Internal Control

Corporate Sustainability

Select...

3 Participants

AssetOwner GEN (AssetOwner)

Executive AUM (AUM_Executive)

Executive BCM (BCM_Executive)

Executive CSM (CSM_Executive)

Executive ERM (ERM_Executive)

Executive ICS (ICS_Executive)

Executive ISM (ISM_Executive)

Enter search text

4 Other Participants

Save

Save and Close

Close

1

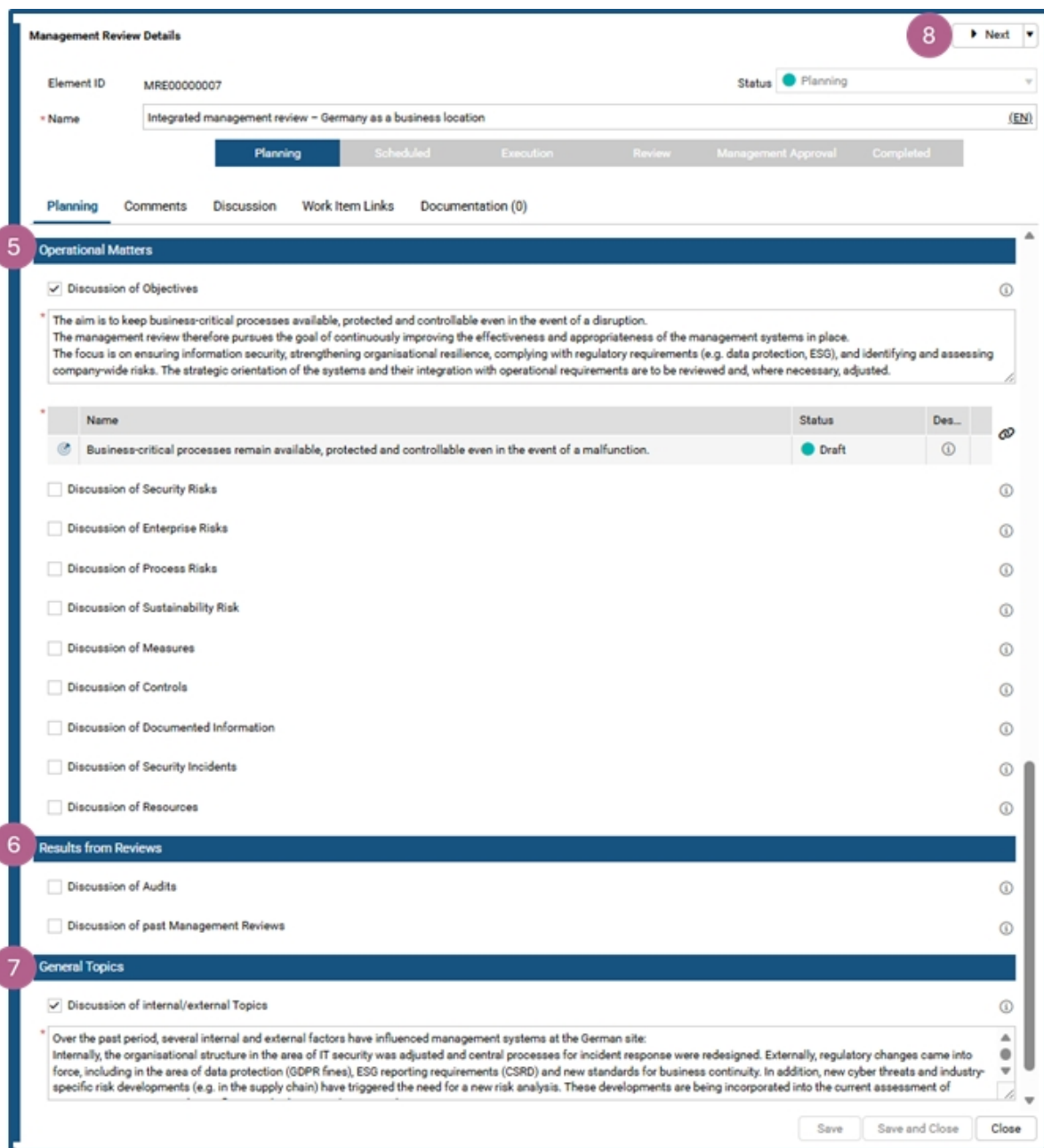
2 **Data Management Review:** This date specifies when the Management Review is to be carried out.

One week before the date is reached, the Editor automatically receives a notification reminding them of the Execution.

- 3 **Participants:** Using the  icon, all users who are active in BIC GRC can be selected to participate in the Management Reviews.
- 4 **Other participants:** The editor can also document participants in writing if they are not Users in BIC GRC.

These persons selected can be manually notified and granted access to the Work Item as needed.

Step 4: Document the Management Review



Management Review Details

Element ID: MRE0000007 Status: Planning

Name: Integrated management review - Germany as a business location (EN)

Planning Scheduled Execution Review Management Approval Completed

Planning Comments Discussion Work Item Links Documentation (0)

5 Operational Matters

☒ Discussion of Objectives

The aim is to keep business-critical processes available, protected and controllable even in the event of a disruption. The management review therefore pursues the goal of continuously improving the effectiveness and appropriateness of the management systems in place. The focus is on ensuring information security, strengthening organisational resilience, complying with regulatory requirements (e.g. data protection, ESG), and identifying and assessing company-wide risks. The strategic orientation of the systems and their integration with operational requirements are to be reviewed and, where necessary, adjusted.

Name	Status	Des...
Business-critical processes remain available, protected and controllable even in the event of a malfunction.	Draft	

☐ Discussion of Security Risks

☐ Discussion of Enterprise Risks

☐ Discussion of Process Risks

☐ Discussion of Sustainability Risk

☐ Discussion of Measures

☐ Discussion of Controls

☐ Discussion of Documented Information

☐ Discussion of Security Incidents

☐ Discussion of Resources

6 Results from Reviews

☐ Discussion of Audits

☐ Discussion of past Management Reviews

7 General Topics

☒ Discussion of internal/external Topics

Over the past period, several internal and external factors have influenced management systems at the German site: Internally, the organisational structure in the area of IT security was adjusted and central processes for incident response were redesigned. Externally, regulatory changes came into force, including in the area of data protection (GDPR fines), ESG reporting requirements (CSRD) and new standards for business continuity. In addition, new cyber threats and industry-specific risk developments (e.g. in the supply chain) have triggered the need for a new risk analysis. These developments are being incorporated into the current assessment of

Save Save and Close Close

- 5 **Operational matters:** If the editor intends to address "operational matters" in the Management Review, they can specify this using various checkboxes.

If the editor clicks a checkbox, two additional attributes are always displayed below the checkbox. One of these is used for Description, the other is used to create a link.

- 6 **Results from reviews:** This section focuses on the results of Audits and previous Management Reviews.
- 7 **General Topics:** This text field allows further discussion if the topic is not applicable elsewhere.
- 8 **Status change:** To change the status, the *Editor DS* selects at least one checkbox and provides a description and link. The Editor can then change the status to "Scheduled."

The entered "Approver Manager" is informed of the status change by means of a notification.

After entering all the necessary information, the Work Item can be saved and a status change can be executed before the window is closed manually.

2.13.10 Perform & review Management Review

The *Editor DS* will be automatically reminded by BIC GRC seven days before the "Management Review Date" is reached.

Step 1: Navigate to Management Review

The *Editor DS* automatically receives an E-Mail from BIC GRC as soon as a *Management Review* is ready for execution. The link to the specific *Management Review* is included in the notification.

Step 2: Perform Management Review

The *Editor DS* continues to have all editing rights in the *Management Review* they created, enabling them to add to the information already entered if necessary.

Management Review Details
Review

Element ID
MRE00000007
Status
Execution

Name
Integrated management review – Germany as a business location
(EN)

Planning
Scheduled
Execution
Review
Management Approval
Completed

Planning
Results
Comments
Discussion
Work Item Links
Documentation (0)

Results

Decisions

- Introduction of uniform monitoring for business-critical processes, taking into account security, BCM and data protection aspects.
- Decision to integrate data protection-related checks into internal control mechanisms (ICS).
- Updating of corporate sustainability targets to align them more closely with ESG reporting requirements in accordance with CSRD.
- Launch of a cross-divisional project to revise the business continuity plan with a focus on supply chain risks.

Finding

Name	Status	De...
Documentation gap in the 2025 emergency test protocol	Registration	

Results from Objective Discussions

- The strategic objectives were generally deemed to remain valid and effective.
- However, there is room for improvement in the operationalisation of objectives in the areas of sustainability and risk transparency.
- In future, objectives will be reviewed in closer coordination with audit results and lessons learned.

Results from internal/external Topic Discussions

A proposal to introduce continuous external requirements monitoring was well received and will be pursued further.

Save
Save and Close
Close

Before execution, it is recommended that to review all entries from the "Planning" tab. Based on the entries, results and decisions can then be documented together with the "Approving Executive." If *Findings* need to be discussed, they can be created using the icon . For more information on creating *Findings*, see [Identifying & creating Findings](#).

Step 3: Perform status transition

After entering all results and decisions, the *Editor DS* can switch to the next status, "Review." In this status, the *Editor DS* remains responsible and can, if necessary, review and finalize the discussed topics one last time independently.

In the "Review" status, the *Editor DS* can edit all attributes in the "Results" tab, while the attributes in the "Planning" tab and the link to the *Findings* remain locked.

Once all results and decisions have been finalized, the *Editor DS* can make a final status transition to "Management Approval." The user in the "Approver Manager" attribute is

notified of the status transition via notification.

2.13.11 Identify & create Finding

If during the execution of a *Management Review* the *Editor DS* identifies potential for improvement that has arisen in the context of the Management Review, the *DS Editor* must create a *Finding*.

Step 1: Create Finding from Management Review

A *Finding* can arise from a Management Review.

It is created using the  icon after a written statement has been made under "Decisions made."

The *Finding* is then automatically included in the *Management Review*.

Step 2: Document the Finding

10

Registration

1

Name

* Documentation gap in the 2025 emergency test protocol (EN)

2

GRC Perspective

P Privacy Management

3

Editor

EditorMeasure

4

Report Date

* 31/07/2025

5

to process by

* 11/09/2025

6

Type of Finding

Observation Recommendation Improvement Request Insignificant Nonconformity Significant Nonconformity

7

Finding for these Assets:

Name	Asset Type	End-u...
Group	Business Structure	

8

Description of Finding

* During the review of the emergency tests carried out, it was found that the complete test protocol for 2025 had not yet been stored in the central document management system. The implementation itself is documented, but the filing process was incomplete.

9

Priority of Finding

* Very Low Low Medium High Critical

Save

Save and Close

Close

1 **Name:** A short but meaningful name for the *Finding* is added here.

2 **GRC Perspective:** The Perspective is selected automatically from the perspectives allocated at the *Management Review*

3 **Editor:** The attribute contains the name of the Editor who is responsible for handling the *Finding* from the *Management Review*.

The Creator is also displayed in this section so that it is clear at a glance who created the *Finding*.

- 4 **Report Date:** Here the date when the *Finding* was officially discovered should be added. The date can differ from the current date.
- 5 **to process by:** The date refers to the date by which the *Finding* should be resolved. It is intended as a guide for downstream users in the workflow to indicate when the *Finding* should ideally be resolved.
- 6 **Type of Finding:** The Editor of the *Management Review* can classify how serious the *Finding* is in terms of the appropriateness or effectiveness of the *Management Review* in the context of five levels.
- 7 **Finding for these assets:** The assets are automatically taken from the Work Item from which it was created.
- 8 **Description of Finding:** The "Description of the finding" should contain as much information and input as possible, for example, how the *Finding* was discovered. Furthermore, conclusions about cause and effect may be drawn.
- 9 **Priority of Finding:** A priority can be assigned to the *Finding*, which can later be used for evaluations on dashboards, for example.
- 10 **Status change:** The Editor can then switch to the "Treatment" status. For more information on the status change, see [View & process Finding](#).

The Editor can then return to Management Review and continue with the documentation of the Management Review. [Editor DS - Perform & review Management Review](#).

2.14 Approver "Domain Specific"

The Approver "Domain Specific" has the most permissions and views for their domain. They are responsible for the appropriate management of BIC GRC and thus not only for the assets, GRC Framework, and Work Item Management, but also for management specifications and data archiving in BIC GRC.

The Approver "Domain Specific" will be abbreviated as *Approver DS* in the following chapters.

In the Data Protection module, the *Approver DS* also serves as the Data Protection Officer, so this user profile is assigned to a single person in the Company.

The Approver DS has the following preparatory tasks:

- Define & create an Objective (forwarding to [Editor Risk - Define & create Objective](#))
- Define & create a Milestone (forwarding to [Editor Risk - Define & create Milestone](#))

An Approver DS has the following ongoing tasks in BIC GRC:

- [Review & approve Processing Activity](#)
- [Review & approve Data Processing Agreement](#)
- [Review & edit Data Breach](#)

- [Open & generate report\(s\)](#)

The *Approver DS* can also create other Work Items in BIC GRC. While this is beyond their primary responsibility, we will refer to other user profiles at this point:

- [Identify & create Processing Activity](#)
- [Define & Create Privacy Request](#)
 - [Review & edit Privacy Requests](#)
- [Define & Create Management Review](#)
- [Identify & create Measures](#)
- [Derive & create Controls](#)

2.14.1 Review & approve Processing Activity

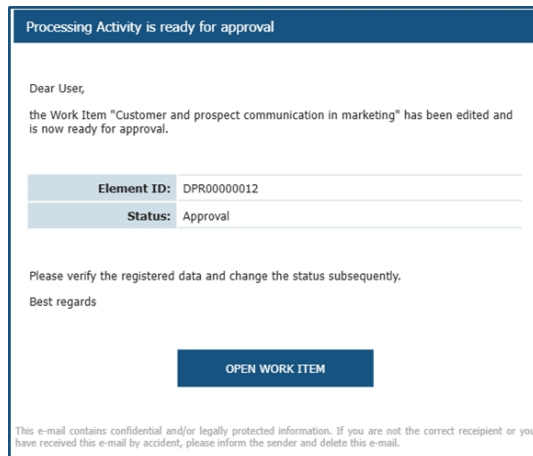
The Approver DS is notified via a medium after a *Processing Activity* has been created and planned.

Step 1: Navigate to Processing Activity

The Approver DS has two options for opening a *Processing Activity* to be approved.

1. Open via notification

The Approver DS automatically receives an E-Mail from BIC GRC as soon as a *Processing Activity* has been created and edited and a status transition has taken place. The link to the specific *Processing Activity* is included in the notification.



Processing Activity is ready for approval

Dear User,

the Work Item "Customer and prospect communication in marketing" has been edited and is now ready for approval.

Element ID:	DPR00000012
Status:	Approval

Please verify the registered data and change the status subsequently.

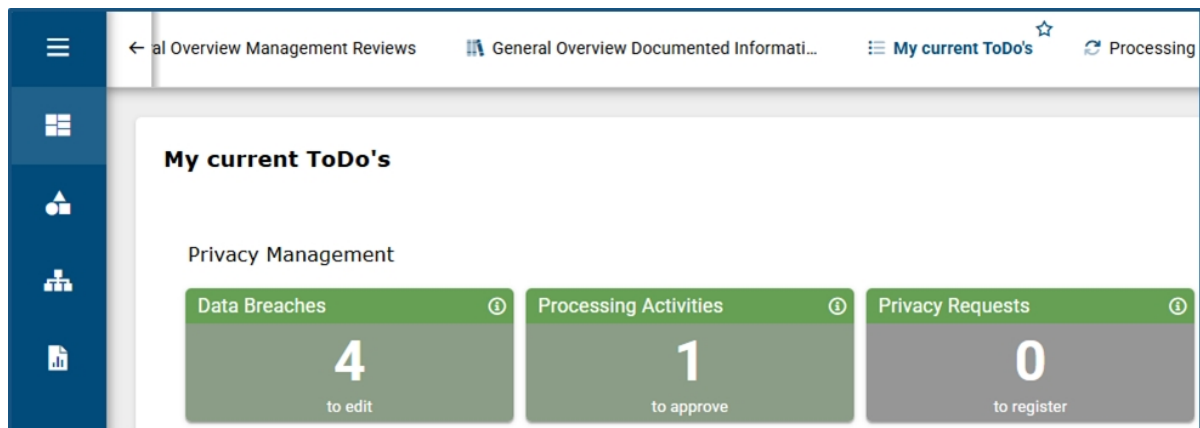
Best regards

[OPEN WORK ITEM](#)

This e-mail contains confidential and/or legally protected information. If you are not the correct recipient or you have received this e-mail by accident, please inform the sender and delete this e-mail.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still require the Approver DS "Approval".



Step 2: Review Processing Activity

The Approver DS has full read access to the evaluated *Processing Activity* so that they can decide, based on the information entered, whether the *Processing Activity* has been correctly classified and the correct conclusions have been drawn.

If further refinement is required, the Approver DS can add a Comment in the "Comment" tab and change the Status to "Draft."

Step 3: Perform status transition execution

If the entries made by the upstream users are correct, the Approver DS can change the status to "Active." The responsible Editor is notified of the status change via notification.

Step 4: Generate report

Once the *Processing Activity* has been changed to "Active" Status, the Editor and Approver DS can generate a report.

The report is a Summary of the entire *Processing Activity*.

The report is generated in the upper right-hand corner of the Work Item window. The output file is a PDF.

2.14.2 Review & approve Data Processing Agreement

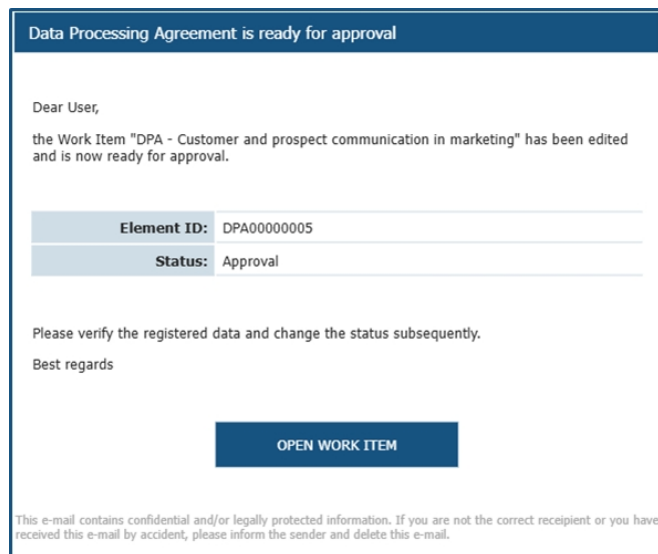
The Approver DS is notified via a medium after the creation and filing of a *Data Processing Agreement*.

Step 1: Navigate to the Data Processing Agreement

The Approver DS has two options for opening a *Data Processing Agreement* to be approved.

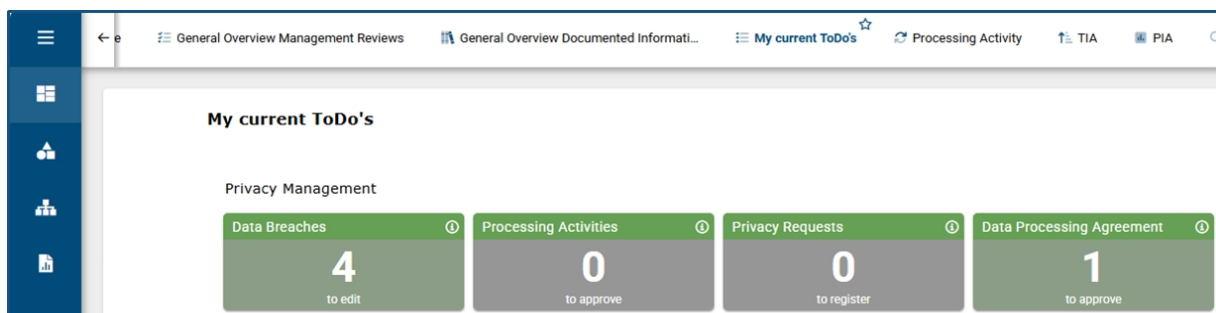
1. Open via notification

The Approver automatically receives an E-Mail from BIC GRC as soon as a *Data Processing Agreement* has been created and edited and a status change has occurred. The link to the specific *Data Processing Agreement* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

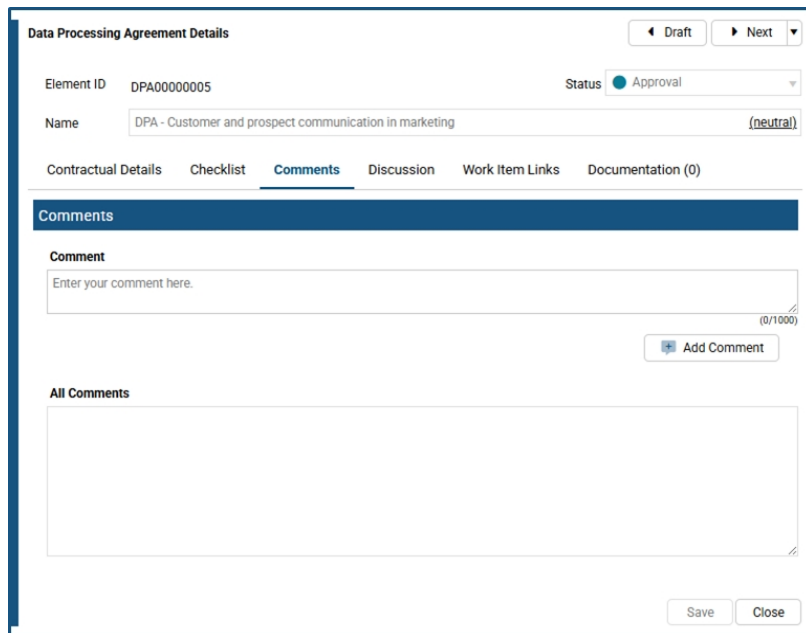
In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still require Approval from the Approver DS.



Step 2: Review the Data Processing Agreement

The Approver DS has all read rights in the created *Data Processing Agreement* to decide, based on the information entered, whether the *Data Processing Agreement* has been correctly classified and the correct conclusions have been drawn.

If further evaluation or review of the *Data Processing Agreement* is required, the Data Protection Officer can leave a comment in the "Comment" tab and change the status to "Draft."



Step 3: Perform status transition execution

If the entries made by the upstream users are correct, the Approver DS can change the status to "Active." The responsible Editor is notified of the status change via notification.

Step 4: Further procedure

The Approver DS is informed about the Status of the Work Item "Data Processing Agreement" by two schedulers.

On the one hand, the Approver DS is notified by means of an automatic notification that the "Valid to" date will be reached in three weeks.

When the "Valid to" date is reached, the Work Item is reset to the "Approval" status. If the Work Item *Data Processing Agreement* remains current, it should be switched to the "Draft" status so that a new "Valid to" date can be entered. If the Work Item is now obsolete, it can be switched to the "Obsolete" status.

2.14.3 Viewing & editing Data Breaches

If a *Data Breach* has been reported in the Company, the Approver DS can document and assess or perform an Evaluation on it.

Step 1: Navigate to specific Data Breach

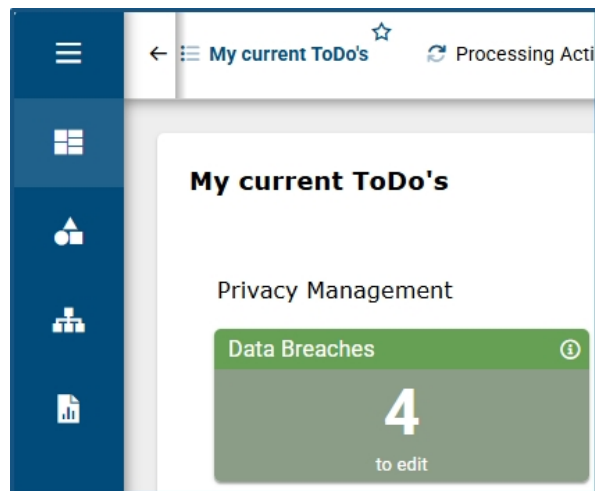
The Editor DS has two options for opening a new *Data Breach*.

1. Open via notification

The Approver DS receives an E-Mail as soon as the Creator has completed the report and changed the status to "Reported." The link to the specific *Data Breach* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still need to be edited by the Approver DS.



Step 2: Review Data Breach

First, the Approver DS should review the entries for the Report before changing the status from "Reported" to "Evaluation."

The Creator of the report is informed of the status change via notification.

Step 3: Provide further details

As a first step, the Approver DS should switch to the "Data Breach" tab.

Data Breach Details

Next▼Report

Element IDDBR00000012StatusProgress▼

* NameUnauthorized access to customer data in the CRM system(neutral)

RegistrationReportedProgressCompleted

ReportData BreachEvaluationReactionCommentsDiscussionWork Item LinksDocumentatio▶

Data breach

1 Affected Processing Activities

Name	Status	D...
Kunden- und Interessentenkommunikation im Marketing	Active	

2 Data Protection Officer

ApproverDomainSpecific DPM (DP... Q

3 Involved IT Systems

Name	Asset Type	End-use...
CRM Tool	Supporting Asset	

4 Type of Violation

Misuse of access rights (e.g. unauthorized retrieval by own employees) X

Select...

5 Consequences of the Data Breach

Breach of confidentiality (e.g. data were stolen or copied) X

Select...

Breach of Confidentiality

Use for Improper Purposes X

Select...

⚠ You have unsaved changes.

SaveClose

Data Breach Details

Next

Report

Element ID

DBR00000012

Status

Progress

Name

Unauthorized access to customer data in the CRM system

(neutral)

Registration

Reported

Progress

Completed

Report

Data Breach

Evaluation

Reaction

Comments

Discussion

Work Item Links

Documentati

6

Minimum Number of affected Records

50

6

Maximum Number of affected Records

200

7

Minimum Number of affected People

50

7

Maximum Number of affected People

200

8

Causes

Die Datenpanne wurde durch eine fehlerhafte Vergabe von Zugriffsberechtigungen im CRM-System verursacht. Infolge einer unzureichenden Rollenabgrenzung konnte ein Mitarbeitender auf Kundendaten zugreifen, die für die Erfüllung der eigenen Aufgaben nicht erforderlich waren.

(273/5000)

9

Likely Consequences

Für die betroffenen Personen besteht das Risiko einer ungewollten Kenntnisnahme ihrer Kontakt- und Kommunikationsdaten durch unbefugte Dritte. Die möglichen Auswirkungen werden als begrenzt eingeschätzt, da überwiegend allgemeine Kunden- und Kontaktdaten betroffen sind und keine besonderen Kategorien personenbezogener Daten verarbeitet wurden.

(346/5000)

You have unsaved changes.

Save

Close

- Affected Processing Activities:** The Approver should use the icon  to perform the assignment of the report to an affected *Processing Activity*.

When selecting *Processing Activities*, only those Work Items that have been assigned to the same "Legal Entity" and are also in "Active" Status are suggested to the Approver.

- Data Protection Officer:** As soon as a Work Item *Processing Activity* has been linked, new attributes appear. One of these contains the Data Protection Officer, which is set automatically and remains fixed.

Since there is only one Approver DS in the Company (because there is only one Data Protection Officer), this user is automatically set and remains consistent.

- Involved IT systems:** The Approver DS can then specify "Involved IT Systems." Only Assets that are "Supporting Assets" and have the appropriate tag "Hardware," "Software," or "Network" set can be linked.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission](#)

Request.

- 4 **Type of violation:** The Approver can identify the "Type of Violation" from the Name, Description, or Additional Information provided by the Creator. One or more types can be specified.
- 5 **Consequences of the breach:** Next, the consequences of the *Data Breach* are assessed. Here, too, the Approver can select from a list.
Unlike with the "Type of Breach," when selecting the "Consequences of the Breach," a separate sublist is displayed for each selection. This must also be filled in with an appropriate value.
- 6 **Number of affected data records:** A minimum and maximum must be specified with an estimate or survey of how many individual data objects (e.g., data records, forms, system entries) are affected.
- 7 **Number of Data Subjects affected:** In addition to the data records, an estimate of the minimum and maximum number of natural Data Subjects affected by the *Data Breach* must also be provided.

These figures are used for the assessment of the obligation to report to the supervisory authority and notify those affected (Articles 33 & 34 GDPR).

- 8 **Causes:** The Approver can provide a description of the technical, human, or organizational cause of the *Data Breach*.
- 9 **Likely consequences:** The Approver DS must provide an estimate of the potential impact on the Data Subjects affected.

This assessment is crucial in determining whether data subjects must also be notified in accordance with Art. 34 GDPR.

- 10 **Special information:** According to Art. 33 (1) sentence 2 GDPR, a report must be made to the supervisory authority immediately, and within 72 hours after becoming aware of the breach. If this has occurred, the Approver must therefore provide their own justification for this circumstance.
- 11 **Additional Points of Contact:** If necessary, the Approver can specify additional internal or external Points of Contact who are involved in the Evaluation, communication, or remediation of the Data Breach. Separate text fields are available for providing this information.
- 12 **Save:** Once the information has been entered, the Approver DS should save it.

Data Breach Details

Next
Report

Element ID
DBR00000012

Status
Progress

Name
Unauthorized access to customer data in the CRM system
(neutral)

Registration
Reported
Progress
Completed

Report
Data Breach
Evaluation
Reaction
Comments
Discussion
Work Item Links
Documentati

10
Special details (as required)

Reasoning in case the Data Breach was reported more than 72 hours after emersion

(0/5000)

11
Additional Contact Point (as required)

Denomination

Postal Address

Function

Email Address

You have unsaved changes.
12
Save
Close

Step 4: Perform evaluation

As a next step, the Approver DS should switch to the "Evaluation" tab.

Data Breach Details

Next

Report

Element ID

DBR00000012

Status

Progress

* Name

Unauthorized access to customer data in the CRM system

(neutral)

Registration

Reported

Progress

Completed

Report

Data Breach

Evaluation

Reaction

Comments

Discussion

Work Item Links

Documentat

Evaluation of the risk for Data Subjects

1 Overall Evaluation

Severity of the disadvantage

Large

Substantial

Manageable

Minor

Minor

Manageable

Substantial

Large

Probability of occurrence of the disadvantage

2 Report to Authority required!

3 Save

Close

- 1 Overall evaluation:** The Approver can use the risk heat map to make a visual and systematic assessment of whether and how serious the potential damage to the Data Subjects is, as required by Articles 33 and 34 of the GDPR.
- 2 Recommendation:** If the information in the risk heat map is in the yellow or red zone, BIC GRC will display recommendations to the Approver as to whether a Report is necessary. If a Report is necessary, a "Report" will be displayed in the upper right window, which the Editor can then download.
- 3 Save:** Once the information has been entered, the Approver should save it.

Step 5: Document the response

As the next step, the Approver DS should switch to the "Response" tab.

- 6 **Status change:** Once all information has been entered, the status is changed to "Completed" in the upper right window.

After the save process, the Creator is notified by means of a notification.

2.15 Document Owner

The Document Owner is a special user profile. Users of this profile deal with the storage and maintenance of one or more *Documented Information* pieces in BIC GRC. Their main task is therefore primarily to create and regularly review the document to ensure that it is up to date.

- [Define & create Documented Information](#)
- [Evaluate & review Documented Information](#)

2.15.1 Defining & creating Documented Information

Documented Information can be used and applied in several places in BIC GRC. The Document Owner is solely responsible for its creation and maintenance.

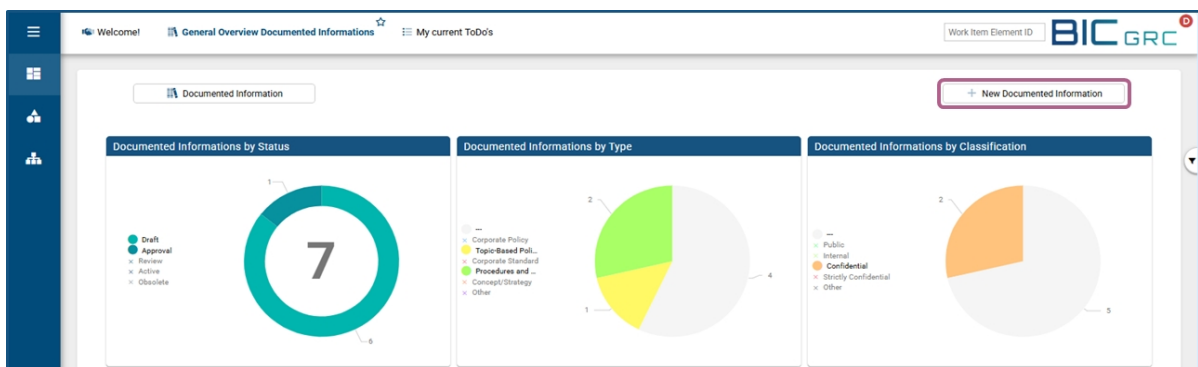
Step 1: Create Documented Information

The Document Owner can create *Documented Information* in several places in BIC GRC.

1. Creation via the "Documented Information Overview" dashboard

The Editor navigates to **Dashboards >> General Overview Documented Information >> "New Documented Information."**

New *Documented Information* is created using a button in the upper right corner of the window.

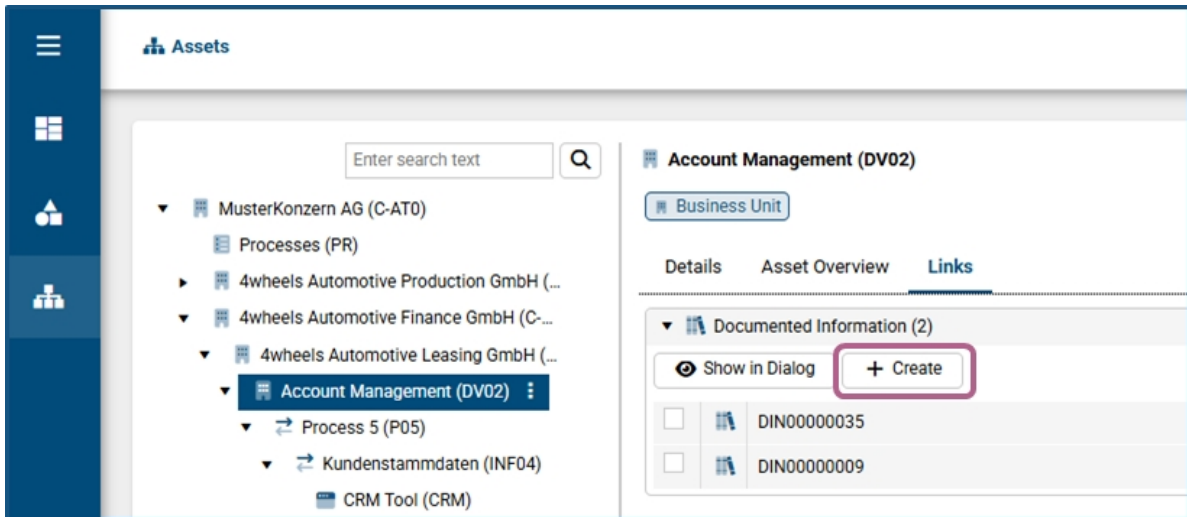


A new window then opens automatically.

2. Creation via Asset List

The Editor navigate to **Assets >> Select asset >> Links >> Open the "Documented Information" tab >> "Create."**

A new *Documented Information* item is created by clicking the "Create" button in the middle of the window.

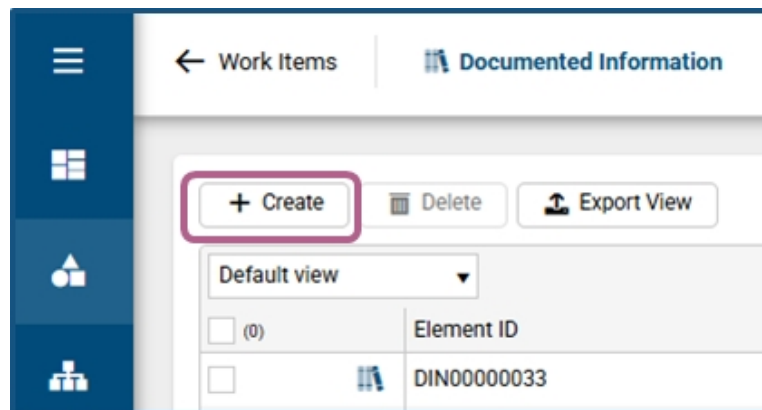


A new window then opens automatically.

3. Creation via Work Item list

The Editor navigates to
Work Items >>
Documented Information
>> "Create".

A new window then opens
automatically.



Step 2: Enter details

Documented Information Details

Status: ● Draft

* Name: Procedural instructions for ensuring the availability of business-critical processes (EN)

Details

Description

This procedure describes the organisational and technical measures aimed at ensuring the availability of business-critical processes, even in the event of a failure. It contains guidelines for identifying critical processes, defining recovery time objectives (RTOs), securing IT systems and external service providers, and conducting regular tests of emergency and recovery procedures.

Scope

Name	Asset Type	End-use...	
Account Management	Business Structure		

You have unsaved changes. Save Close

1 Name: The first step is to enter a short but meaningful name for the *Documented Information*.

2 Description: Next, enter a description of the *Documented Information*. All users downstream in the *Documented Information* workflow refer to this description, so it should contain as much necessary information and data as possible.

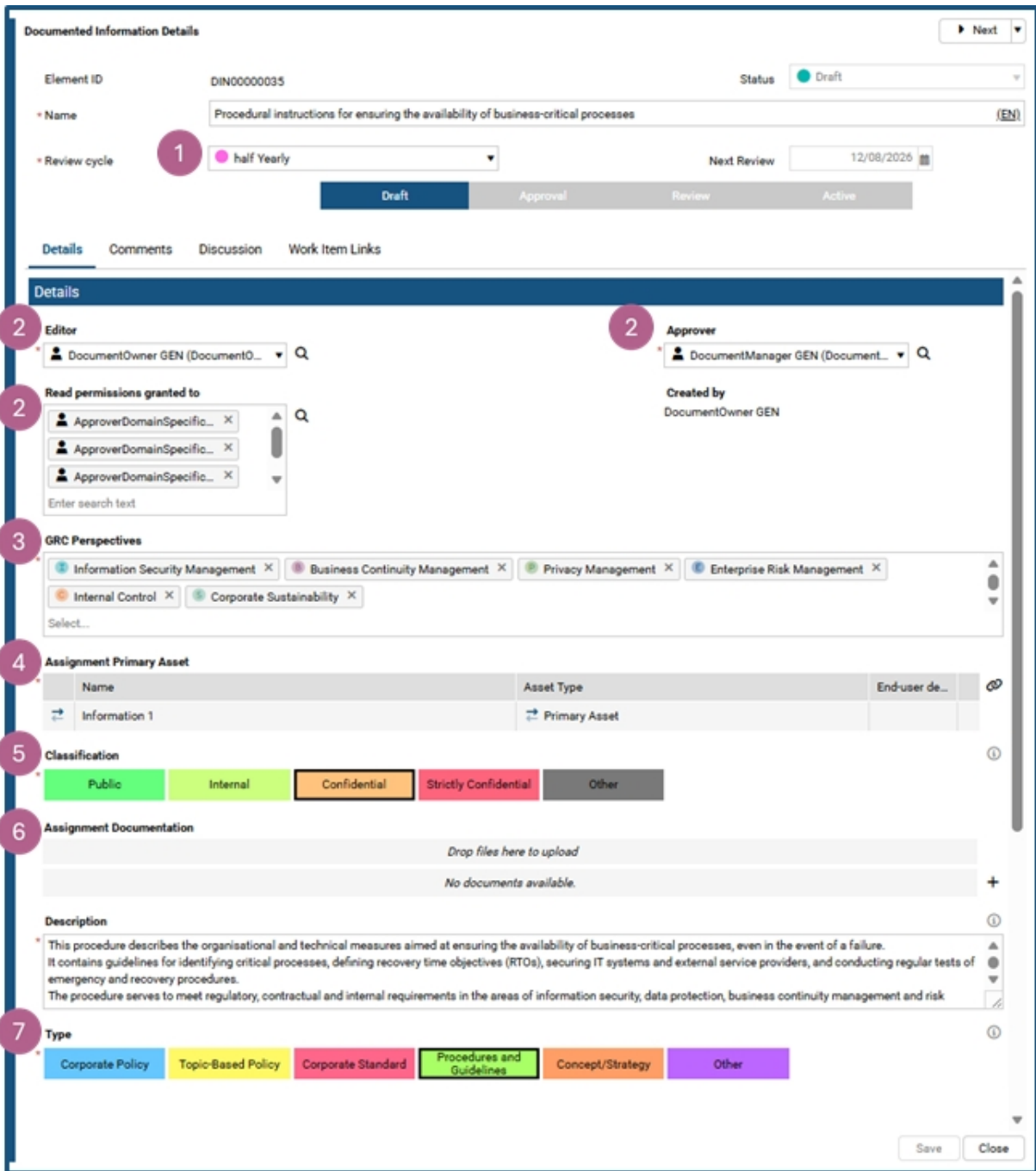
3 Scope: The *Document Owner* can link an Asset using the  icon.

The system supports assets of the types "Primary Asset" and "Business Unit".

The "Scope" link is automatically filled in if the creation was made via the Asset view (2).

4 Save: Once the information has been entered, the Document Owner can save it..

Step 3: Complete entries



The screenshot shows the 'Documented Information Details' form. The form is titled 'Documented Information Details' and has a 'Next' button in the top right corner. The form contains the following fields and sections:

- Element ID:** DIN00000035
- Status:** Draft
- Name:** Procedural instructions for ensuring the availability of business-critical processes (EN)
- Review cycle:** 1 half Yearly
- Next Review:** 12/08/2026
- Details:**
 - Editor:** 2 DocumentOwner GEN (DocumentO...)
 - Approver:** 2 DocumentManager GEN (Document...)
 - Created by:** DocumentOwner GEN
 - Read permissions granted to:** 2
 - ApproverDomainSpecific...
 - ApproverDomainSpecific...
 - ApproverDomainSpecific...
 - GRC Perspectives:** 3
 - Information Security Management
 - Business Continuity Management
 - Privacy Management
 - Enterprise Risk Management
 - Internal Control
 - Corporate Sustainability
 - Assignment Primary Asset:** 4

Name	Asset Type	End-user de...
Information 1	Primary Asset	
 - Classification:** 5
 - Public
 - Internal
 - Confidential
 - Strictly Confidential
 - Other
 - Assignment Documentation:** 6
 - Drop files here to upload
 - No documents available.
 - Description:**

This procedure describes the organisational and technical measures aimed at ensuring the availability of business-critical processes, even in the event of a failure. It contains guidelines for identifying critical processes, defining recovery time objectives (RTOs), securing IT systems and external service providers, and conducting regular tests of emergency and recovery procedures. The procedure serves to meet regulatory, contractual and internal requirements in the areas of information security, data protection, business continuity management and risk.
 - Type:** 7
 - Corporate Policy
 - Topic-Based Policy
 - Corporate Standard
 - Procedures and Guidelines
 - Concept/Strategy
 - Other

At the bottom right, there are 'Save' and 'Close' buttons.

- 1 Review Cycle:** The Document Owner must specify a "Review Cycle." The Review Cycle specifies how often *Documented Information* is returned to the "Review" Status in order to review the *Documented Information* at regular intervals.

The "Next Review" attribute field is set automatically by BIC GRC.

- 2 Responsible Persons:** The Document Owner is automatically stored in the "Editor" field and remains fixed. The Editor must store a Document Manager responsible for approving the *Documented Information* in the "Approver" user attribute.

Additionally, "Read-Only Persons" can be selected who require access to this information even though their user profile normally does not include read access.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

To make it clear at a glance who created the *Documented Information*, the Creator is also displayed in this section.

- 3 **GRC Perspective:** In order to clearly assign the *Documented Information* to one or more perspectives, the Document Owner must store perspectives.

The number of GRC Perspectives displayed depends on the modules that have been activated.

- 4 **Assigned Primary Asset:** This link can be filled in voluntarily, as a "Primary Asset" can also primarily be information, thus creating a connection.

- 5 **Classification:** Using a classification scheme, the *Documented Information* can be assigned one or none of the confidentiality levels.

- 6 **Assignment Documentation:** The assignment is the core of the Work Item, as the information is attached here.

- 7 **Type:** The type helps to classify the extent to which the *Documented Information* should be accessible to one or more user groups.

If the *Document Owner* seeks a more specific option, they can select "Other type." When "Other" is chosen, the *Document Owner* is shown an additional attribute in which they can manually enter text.

- 8 **Exception Scope:** In addition to the scope initially stored, the Document Owner can also specify in writing whether there are any exceptions to this scope.

- 9 **Reference controls:** The "reference control" leads to the Control Catalogs of

- ISO 27701:2019

- 10 **Status change:** After all information has been entered, a status change to "Approval" is performed in the upper right window.

The Document Manager is automatically informed of the status change by means of a notification.

Context

Scope

Name	Asset Type	End-user ...
Account Management	Business Structure	

8 Exception Scope

9 Reference Controls

No existing mapping.

Kontext

Scope

Name	Asset-Typ	Beschrei...
Standort Österreich	Unternehmensorganisation	

8 Ausnahme Scope

9 Referenz ISO 27001

Name	Katalog	B...
6.2 Informationssicherheitsziele und Planung zu deren Erreichung	ISO/IEC 27001:20...	

Dokumentierte Informationen nach ISO 27001

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)

After entering all the necessary information, the Work Item can be saved and a status transition can be executed before the window is closed manually.

If the entries require further attention, the Document Manager can leave a Comment in the "Comment" tab and reset the *Documented Information* to "Draft" Status. The Document Owner is notified of this process by means of a notification.

2.15.2 Evaluating & reviewing Documented Information

The *Document Owner* should regularly review the *Documented Information* to ensure that it remains up to date and correct.

The "Next review" field helps you to review this at regular intervals. Two weeks before the date is reached, the Editor automatically receives a notification reminding them of an upcoming reassessment.

On the day of the "Next Review," the *Documented Information* is switched from "Active" to "Review" status, and the assigned User automatically receives another notification.

The date is automatically reset after the status change depending on the time specified in "Review Cycle."

If the *Documented Information* has one of the review cycles "Every ... days," "Event-related," "Daily," or "Weekly," the status is not automatically reset.

Step 1: Navigate to Documented Information

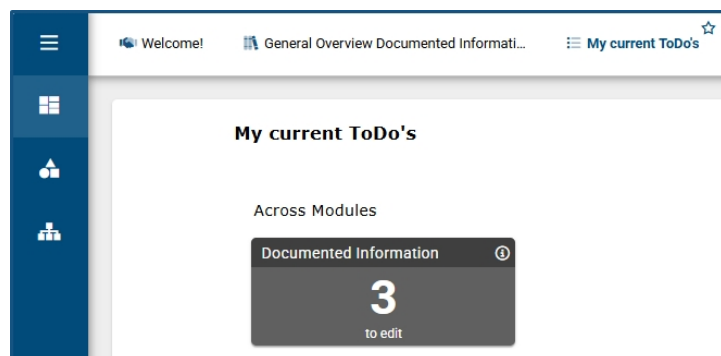
The *Document Owner* has two options for opening *Documented Information* to be edited.

1. Open via notification

The *Document Owner* automatically receives an E-Mail from BIC GRC as soon as the Review Cycle date is reached. The link to the specific *Documented Information* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

At the top of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still require action from the *Document Owner*.



Step 2: Review Documented Information

When reviewing, the *Document Owner* should start by reviewing the "Details" tab.

The Document Owner can view the entries in the "Review" status, and to make changes, they can switch back to the "Draft" status.

Step 3: Leave a comment

The *Document Owner* must still review the "Note" tab to ensure that the document is complete and up to date by clicking the "Document completeness and currency reviewed" checkbox.

Documented Information Details

◀ Draft

▶ Approval

Element ID

DIN00000035

Status

● Review

Name

Procedural instructions for ensuring the availability of business-critical processes

(EN)

Review cycle

● half Yearly

Next Review

12/08/2026

Draft

Approval

Review

Active

Details

Annotations

Comments

Discussion

Work Item Links

Annotations

Review

Review Date

Remarks of Review

* ☐

Completeness and timeliness of this document was verified

Save

Close

The "Review Date" is automatically set by BIC GRC as soon as the Document Owner has changed the status.

After the status has been changed to "Approval," the window can be closed.

2.16 Document Manager

The *Document Manager* user profile is responsible for approval and proper filing of specific information in BIC GRC.

2.16.1 Review & release Documented Information

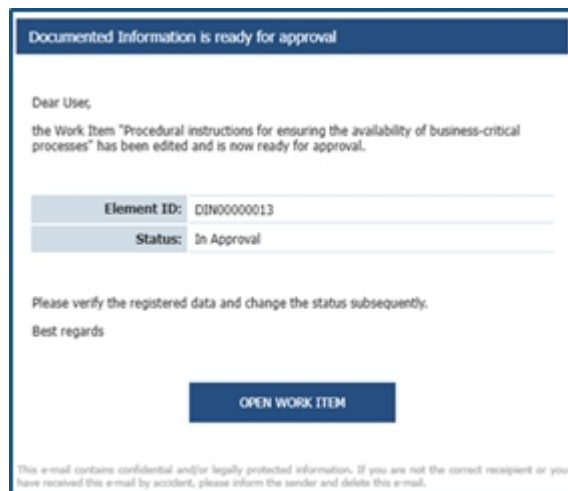
After a *Document Owner* has created and stored *Documented Information*, the *Document Manager* reviews it to prepare for activation and approval.

Step 1: Navigating to the Documented Information

The *Document Manager* has two options for opening *Documented Information* to be edited.

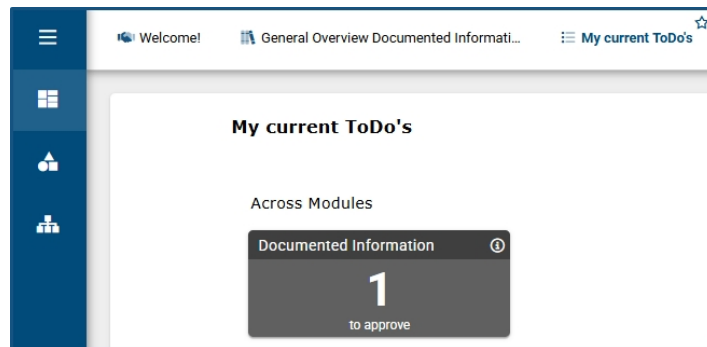
1. Open via notification

The *Document Manager* receives an E-Mail as soon as the *Document Owner* changes the Status of the *Documented Information* to "Approval." The link to the specific *Documented Information* is included in the notification.



2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still require action from the *Document Manager*.



Step 2: Review Documented Information

The *Document Manager* has full read access to the created and stored *Documented Information* in order to decide, based on all the information entered, whether the *Documented Information* has been sufficiently described and classified. If this is the case, the *Document Manager* can switch to "Active" status.

If further refinement is required, the *Document Manager* can add a Comment in the "Comment" tab and change the Status to "Draft."

Step 3: Leave a note

The *Document Manager* must still give the necessary approval in the "Annotation" tab by clicking the "Document complies with the necessary specifications" checkbox.

Documented Information Details ◀ Draft ▶ Active

Element ID: DIN00000035 Status: ● Approval

Name: Procedural instructions for ensuring the availability of business-critical processes (EN)

Review cycle: half Yearly Next Review: 12/08/2026

Draft **Approval** Review Active

Details Annotations Comments Discussion Work Item Links

Annotations

Review

Review Date:

Remarks of Review:

☐ Completeness and timeliness of this document was verified

Approval

Approval Date:

Remarks of Approval:

☒ Document corresponds with necessary guidelines

Save Close

A Remark of Approval may also be entered.

The "Approval Date" is set automatically by BIC GRC as soon as the *Document Manager* has changed the status.

2.17 Editor Audit

The *Editor Audit* is responsible for planning, creating, and executing *Audits* in BIC GRC. They can perform *Audits* using the information available in the modules in BIC GRC.

An Editor Audit in BIC GRC has the following tasks:

- [Define & create Audit](#)
- [Define & plan Audit Activity](#)
- [Start & execution Audit](#)
 - [Start & execute Audit Activity](#)
- [Identify & create Finding](#)
- [Manage & handle Finding](#)
- [Define & create Measures](#)
- [Evaluate & complete Audit](#)

2.17.1 Define & Create Audit

Audits can be performed at regular intervals in BIC GRC.

Audits can be performed voluntarily based on the information and data in BIC GRC.

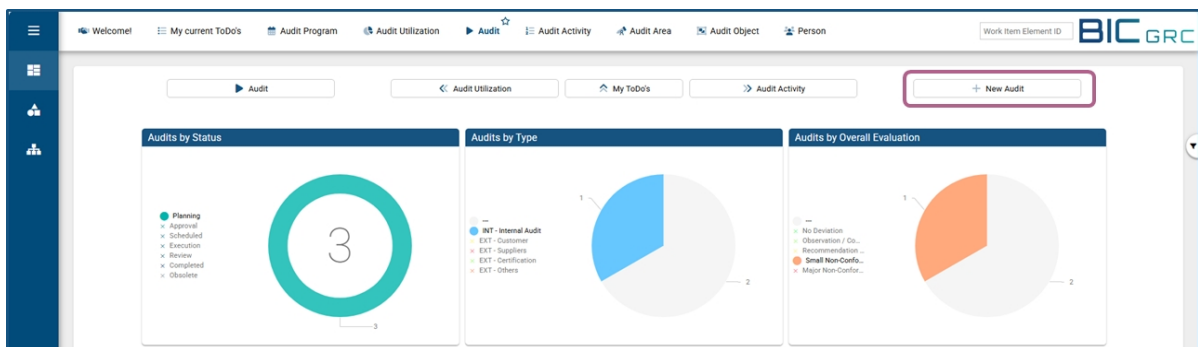
Step 1: Create Audit

The Editor Audit can create *Audits* in several places in BIC GRC.

1. Creation via the "Audit" Dashboard

The editor navigates to **Dashboards >> Audit >> "New Audit"**.

A new *Audit* is created by clicking a button in the upper right corner of the window.

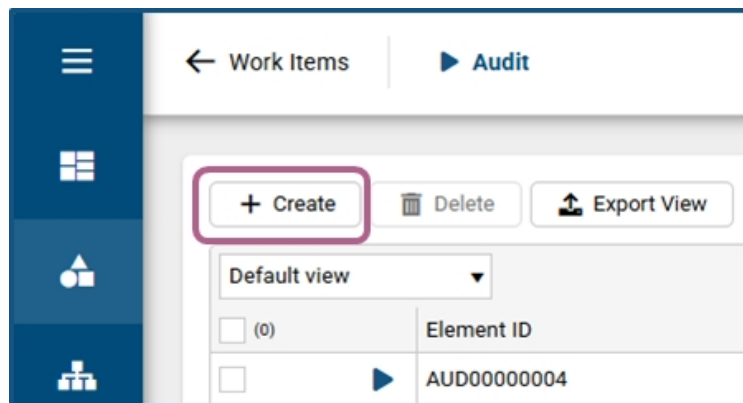


A new window will then open automatically.

2. Creation via Work Item List

The Editor navigates to **Work Items >> Audit >> "Create"**.

A new window will then open automatically.



Step 2: Enter details

Audit Details

Status: ● Planning

* Name 1 Comprehensive GRC audit to ensure the resilience and regulatory compliance of company-wide processes (EN)

Details

2 **Organizational Unit or Primary Asset**

Name	Asset Type	End-us...	
Location Austria	Business Structure		

3 You have unsaved changes. Save Save and Close Close

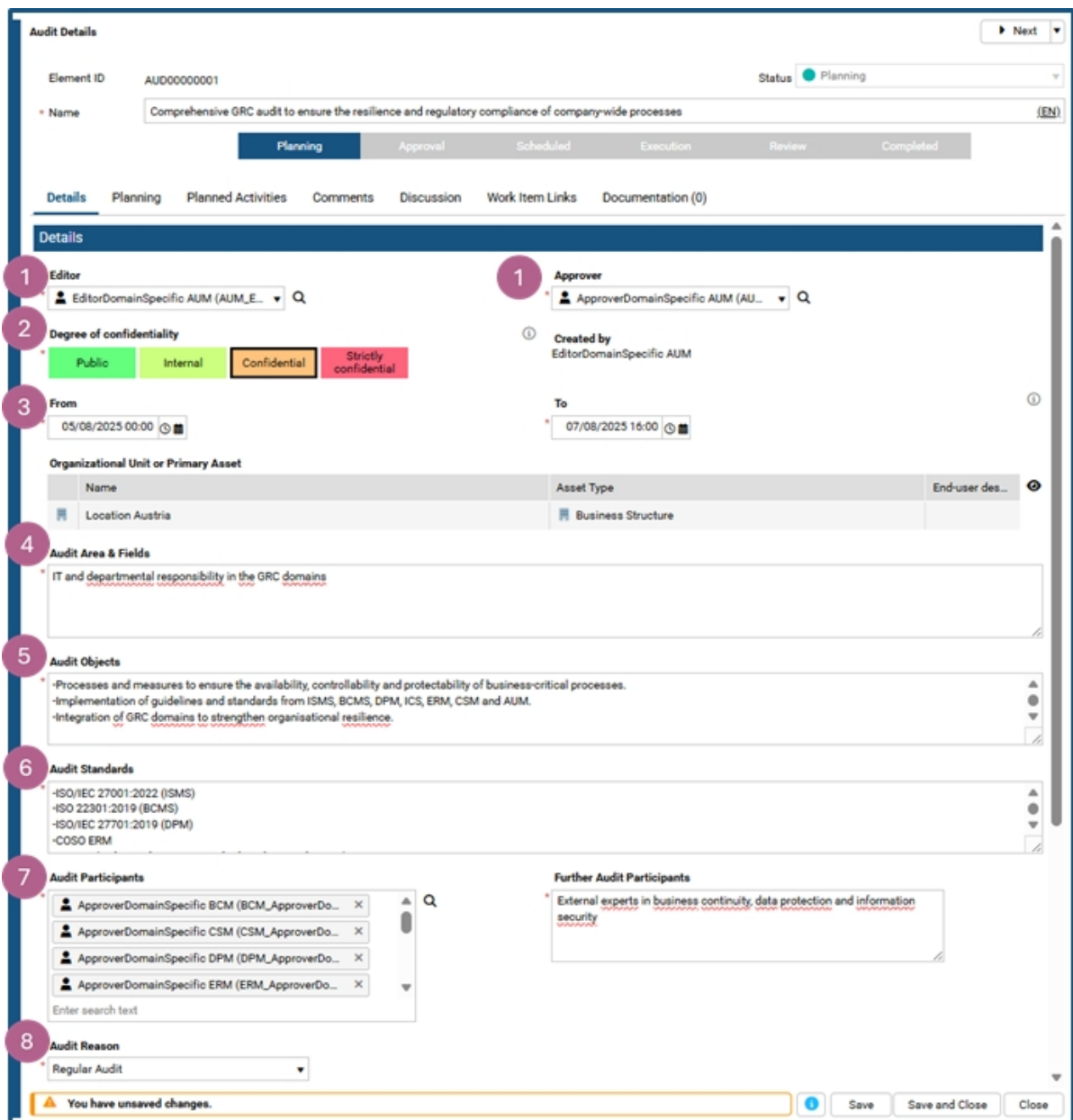
1 Name: The first step should be to enter a short but meaningful name for the *Audit*. The *Audit* is unique when the "name" is combined with the "Element ID."

2 Organizational unit or Primary Asset: A link to a "Business Unit" or "Primary Asset" is required using the icon  whereby preselected assets for which the Editor has permissions are displayed.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request..](#)

3 Saving process: After entering the necessary information, the *Audit* can be saved for the first time.

Step 3: Add details



- Responsibilities:** The current Editor is automatically entered in the "Editor" attribute. In addition, an "Approver" must be nominated to approve the *Audit*.

This User is searched for and linked using the  icon or suggested by entering the User's name in the attribute.

The initial Creator of the Work Item is also displayed in this section so that it is clear at a glance who created the *Audit*.

- Degree of Confidentiality:** The Editor can specify the Confidentiality level with which this *Audit* is to be treated.

This information is also displayed later on the cover sheet when the report is created.

- 3 **Period:** A period should be specified in which the *Audit* will be carried out. A suggested date for the next day is automatically stored when the Editor saves the *Audit* for the first time.

In addition to specifying a time period using dates, the exact time of day can also be entered. For example: An *Audit* may only be scheduled for 2 hours on a given day.

- 4 **Audit Area & fields:** In addition, the "Audit Area & fields" text field must be filled in.

- 5 **Audit Objects:** The Editor must specify in writing which Audit Objects will be used as the basis for the *Audit*.

- 6 **Audit Standards:** The Editor must specify in writing which standards serve as the basis.

- 7 **Contributors & Further Contributors:** The Editor can select contributing users from BIC GRC using the  icon. If the users aren't already registered in BIG GRC their contributions can be specified via text.

- 8 **Audit Reason:** In BIC GRC, there are two kinds of an *Audit*: a Regular Audit or a Special Audit.

If the reason is a "Special Audit," the Editor must also specify the category of the event or describe the event in a few words.

- 9 **Audit Type:** The "Audit Type" specifies whether it is an internal or external *Audit* or a customer or supplier *Audit*.

If "Special Audit" is specified under "Reason for audit," the User can select the "Certification" type.

If either supplier or customer *Audit* is selected, the Editor is also shown a link to the appropriate GRC framework so that the supplier/customer concerned can be linked directly.

- 10 **Audit Category:** The Editor is shown several categories from which they can select the type of *Audit*.

- 11 **Audit Dimension:** The Editor must decide whether it will be a full or partial *Audit*. Depending on the entry, the scope of the *Audit* will be larger or smaller.

- 12 **Audit Description:** Finally, the Editor must describe the *Audit* in words. Important information that is best suited for this field can also be stored here.

- 13 **Audit Non-Goals:** In addition to the scope, the Editor can also specify what aspects are outside the scope of the *Audit* and should not be targeted.

- 14 **Save:** Once all information has been entered, the *Audit* can be saved.

Once all details have been entered, you can switch to the "Planning" tab and continue

with step 4.

Audit Details

Next

Element ID

AUD00000001

Status

Planning

Name

Comprehensive GRC audit to ensure the resilience and regulatory compliance of company-wide processes

(EN)

Planning

Approval

Scheduled

Execution

Review

Completed

Details

Planning

Planned Activities

Comments

Discussion

Work Item Links

Documentation (0)

Context

9 Audit Type

INT - Internal Audit

10 Audit Category

Process Audit

11 Audit Dimension

Full Audit

12 Audit Description

This audit checks across domains whether the company's GRC components (in particular ISMS, BCMS, data protection, ICS, ERM and AUM) interact effectively to ensure the availability, controllability and protection of business-critical processes – even under disruptive or crisis conditions. The audit examines policy implementation, organisational resilience mechanisms, technical protective measures, policy compliance and the interaction of

13 Audit Non-Goals

This audit does not examine individual operational risks, but focuses on cross-domain GRC integration to ensure critical process availability.

You have unsaved changes.

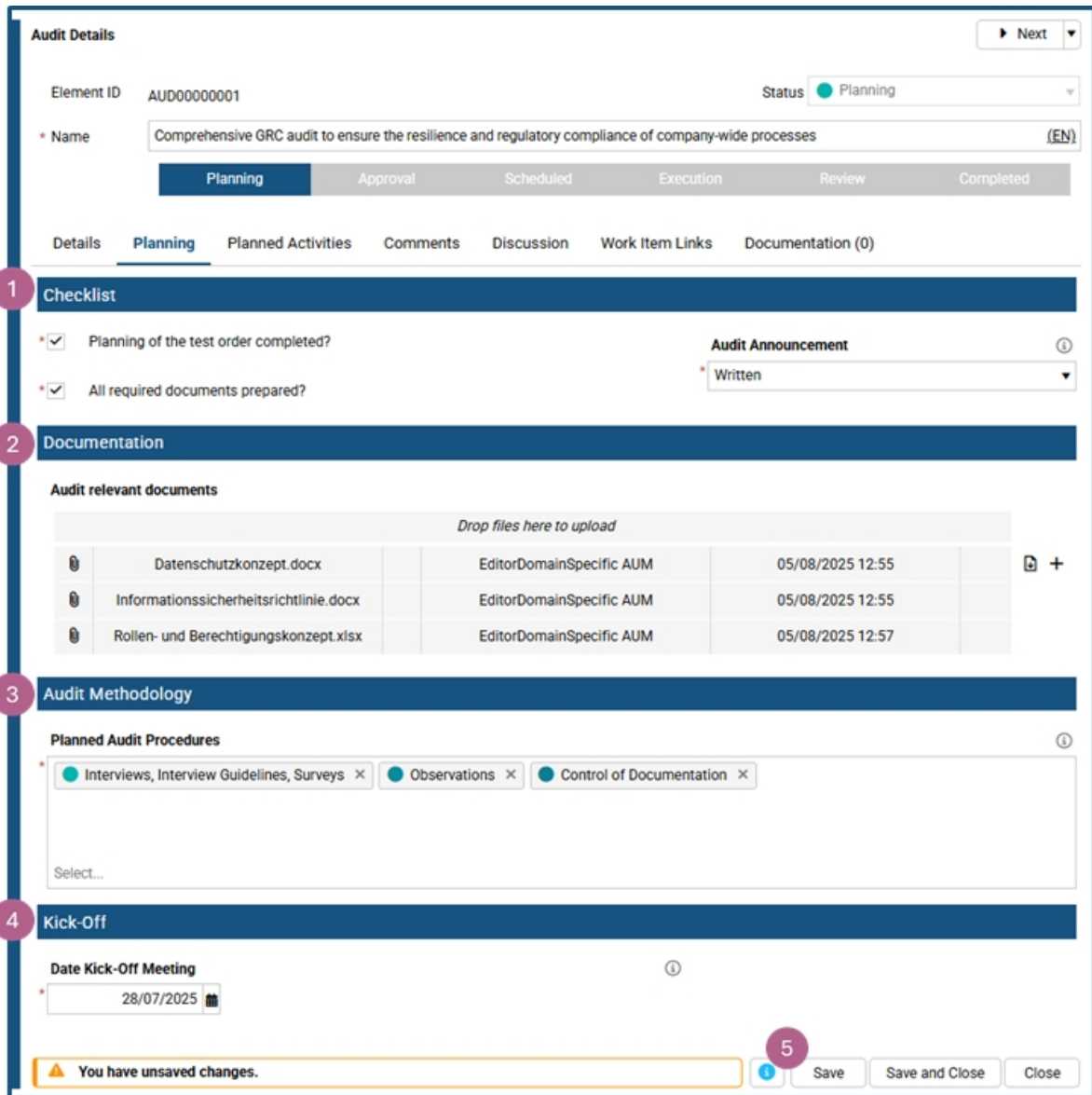
14

Save

Save and Close

Close

Step 4: Save Planning



Audit Details Next

Element ID: AUD00000001 Status: Planning

* Name: Comprehensive GRC audit to ensure the resilience and regulatory compliance of company-wide processes (EN)

Planning | Approval | Scheduled | Execution | Review | Completed

Details | **Planning** | Planned Activities | Comments | Discussion | Work Item Links | Documentation (0)

1 Checklist

* ☒ Planning of the test order completed?

* ☒ All required documents prepared?

Audit Announcement i

* Written

2 Documentation

Audit relevant documents

Drop files here to upload

	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 Audit Methodology

Planned Audit Procedures i

* Interviews, Interview Guidelines, Surveys Observations Control of Documentation

Select...

4 Kick-Off

Date Kick-Off Meeting i

* 28/07/2025

5 You have unsaved changes. Save Save and Close Close

- 1 Checklist:** Using the checklist, the Editor officially indicates whether the planning has been completed and all necessary documents have been prepared and saved.

In addition, the Editor must indicate whether and in what form the "Audit Announcement" has been made.

- 2 Audit-relevant documents:** To substantiate the question on the checklist as to whether all documents have been prepared, the Editor can enter relevant documents that should be used in the *Audit*.

These can be internal checklists, memos on the kick-off meeting, links to the internal SharePoint, or other relevant documents.

- 3 Planned Audit Procedures:** Under "Scheduled Audit Procedures," the Editor specifies which actions they want to take in the *Audit*.

In most *Audits*, at least one interview is conducted, and in financial *Audits*, "Document Control" is often carried out.

4 Kick-Off meeting: In addition to specifying the form in which the Audit Announcement was made, the date on which the official "Initial Meeting" takes place must be specified.

5 Save: Once the necessary information has been entered, the *Audit* can be saved for the first time.

Once all the details have been entered, you can switch to the "Scheduled Activities" tab and continue with step 5.

Step 5: Plan Audit Activities

The Editor can plan *Audit Activities* that will be executed later during the *Audit* period. The Editor creates *Audit Activities* using the icon . For more information on creation, see [Editor Audit - Define & Plan Audit Activity..](#)

No already existing *Audit Activities* can be linked. Instead, they always have to be created as new entries.

Step 6: Change status

Once all information has been entered and is correct, the Editor can change the status to "Approval."

The *Audit Approver* is informed of the status change via notification.

To switch to the "Approval" status, the Editor must first set all planned *Audit Activities* to "Scheduled".

2.17.2 Define & plan Audit Activity

After creating an *Audit*, suitable *Audit Activities* can be scheduled and carried out as part of the *Audit*.

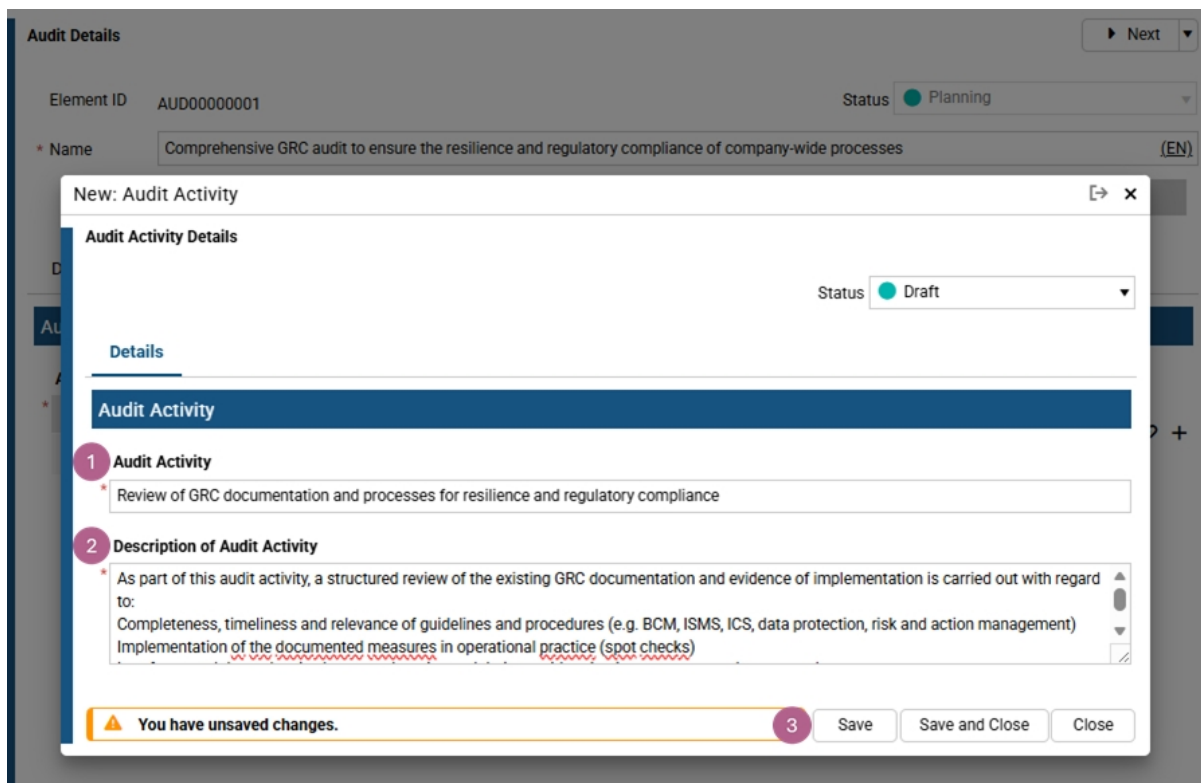
Step 1: Create Audit Activity

The *Audit Activity* can be created exclusively by the Responsible Editor from the *Audit* Work Item. A new *Audit Activity* is created in the "Audit Activities" tab of the Work Item.

Details	Planning	Planned Activities	Comments	Discussion	Work Item Links	Documentation (0)
Audit Activities						
Audit Activities						
	Element ID	Name	Status	Responsible		
	AUA00000005	Ganzheitliches GRC-Audit zur ...	Execution	EditorDomainSpecific AUM		

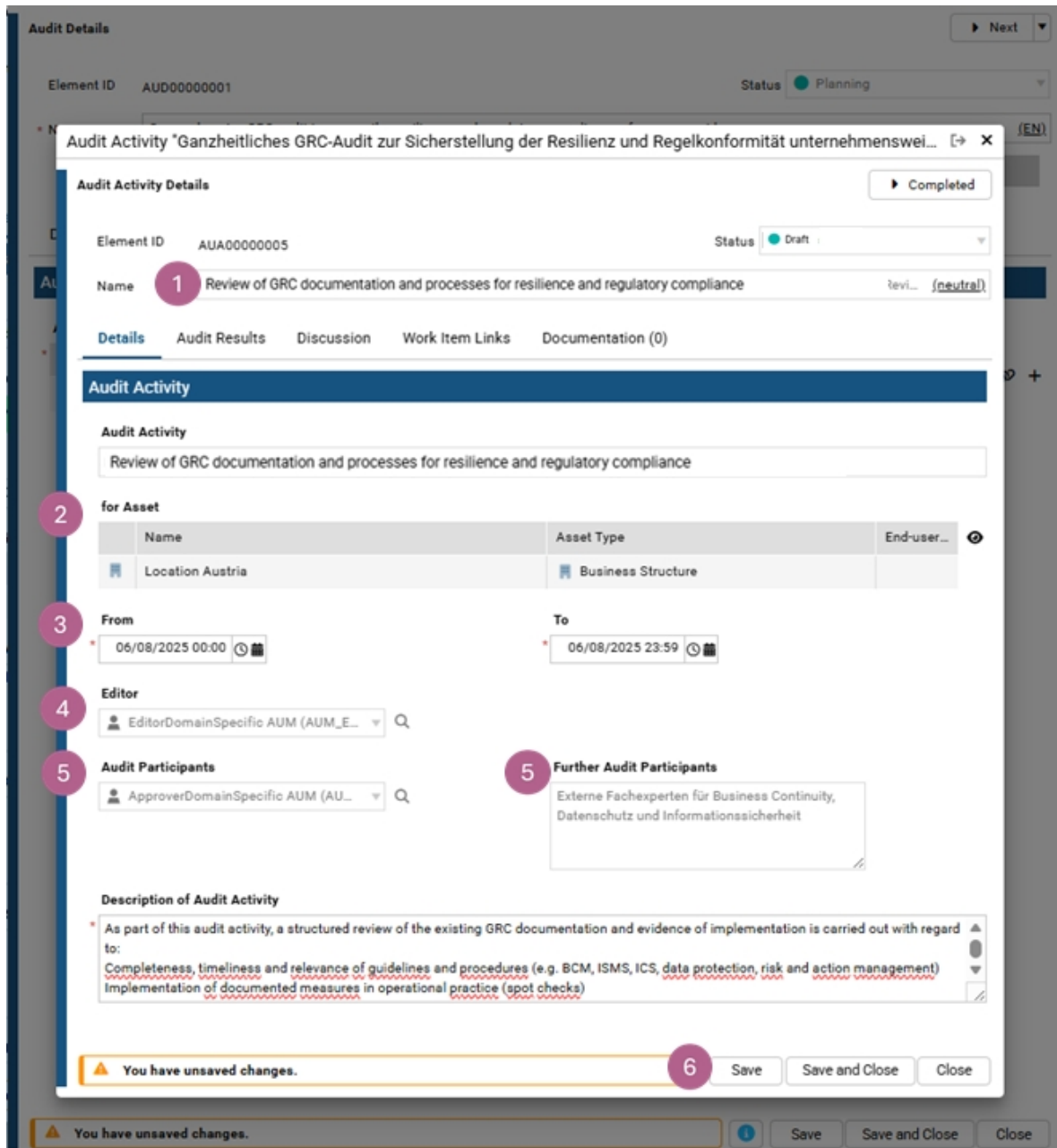
The *Audit Activity* is integrated into the *Audit* rather than opened in a new window.

Step 2: Define Audit Activity



- 1 Audit Activity:** The editor manually enters a name for the Audit Activity.
- 2 Description of Audit Activity:** The Editor can provide a detailed description of what needs to be done during the *Audit Activity*.
- 3 Save:** Once all information has been entered, the *Audit Activity* can be saved for the first time.

Step 3: Further procedure



Audit Details

Element ID: AUD00000001 Status: Planning

Audit Activity *Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmenswei...

Audit Activity Details

Element ID: AUA00000005 Status: Draft

Name (1): Review of GRC documentation and processes for resilience and regulatory compliance

for Asset (2)

Name	Asset Type	End-user...
Location Austria	Business Structure	

From (3): 06/08/2025 00:00 **To**: 06/08/2025 23:59

Editor (4): EditorDomainSpecific AUM (AUM_E...)

Audit Participants (5): ApproverDomainSpecific AUM (AU...)

Further Audit Participants (5): Externe Fachexperten für Business Continuity, Datenschutz und Informationssicherheit

Description of Audit Activity (6): As part of this audit activity, a structured review of the existing GRC documentation and evidence of implementation is carried out with regard to: Completeness, timeliness and relevance of guidelines and procedures (e.g. BCM, ISMS, ICS, data protection, risk and action management) Implementation of documented measures in operational practice (spot checks)

You have unsaved changes. Save Save and Close Close

1 **Name:** Once the *Audit Activity* has been saved for the first time, the name is set automatically.

The name is derived from the text entered in "Audit Activity."

2 **Asset:** The Asset is automatically transferred from the *Audit* when saving.

The Asset is Read Only and remains unchanged.

- 3 **Period:** The period is also taken from the *Audit* during the save process. However, the Editor can manually adjust the period to better specify the *Audit Activity* and its scope in terms of time.

If the Editor specifies a time period that aligns with the *Audit*, they will be notified.

- 4 **Editor:** The Editor is automatically transferred to the "Editor " attribute and remains fixed.

- 5 **Audit Participants:** The Editor can assign "Participants" in the *Audit Activity*, as in the *Audit*.

- 6 **Save:** Once the necessary information has been entered, the *Audit Activity* can be saved.

After entering all necessary information, the Work Item can be saved and a status transition can be performed before closing the window.

If the *Audit Activity* is unlinked from its *Audit*, it is deleted directly and is fully removed from the system.

If the *Audit* is set to "Obsolete" Status, the Audit Activity is also set to "Obsolete."

2.17.3 Start & Execution of Audit

The Editor is reminded by means of a notification in a scheduler that the *Audit* is to be executed. The reminder refers to the stored date on which the *Audit* is to begin.

Step 1: Navigate to Audit

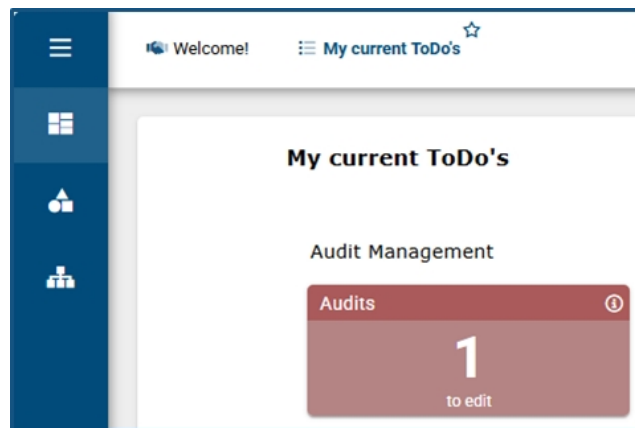
The *Editor Audit* has two options for opening an *Audit* to be performed.

1. Open via notification

The *Editor Audit* receives an E-Mail as soon as the date on which the *Audit* is to be performed has been reached. The link to the specific *Audit* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that the Editor still has to complete.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Audit*.

Step 2: Perform Audit Activities

The Editor Audit should switch to the "Audit Activities" tab. There they will find all the *Audit Activities* they have scheduled.

If additional *Audit Activities* are required, the Editor can add more as needed.

The Editor can find further steps for the execution of the *Audit Activities* under [Start & perform Audit Activity](#).

The Editor should then continue with step 3 in this section.

Step 3: Complete Audit Activities

Once all *Audit Activities* have been completed, the Editor should give a final evaluation of the entire *Audit*. For more information on this step, see [Assess & complete Audit](#).

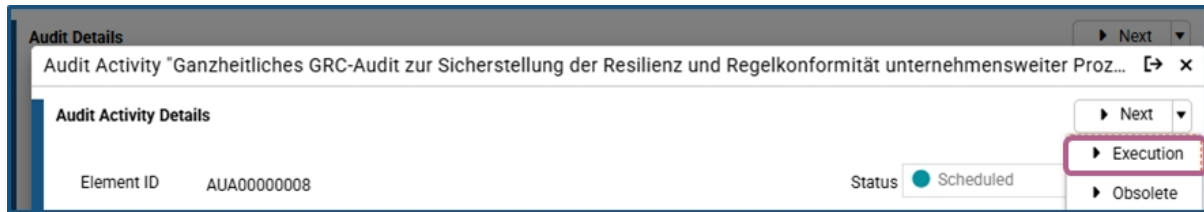
To switch to the "Review" status, all *Audit Activities* must have the status "Completed."

2.17.4 Start & Execution of Audit Activity

Once an *Audit* has been started, the Editor can also start executing the *Audit Activities*.

Step 1: Open Audit Activity

The *Audit Activity* should be opened via the *Audit* Work Item. The Editor can open the respective *Audit Activity* by double-clicking on an *Audit Activity* in the list.



The *Audit Activity* is integrated into the *Audit* rather than opened in a new window.

The Editor should switch to the "Execution" Status in the upper right corner of the window and to the "Audit Results" tab.

Step 2: Perform Audit Activity

Audit Activity "Ganzheitliches GRC-Audit zur Sicherstellung der Resilienz und Regelkonformität unternehmenswei..." [X] Next

Audit Activity Details Completed

Element ID: AUA00000005 Status: Execution

Name: Review of GRC documentation and processes for resilience and regulatory compliance (neutral)

Details **Audit Results** Discussion Work Item Links Documentation (0)

1 Audit Result

Target State

* Appropriate organisational, technical and documented measures ensure that all business-critical processes remain available, protected and controllable even in the event of a malfunction. These include:
Complete and up-to-date documentation of processes
An established procedure for emergency management and recovery

Actual State

* The documentation of the restart procedures is only available in its current form for some processes. There is no evidence of regular testing of the emergency and recovery plans. Responsibilities in crisis situations are not consistently regulated. Access protection concepts are not implemented uniformly and in some cases are not documented and reviewed.

2 Result

Result Evaluation

* No deviation Observation / Comment Recommendation / Determination Small non-conformity Major nonconformity / deficiency

3 Description of Deviation

* There are minor deviations from the documented procedural instructions for ensuring the availability of business-critical processes. In particular, there is a lack of complete evidence of the test cycles and the evaluation of the RTO specifications. The lack of clarity regarding responsibilities can lead to delays in crisis response in an emergency.

Recommendation of Treatment

* Complete update of procedural instructions and restart plans
Definition and communication of clear responsibilities in the event of a malfunction
Introduction of a standardised format for documenting emergency tests
Conducting internal training on crisis response and availability assurance

4 Finding

Finding

Element ID	Name	Responsible	Status	Report Date	to process by
FIN00000017	Unvollständige Ums...	EditorDomainSpecif...	Registrati...	08/08/2025	

5 You have unsaved changes. Save Save and Close Close

1 Audit Result: The editor documents the desired "Target State" before and a description of the actual "Current State."

2 Result Evaluation: Once there is an overview of the possible gap between the Target State and the Current State, the Editor must assess the result.

In the best case, there is "no deviation" between the Target State and the Current State, and in the most challenging case, a "major deficiency."

If the result is a Small or Major Non-Conformity, the Editor must specify a *Finding*.

- 3 **Description of the Deviation & Recommendation of Treatment:** The Editor must also submit a written statement. In the "Description of the Deviation" text field, they can specify what deviations they believe have occurred and at the same time make "Recommendations of Treatment" to improve the situation.

If there is a deviation—regardless of its classification—it must be entered in the two text fields.

- 4 **Finding:** Creating a *Finding* allows the Editor to specify more precisely what they noticed during the *Audit Activity*. For more information, see [Editor Audit - Identifying & Creating Findings](#).
- 5 **Save:** Once all information has been submitted, the *Audit Activity* can be saved.

Step 3: Complete Audit Activity

Once all entries have been made and findings created, the *Audit Activity* can be set to "Completed" Status.

Return to the step [Editor Audit - Start & perform Audit](#) Step 5.

2.17.5 Identify & create Finding

If, while executing an *Audit Activity*, the audit processor identifies opportunities for improvement or deviations, the *Editor Audit* must create a *Finding*.

Step 1: Create Finding from Audit Activity

A *Finding* can arise from an *Audit Activity*.

It is created using the  icon after a written statement has been made under "Decisions made."

Step 2: Documenting Finding

10

Registration

1

Name

* Documentation gap in the 2025 emergency test protocol (EN)

Details

2

GRC Perspective

P Privacy Management

3

Editor

EditorMeasure

4

Report Date

* 31/07/2025

5

to process by

* 11/09/2025

6

Type of Finding

Observation Recommendation Improvement Request Insignificant Nonconformity Significant Nonconformity

7

Finding for these Assets:

Name	Asset Type	End-u...
Group	Business Structure	

8

Description of Finding

* During the review of the emergency tests carried out, it was found that the complete test protocol for 2025 had not yet been stored in the central document management system. The implementation itself is documented, but the filing process was incomplete.

9

Priority of Finding

Very Low Low Medium High Critical

Save

Save and Close

Close

- Name:** The first step should be to enter a short but meaningful name for the finding.
- GRC-Perspective:** The Perspective is selected manually from the *Audit Activity*; the Editor can choose the Perspectives that were considered in the context of the *Audit Activity*.
- Editor:** The Editor responsible for handling the *Finding* of the *Audit Activity* is entered in this attribute.

The Creator is also displayed in this section so that it is clear at a glance who created the *Finding*.

For more information on treating *Findings*, see [Editor Audit - Manage & treat findings](#).

- 4 **Report Date:** The Creator specifies when they officially reported or discovered the *Finding*, which can differ from the current date.
- 5 **To process by:** The date below refers to the date by which the *Finding* should be resolved. It is intended as a guide for downstream users in the workflow to indicate when the *Finding* should ideally be resolved.
- 6 **Type of Finding:** The Creator can classify how serious the *Finding* is in the Context of the *Audit Activity* on a scale of five levels.
- 7 **Finding for this asset:** The asset is entered manually rather than being automatically transferred from the Work Item.

If the user wishes to link an Asset but has not yet been assigned a role on it, the user can use the Work Item *Permission Request* to request the appropriate authorization for the Asset. For more information, see [Standard User - Define & create Permission Request](#).

- 8 **Description of the finding:** The "Description of the finding" should contain as much information and input as possible, for example, how the finding was discovered. Furthermore, conclusions about cause and effect may be drawn.
- 9 **Priority of finding:** A priority is assigned to the *Finding*, which can later be used for evaluations on dashboards.
- 10 **Status change:** The Creator can then switch to the "Treatment" status. For more information on changing the status, see View & Process Findings.

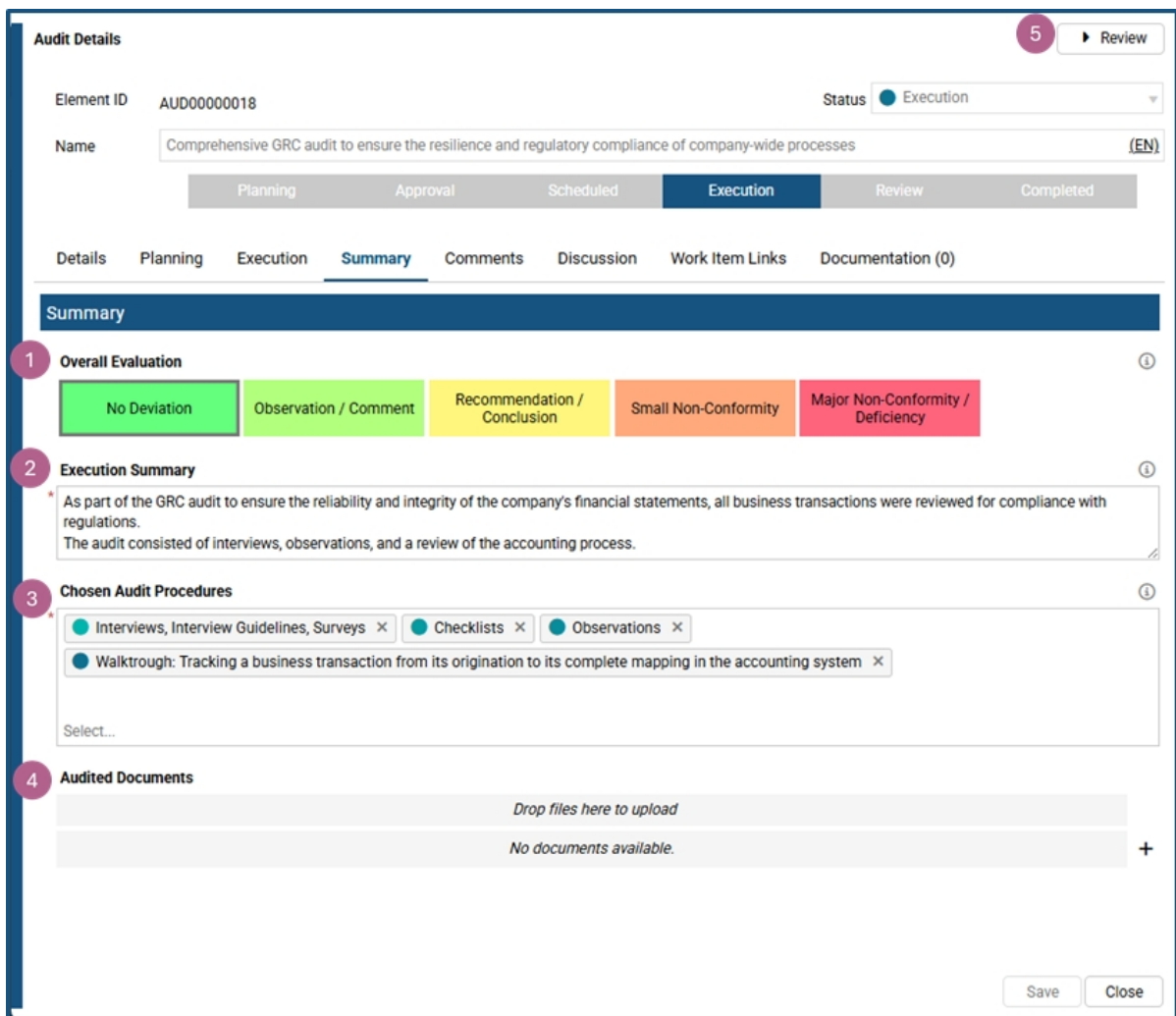
The Editor can then return to the *Audit Activity* and continue working there. [Editor Audit - Start & Perform Audit Activity](#).

2.17.6 Evaluate & complete Audit

After the execution of all *Audit Activities*, the *Editor Audit* must provide an overall assessment of the *Audit*.

The entire *Audit* is evaluated in the "Summary" tab.

Step 1: Evaluate Audit



Audit Details 5 Review

Element ID: AUD00000018 Status: Execution

Name: Comprehensive GRC audit to ensure the resilience and regulatory compliance of company-wide processes (EN)

Progress: Planning Approval Scheduled **Execution** Review Completed

Details Planning Execution **Summary** Comments Discussion Work Item Links Documentation (0)

Summary

1 **Overall Evaluation**

No Deviation Observation / Comment Recommendation / Conclusion Small Non-Conformity Major Non-Conformity / Deficiency

2 **Execution Summary**

As part of the GRC audit to ensure the reliability and integrity of the company's financial statements, all business transactions were reviewed for compliance with regulations. The audit consisted of interviews, observations, and a review of the accounting process.

3 **Chosen Audit Procedures**

Interviews, Interview Guidelines, Surveys Checklists Observations Walkthrough: Tracking a business transaction from its origination to its complete mapping in the accounting system

Select...

4 **Audited Documents**

Drop files here to upload

No documents available.

Save Close

- 1 **Overall evaluation:** After the Editor has reviewed all *Audit Activities* and their results once again, they can enter an "overall evaluation" of the *Audit*.

The result of the "Overall evaluation" applies to the entire *Audit* and to all parts of the *Audit*.

If the "Overall evaluation" identifies an opportunity for improvement or a significant area for enhancement, the manager of the Audit Management module is notified of the result.

- 2 **Execution Summary:** In this text field, the Editor must indicate how the overall impression of the *Audit*, the execution, and any challenges were managed.
- 3 **Chosen audit procedures:** The *Audit* procedures ultimately used may often differ from the planning. Therefore, the Editor must indicate which *Audit* procedures were performed for the *Audit*.

The "Scheduled Audit Procedures" are automatically adopted as a proposal, and they can be revised as necessary.

4 **Audited Documents:** The Editor must record which documents were ultimately used for the *Audit*.

5 **Status change:** The Editor can finally switch to the "Completed" status.

Once an *Audit* has been closed, it is considered final.

2.18 madcApprover Audit

An Approver Audit in BIC GRC is responsible for the final review and formal approval of an *Audit*. They ensure that all *Audit Activities* have been carried out and documented properly and that the findings are traceable and compliant with regulations.

The *Approver Audit* in BIC GRC has the following tasks:

- [Review & approve Audit](#)

2.18.1 Review & approve Audit

The *Audit Approver* is notified after an *Audit* has been created by the Editor Audit .

Step 1: Navigate to Audit

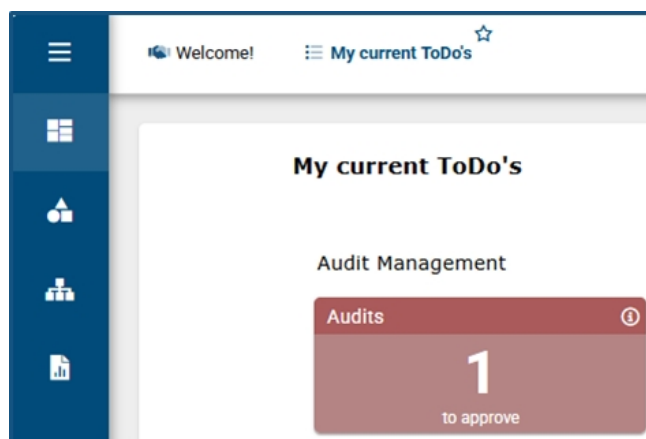
The *Approver Audit* has two options for opening an *Audit*.

1. Open via notification

The *Approver Audit* automatically receives an E-Mail from BIC GRC as soon as an *Audit* has been created and edited and a status transition has taken place. The link to the specific *Audit* is included in the notification.

2. Open via the "My current ToDo's" Dashboard

In the upper part of the "My current ToDo's" dashboard, there are tiles that show the number of Work Items in each Status. Clicking on the tile opens a list of all Work Items in this Status that still require Approval from the Approver.



Step 2: Review Audit

The *Approver Audit* has full read access to the scheduled *Audit* so that they can use the information entered to decide whether the *Audit* has been planned correctly and the effort required for the *Audit* has been estimated correctly.

If further adjustments are required, the Approver Audit can leave a comment in the "Comment" tab and change the status to "Planning."

Audit Details

Element ID: AUD00000018 Status: ● Approval

Name: Comprehensive GRC audit to ensure the resilience and regulatory compliance of company-wide processes (neutral)

Planning **Approval** Scheduled Execution Review Completed

Details Planning Planned Activities **Comments** Discussion Work Item Links Documentation (0)

Comments

Comment

Enter your comment here. (0/1000)

+ Add Comment

All Comments

Save Close

Step 3: Perform status transition execution

If the entries made by the upstream user are correct, the Approver can change the status to "Scheduled." The responsible Editor is notified of the status change via notification.

The "Scheduled" status remains until the *Audit* is actually started.

2.19 Executive

Users with the *Executive* user profile are part of the Organization's management board. They have extensive rights in BIC GRC to make decisions for different areas based on the data and information entered in the system. They focus exclusively on strategic decision-making.

Management has the following tasks in BIC GRC:

- [Review & approve Security Risks](#)
- [Review & approve Management Review](#)
- [Open & generate report\(s\)](#)

2.19.1 Review & approve Security Risk

A Security Risks is created and evaluated by the person responsible for the risk before it is approved by various authorities. If the Security Risk has a particularly high Risk Value, the Executive can be informed by setting this specific Security Risk to “Management Approval” status.

This option must be enabled in the “Solution Configuration.”

Step 1: Navigate to specific Security Risk

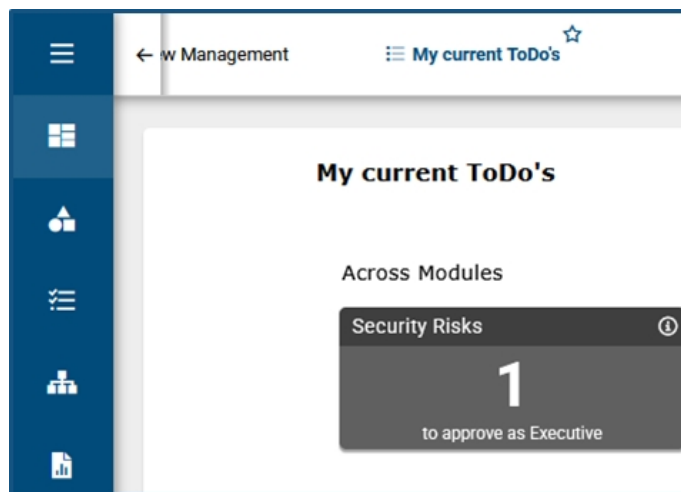
The Executive has two options for opening a Security Risks.

1. Open via notification

The Executive receives an E-Mail as soon as the Approver changes the status of the Security Risks to “Management Approval.” The link to the specific Security Risks is then included in the notification.

2. Open via the “My current ToDo's” dashboard

The upper part of the “My To- Do's” dashboard contains tiles that display the number of Work Items in each Status. Clicking on a tile opens a list of all Work Items in that Status that require Approval by the Executive .



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for Security Risks.

Step 2: Perform Approval

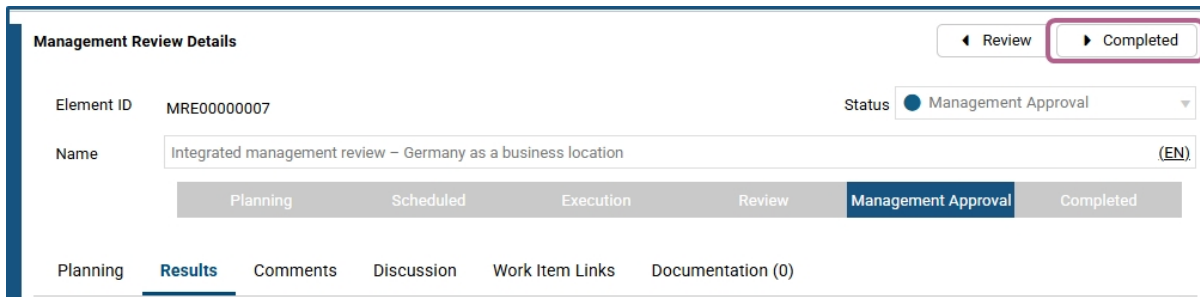
The *Executive* has full read access to the created and evaluated Security Risks in order to decide, based on the information entered, whether the Security Risks have been mitigated to a sufficient extent and whether the residual risk for the Company can be borne in its scope.

If this is not the case and the Security Risks needs to be reassessed from the *Executive* 's perspective, the *Executive* can leave a comment in the “Comment” tab and change the status to “Gross Evaluation” or “Net Evaluation.”

If further evaluation from the perspective of the Approver Risk is required, the Executive can leave a comment in the "Comment" tab and change the status to "Review."

Step 3: Perform status transition execution

If the entries made by the upstream User are correct, the *Executive* should change the Status to "Completed."



The screenshot shows the 'Management Review Details' form. At the top right, there are two buttons: 'Review' and 'Completed'. The 'Completed' button is highlighted with a red box. Below the buttons, the 'Status' dropdown menu is set to 'Management Approval'. The 'Element ID' is 'MRE00000007' and the 'Name' is 'Integrated management review – Germany as a business location'. Below the form, there is a progress bar with stages: Planning, Scheduled, Execution, Review, Management Approval, and Completed. The 'Management Approval' stage is currently active. At the bottom, there are tabs for Planning, Results, Comments, Discussion, Work Item Links, and Documentation (0). The 'Results' tab is selected.

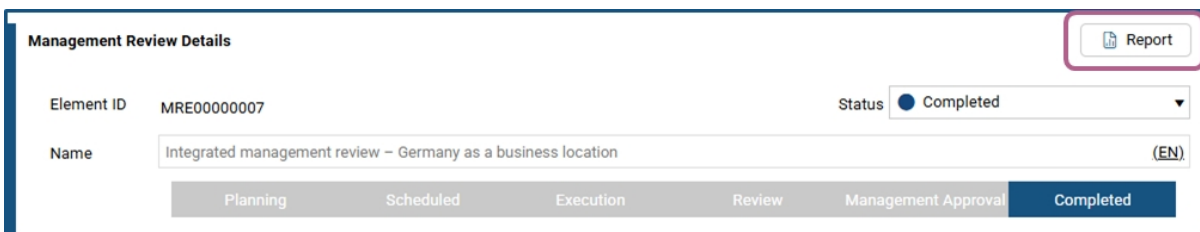
The Editor is notified of the status change to "Completed" by means of a notification.

Step 4: Generate report

Once the *Management Review* has been changed to "Completed" status, the Editor and the Executive can generate a report.

The report is a summary of the entire *Management Review*.

The report execution occurs in the upper right-hand corner of the Work Item window. The output file is a PDF.



The screenshot shows the 'Management Review Details' form with the status changed to 'Completed'. The 'Status' dropdown menu is now set to 'Completed'. The 'Element ID' is 'MRE00000007' and the 'Name' is 'Integrated management review – Germany as a business location'. Below the form, the progress bar shows the 'Completed' stage as the final stage. At the top right, the 'Report' button is highlighted with a red box.

2.20 Special User Profiles

In addition to the standardized and technical user profiles, there are also "Special User Profiles." These user profiles have a specific task in BIC GRC.

"Special User Profiles" can be assigned to specific Users in addition to their actual user profiles.

Internal request recipient:

- [Answer & process Internal Requests](#)

Authorization Request Recipient:

- [Respond to & edit Permission Requests](#)

2.20.1 Respond to & process Internal Requests

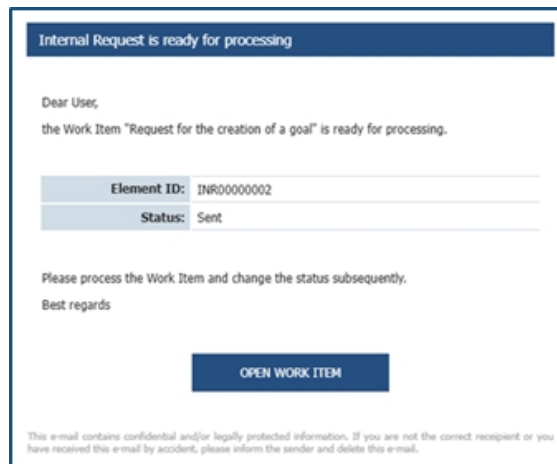
After a *Standard User* has submitted an *Internal Request*, an user who is a member of the "Internal Request Receiver" group must respond to it.

Step 1: Navigating to the Internal Request

The Recipient has two options for opening an *Internal Request*.

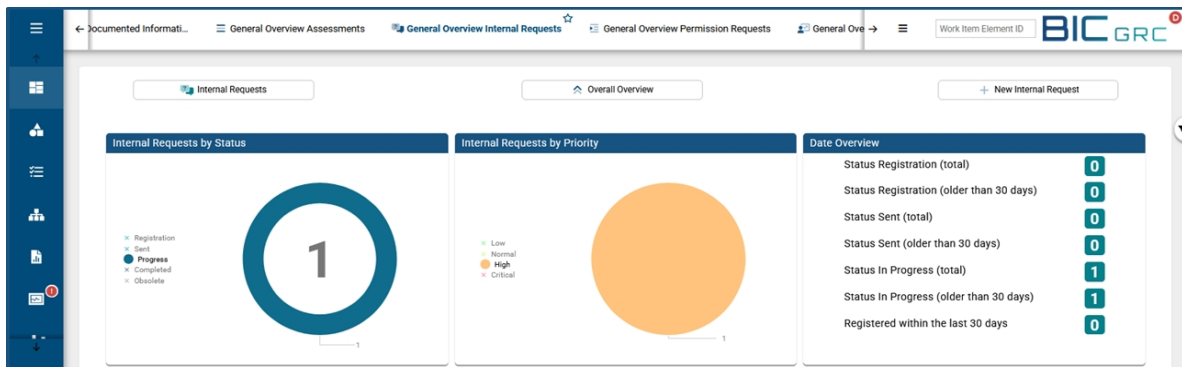
1. Open via notification

The recipient receives an E-Mail as soon as the Creator of the *Internal Request* changes the Status to "Sent." The link to the specific *Internal Request* is included in the notification.



2. Open via the "Internal Request" Dashboard

The Recipient can filter for their *Internal Requests* in the dashboard.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Internal Request*.

Step 2: View Internal Request

First, the Recipient should change the status from "Sent" to "Progress."

The Creator is informed of the status change via notification.

The Recipient has full read access to the created *Internal Request* so that they can decide how to proceed with the *Internal Request* based on the information entered. To do this, they should review the entries in the "Request" tab before starting a discussion in the "Discussion" tab. The "Discussion" tab should help the Recipient find the right contact person for the discussion and obtain all the information they need to respond to the *Internal Request*.

If the Recipient is also the Processor, they can switch to the "Progress" tab and begin responding to the Request. If another Processor is more suitable, the recipient can select them in the "Progress" status. The Processor will be notified of the nomination.

Step 3: Edit Internal Request

Internal Request Details

Element ID: INR00000001 Status: In Progress

Name: Request for the creation of a goal (neutral)

Request Discussion **Processing**

Processing of Request

1 **Processor**: Fachadministrator Rainer (Functional...)

2 **Date of Processing**: 12/08/2025

3 **Description of Processing**: Onboarding for goal setting held

4 **Further Implications**: Please describe which further implications, if any, result from the request.

5 **Status**: In Progress (Registration, Next)

- 1 **Processor**: The Editor is automatically set to the user who was entered as the "Recipient" by the Creator.
- 2 **Date of Processing**: The Editor must specify the date on which they processed the *Internal Request*.
- 3 **Description of processing**: The Editor must then describe how they handled and processed the *Internal Request*.
- 4 **Further Implications**: Furthermore, information can be provided on the consequences of the *Internal Request*.
- 5 **Status change**: Once the information has been entered, the user can save it and change the status to "Completed."

The Creator is informed of the status change via notification.

After the status change, the window can be closed.

2.20.2 Respond to & edit Permission Requests

After a *Standard User* has submitted a *Permission Request*, an user who is a member of the "Permission Request Receiver" group must respond to it.

Step 1: Navigate to the Permission Request

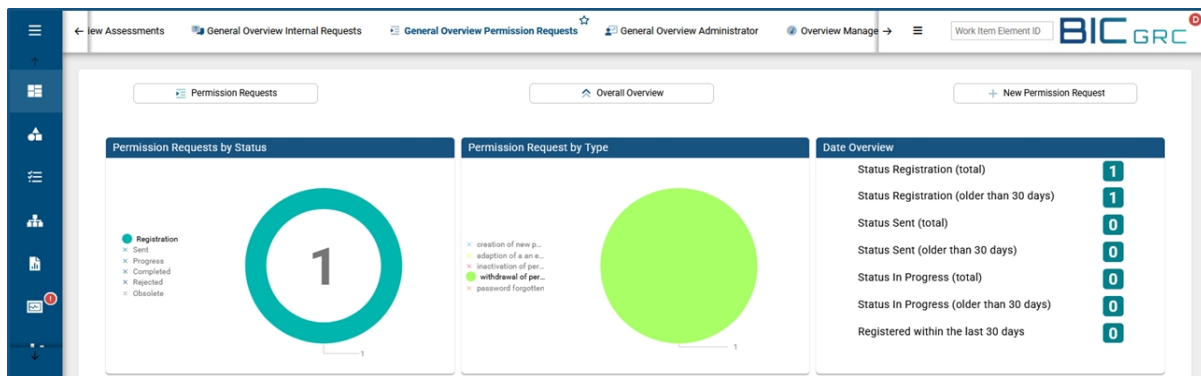
The Recipient has two options for opening a *Permission Request*.

1. Open via notification

The recipient receives an E-Mail as soon as the Creator of the *Permission Request* changes the Status to "Sent." The link to the specific *Permission Request* is included in the notification.

2. Open via the "Internal Request" dashboard

The Recipient can filter for their *Permission Request* in the dashboard.



Clicking on the notification link or a list item in BIC GRC automatically opens a new window for the *Permission Request*.

Step 2: View Permission Request

First, the Recipient should change the status from "Sent" to "Progress."

The Creator is informed of the status change by means of a notification.

The Recipient has full read access to the *Permission Request* that has been created so that they can decide how to proceed with the *Permission Request* based on the information entered. To do this, they should review the entries in the "Permission Request" tab.

If, after reviewing the information, the Request Processor decides that the *Permission Request* is justified, they can approve it. To do this, they can change the status to "Approved."

The Creator is notified of this status change via notification as a medium.

Otherwise, the Request Editor can begin processing the request.

Step 3: Edit Permission Request

Permission Request Details

Element ID: PER00000001 Status: In Progress

Name: Max Mustermann hat sein Passwort vergessen (neutral)

Navigation: Permission Request | **Processing** | Comments | Discussion

Processing of Request

- ☒ Specific approval is necessary
- Approver**

Technischer-Administrator Susanne (...)

Relationship to User

Technischer Admin
- Scheduled Review of the Permissions**

- Approval Remarks**
- ☒ I hereby confirm the legitimacy of the request.
- Date of Implementation**

12/08/2025

Buttons: Save Save and Close Close

- 1 Special approval:** If the Request Processor is unsure whether they can grant the authorization, they should also nominate an "Approver."

The registered "Approver" will be informed by notification as a medium.

- 2 Scheduled review of the Permissions:** It is possible to specify whether and when a review of the newly granted authorizations should be carried out.

A date is set automatically unless "Event-driven" is selected.

The Request Processor will be automatically notified by means of a notification 14 days before the next evaluation of the authorization. For this, the *Permission Request* must have the Status "Completed."

- 3 **Approval Remarks:** The note refers to the legitimacy of the authorization assignment and can be expanded by the Request Processor to include all necessary information.
- 4 **Approval:** The Processor of the request clicks the corresponding checkbox "I hereby confirm the legitimacy of the request." This action enables a status change.
- 5 **Date of Implementation:** Finally, the Request Processor must specify the date when they carried out the Execution.
- 6 **Status change:** Once the information has been entered, the Request Processor can save it and change the status to "Completed."

The Creator of the request is informed of the status change via notification.

After the status change, the window can be closed.

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.