Event Management User Manual

CERRIX B.V.
Version 6.2
2021

Confidential

This standard is used by:

CERRIX B.V.

CERRIX Version	6.2
Document Version	1.0
Date	01-07-2021
Classification	Confidential
Author(s)	N. van der Heijden & R. Andeweg

Table of contents

1. Introduction

This manual describes the function and roles for the Events module in CERRIX. The module used to be named Loss Events Registration (LER) but is renamed since CERRIX Version: 4.18.9

1.1. Events

Besides the registration of events or incidents, users can also report near loss events or incidents. The events or incidents are assessed, evaluated, enriched with additional data, related to risks and controls and reported.
An event has a lifecycle of six states:

1. The event is reported by a reporter and updates to status 'Awaiting Acceptance';
2. The Event Assessor assesses the event and then choose to reject the event **or** accept the event and update the event to the status 'Awaiting Improvements'. He/she can choose to add measures of improvement (MoI's) before updating the event to the next status.
4. The Event Responsible can add measures of improvement while the event is still in the 'Awaiting improvements' status. The Event Assessor or Responsible completes the event and sets the status to 'Ready for Approval'. However, this is only possible if the attached measures of improvement are completed;
5. The Event Assessor approves and closes the event **or** doesn't approve and set back to status 'Awaiting Improvements';
6. The event is completed and ready for reporting.

1.2. Data Breaches

In the Event module, users are also able to report Data breaches related to their organization. When a Data breach occurred, users can specify the type of breach, data, consequences and notifications to the authorities. Data Breaches follow the lifecycle of the Event it is attached to.

1.3. Email notifications

Throughout the lifecycle of the event, email notifications can be sent by the system to relevant people that are assigned to the event or data breach. These messages can be managed in standing data.

For the Event module, an additional notification option was created to make sure that some people or even departments were always notified of a new event/data breach. Two email addresses can be added under 'Settings' in the landing page (see picture below). One for events, one for Data Breaches. This option can be used for personal email addresses, but also for departmental email boxes where everyone can see the latest events that were reported.

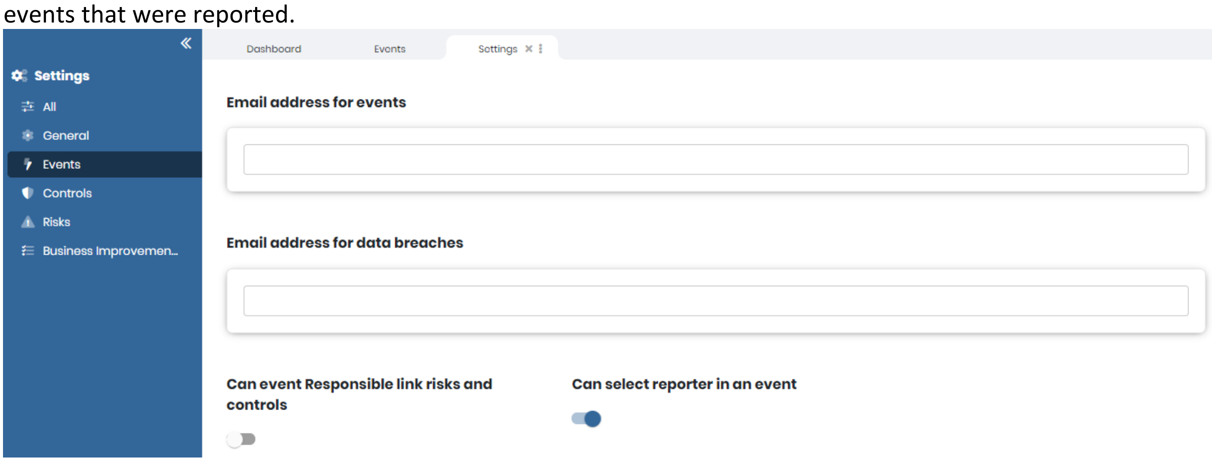


Figure 1: Event settings

2. User Roles

There are ten different types of users in the Event management module, represented by user roles. Each role has certain rights predefined, which allows the users to use specific parts of the module. These roles need to be assigned to the user. In order to give one user more rights, multiple roles can be selected.

Table 1: Roles and rights of Events

Event Roles	Event Unrestricted Administrator	Event Restricted Administrator	Event Assessor	Event Responsible	Event Reporter	Event Informed	Event Unrestricted Viewer	Data Breach Assessor	Data Breach Responsible	Data Protection Officer
Search for Events	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Operational										
Report new Events	✓	✓			✓					
Report Data Breach with Event	✓	✓	✓	✓						
Delete Events	✓	✓								
Restore deleted Events	✓	✓								
Accept/Reject Event	✓	✓	✓							
Set Event to Ready for approval	✓		✓	✓						
Approve&Close or not Approve Events	✓	✓	✓							
Reopen Approved&Closed Events	✓	✓								
Complete and adjust Event details	✓	✓	✓							
Complete and adjust Event details, except the 'Assessor' and 'Responsible'				✓						
Open Events in read-only state					✓	✓	✓	✓	✓	✓
Export Event details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Upload documents	✓	✓	✓	✓	✓					
Delete documents	✓	✓	✓*	✓*	✓*					
Access to Navigator - Business Dimensions	✓	✓								
Audit										
Report a new Event MoI	✓	✓	✓	✓						
Can be assigned as Auditor in Event MoIs	✓	✓	✓	✓						
Complete and adjust Event MoI details	✓	✓	✓	✓						
Confirm or decline Event MoIs	✓	✓								
Set Event MoI to status Ready for Acceptance	✓	✓	✓ ✓	✓						
Accept or Reject Event MoI	✓	✓	✓ ✓	✓						
Close and Reopen Event MoI	✓	✓	✓ ✓	✓						
Add comments and update progress	✓	✓								
Add comments without updating progress	✓	✓	✓ ✓	✓						
Upload documents	✓	✓	✓	✓	✓					
Delete documents	✓	✓	✓*	✓*	✓*					

Event Roles	Event Unrestricted Administrator	Event Restricted Administrator	Event Assessor	Event Responsible	Event Reporter	Event Informed	Event Unrestricted Viewer	Data Breach Assessor	Data Breach Responsible	Data Protection Officer
Data Breaches										
Complete and adjust Data Breach details	✓	✓	✓					✓		
Complete and adjust Data Breach details except 'Assessor', 'Responsible' and 'Notifications'									✓	
Export Event and Data Breach details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Settings										
Maintain Standing data	✓									
Modify mail messages	✓									

Legenda	
✓	Only when assigned to Event
✓	Events from own organization
✓	Events from every organization
✓*	Only documents they uploaded themselves

2.1. Event Unrestricted Administrator

The Event Unrestricted Administrator is the user who will set up and keep the complete overview of the Event module. Therefore, this role has rights to all functionality in this module. With this role it is possible to see all events in the module and edit them.

2.2. Event Restricted Administrator

The Event Restricted Administrator has the same rights as the Event Unrestricted Administrator except for maintaining the Standing data. Furthermore, the Event Restricted Administrator is restricted to his own organization.

2.3. Event Assessor

The Event Assessor has all write rights for assigned events or events from his own organization.

2.4. Event Responsible

The Event Responsible has all write rights, with the exception of appointing users for assigned events.

2.5. Event Reporter

Has the ability to report new events in CERRIX for every organization.

2.6. Event Informed

Can view all the events to which he/she is assigned.

2.7. Event Unrestricted Viewer

Can view all events in a read-only mode.

2.8. Event Restricted Viewer

Can view events in a read-only mode that are restricted to the own organization of the user.

2.9. Data Breach Assessor

The Data Breach Assessor has all write rights for assigned data breaches and data breach from his own organization. The event details from those data breaches can be viewed in read-only mode.

2.10. Data Breach Responsible

The Data Breach Responsible has all write rights for assigned data breaches, with the exception of appointing users, for assigned data breaches. The event details from those data breaches can be viewed in read-only mode.

2.11. Data Protection Officer

The Data Protection Officer can see all events with data breaches in a read-only mode.

3. Reporting an Event

To report a new Event the user has two options:

1) Create a new Event through the workspace.
2) Create a new Event through Forms.
    a. Creating an Event through Forms is explained in the Forms Manual. Please consult the Forms Manual for further instructions.

In order to add an Event, the standing data must be defined first. This will be explained in chapter 4.

3.1. Workspace

The workspace screen is a quick way to view which events are present in the database and in which state they are in. In the workspaces you must select the “Events” workspace (figure 2).

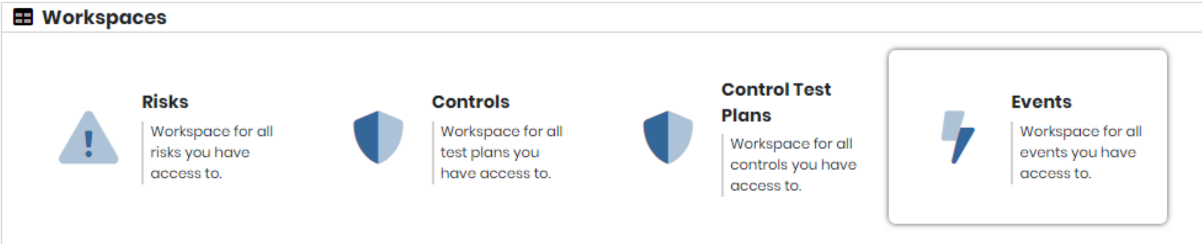
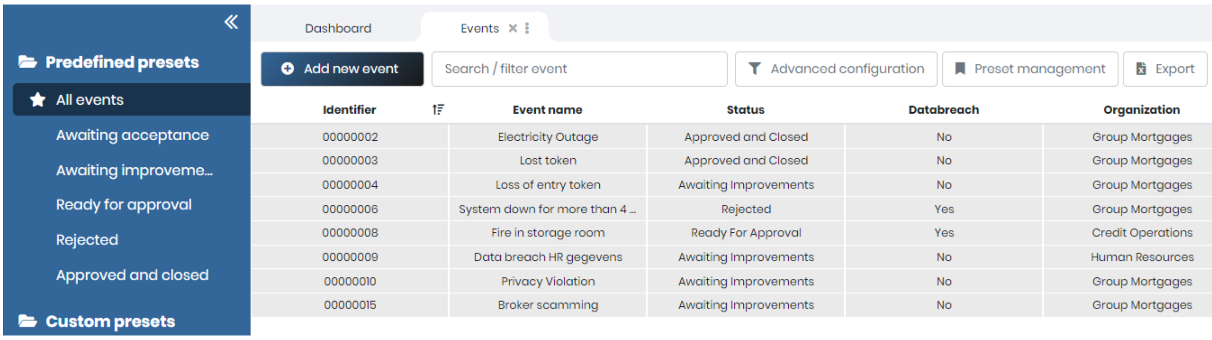


Figure 2: The way to access the Events workspace

When the Events Workspace is opened, the overview list provides the Event items and their status. An Event can be in the following filter groups: All events, awaiting acceptance, awaiting improvement, Ready for approval, Rejected and Closed. The user starts with ‘All Events’, all events that the user is allowed to see. The filter groups are shown in the side menu of figure 3 below. When choosing one of the other point of views, the list with events will change. You can sort order the columns by clicking on the header.



Identifier	Event name	Status	Databreach	Organization
00000002	Electricity Outage	Approved and Closed	No	Group Mortgages
00000003	Lost token	Approved and Closed	No	Group Mortgages
00000004	Loss of entry token	Awaiting Improvements	No	Group Mortgages
00000006	System down for more than 4 ...	Rejected	Yes	Group Mortgages
00000008	Fire in storage room	Ready For Approval	Yes	Credit Operations
00000009	Data breach HR gegevens	Awaiting Improvements	No	Human Resources
00000010	Privacy Violation	Awaiting Improvements	No	Group Mortgages
00000015	Broker scamming	Awaiting Improvements	No	Group Mortgages

Figure 3: Overview of the events workspace

To search for a specific Event, the search bar can be used. Filtering on specific information can be done with advanced configuration. Click on the button “**Advanced configuration**” to open the following overview:

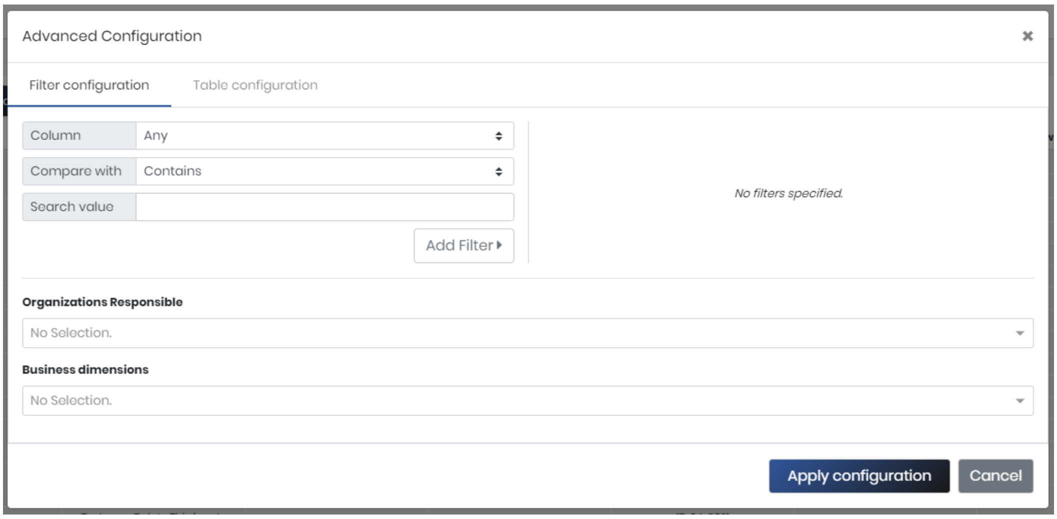


Figure 4: Advanced configuration

Advanced configuration makes filtering possible in a several ways:

1. You can filter on structures like Organization (Responsible) and Business Dimensions. These filter options are shown at the bottom of the Advanced Configuration screen (See figure 4 – Advanced configuration).
2. You can also filter on the value of specific columns.
    a. Click on the arrows right in the upper field (Figure 5) to choose a column to filter on.
    b. After selecting the column, you can determine the way to filter with the option “**Compare with**”.
    c. At last, you must add a search value. The search value can be different, depending on the column you are filtering on. The example below filters on the column “**classification**” compared with “**Contains**”. In this situation, the search value could be ‘medium, high or low’.
    d. Click on “**Add filter**” after filling in the search value you want to filter on.
    e. To apply the filter, you have to close the advanced configuration by clicking on the “**Apply configuration**” button.

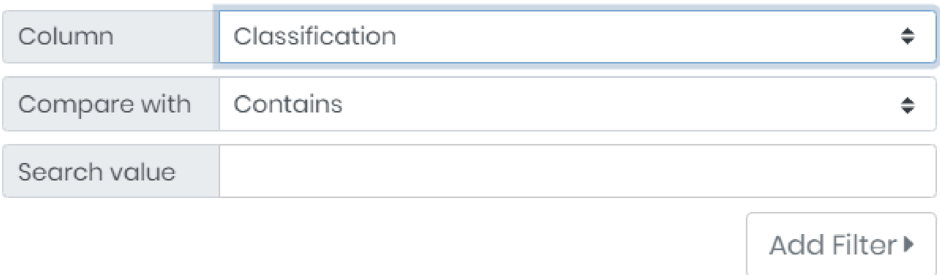


Figure 5: Filtering on column value

3. You can arrange the columns you want to see. Choose “Table configuration” at the top, after opening Advanced Configuration. Table configuration is possible by dragging a field type to the place you want to see it on your Workspace (see figure 6 below). It is also possible to hide a field by clicking on it, you can see the field change to ‘Hidden Headers’. When you have the right order of active columns click on ‘Apply configuration’. This way, the Events workspace will change to your preferences.

Figure 6: Table configuration

4. After arranging the workspace to your preferences, it is possible to save the configuration as a preset. This way, a personal configuration can be saved after customizing the workspace via advanced configuration.
    a. Use advanced configuration to arrange the workspace to your preferences.
       Click on “Preset Management”.

3.2. Creating an Event

After defining the standing data, the Event can be reported or added. This can be done by the Event (Un)Restricted Administrators and Event Reporters, who can create new events via the Events workspace. By clicking on the **"Add new event"**-button (see figure 7), an empty event detail screen is opened (see figure 8).

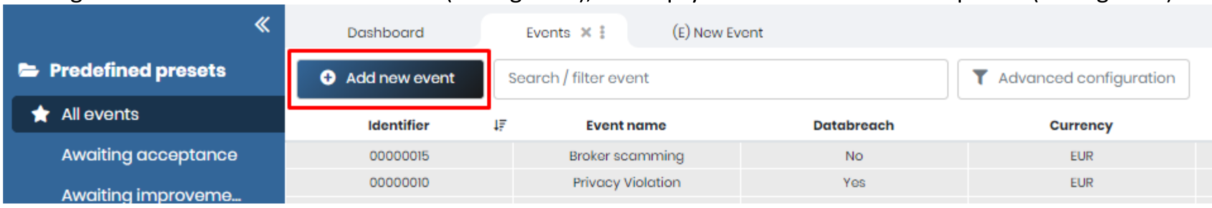


Figure 7: Adding a new Event

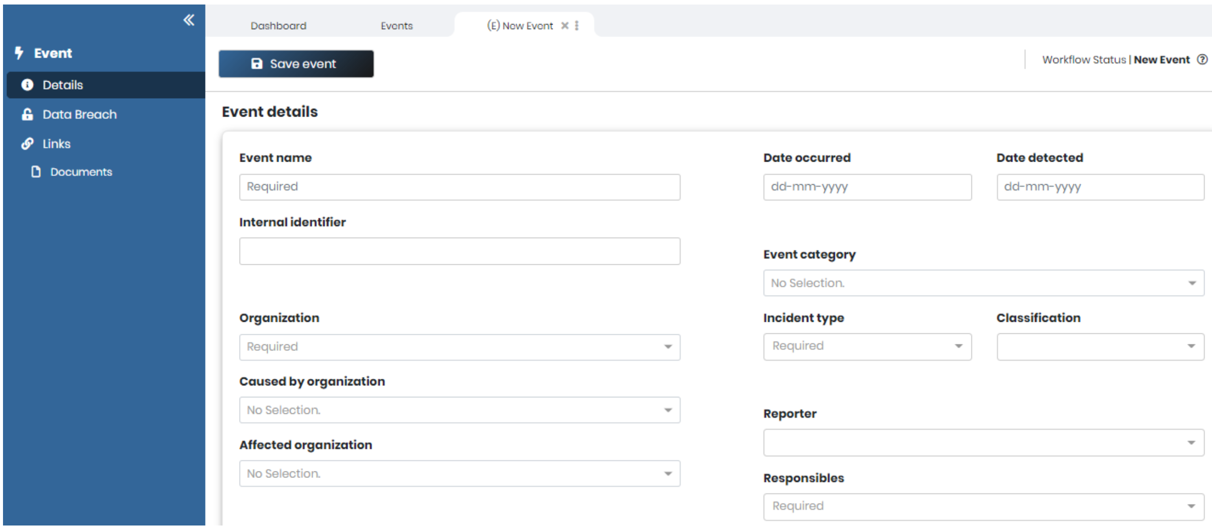


Figure 8: Event details screen

The details screen of Events consists of the following fields:

Comments

- Comment: The comment field is required to fill when changing the status of the event. The comments are shown at the top of the Event details screen. The field can only be filled when changing the status (not when adding a new event). The type (status), user and date are shown after the comment is added.

Event details

- **Event Name:** A short name for the event. This field is **required**.
- **Internal Identifier:** An optional ID for the event, that is editable by users. This can be used for Events that were already registered with an ID before documenting them in CERRIX.
- **Organization:** Select the organization for the event. This field is **required.**
- **Caused by Organization:** The organization that caused the event.
- **Affected Organization:** The (second) organization affected by the event.
- **Business dimensions:** The Business dimensions that are applicable to this event can be selected.
- **Business line:** The business line that is applicable to the event.
- **Event category:** The category in which the event occurred.
- **Incident type:** The type of incident that occurred. This field is **required.**
- **Classification:** How can this event be classified.
- **Date Occurred:** Date that the event occurred. This field is **required.**
- **Date Detected:** Date the event was detected. This field is **required.**

- **Reporter:** The user who reported the event. This field is **filled automatically.**
- **Responsible:** The user that is responsible for filling in the event details. This field is **required.**
- **Assessors:** The assessor of the event. This field is **required.**
- **Informed:** The user that needs to be informed about the events but does not have any responsibility within.
- **Event Description:** A short description of the event. This field is **required.**
- **Impact Description:** A short description of the impact that the event has.
- **Cause Description:** A description of the cause of the event.
- **Primary Cause:** The primary cause of the event. This field is **required.**
- **Secondary Cause:** A second cause for the event.
- **Effects:** What is/are the effect(s) of the event on the organization.
- **Effects Description:** A short description of the selected effect(s) on the organization.
- **Gross Impact:** The gross costs of the event for the organization.
- **Recovery:** Deducted from the gross impact. What was saved that previously was considered a cost.
- **Net Impact:** The remain costs after the recovery is deducted from the gross costs. **This field is filled automatically.**
- **Currency:** The currency in which the costs are measured.
- **Reputation Impact:** The impact of the event on the organizations targets, strategic planning and/or reputation.
- **Reputation Impact Description:** A description of the previously chosen impact scale.
- **Risk Opinion:** The comment from the risk manager.
- **Comments:** Comment by the user(s) responsible for the event (This field differs from the comment field at the top of the page and can be added and edited at each moment).

When the user is done filling in the fields in the event details screen, the event needs to be saved. This can be done using the "**Save**"-button in the top left (figure 8).

Apart from the fields described above, there is also an automatically generated field with the important event information (figure 9 below). This field is generated and updated after the event is being saved. The **ID**, **Registration date** and **Date closed** are unique and can't be edited by changing the event details.

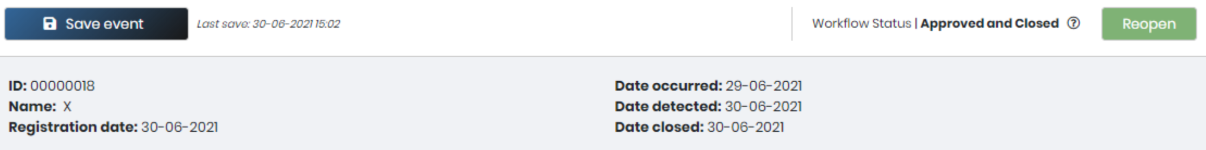


Figure 9: Automatically generated event information

3.3. Report a Data Breach

If the event led to a Data Breach, reporters can click on the tab “Data Breach” in the side menu (figure 10). By clicking on the tab, the Data Breach screen opens. A checkbox “**Is data breach**” is shown. The details become available by clicking on the checkbox.

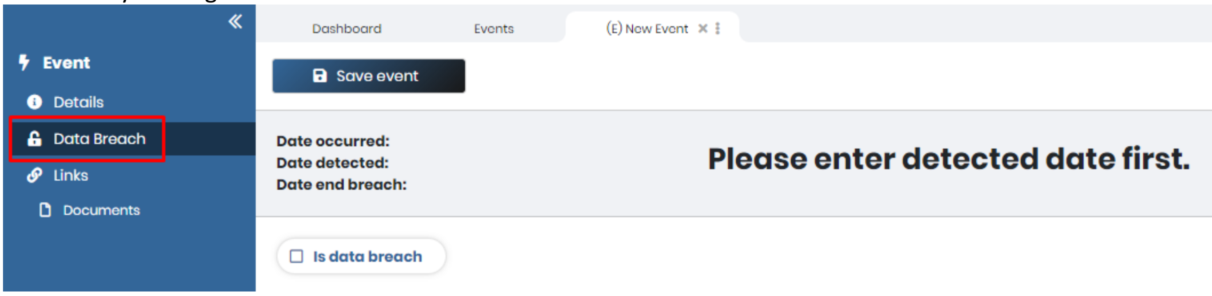


Figure 10: Data Breach

The Data Breach details screen consists of the following fields:

Data Breach details

- **Internal Breach Identifier:** An optional ID for the Data Breach, that is editable by users. This can be used for Data Breaches that were already registered with an ID before documenting them in CERRIX.
- **External Breach Identifier:** Authorities will provide their own ID numbers. These can be added in this field.
- **Organization:** The organization where the data breach occurred. This field is **required.**
- **Data Breach Responsible(s):** The user that is responsible for filling in the data breach details. This field is **required.**
- **Data Breach Assessor(s):** The assessor of the data breach details.
- **Data Protection Officer:** The Data Protection Officer from the organization.
- **Data Breach Occurred:** The date the data breach occurred. This field is **required.**
- **Data Breach Detected:** The date and timestamp the data breach was detected in the organization. This field is **required.**
- **Date End of Breach:** Th date the data breach has ended.

Breach Analysis

- **Nature of breach:** A field to select the nature of the Data that has been breached.
- **Nature of incident:** The nature of the incident that caused the breach.
- **Description of Breach:** A description of the data breach. This field is **required.**
- **Type(s) of Breach:** Select the type(s) of data breaches.
- **Cause of Breach:** A cause for the data breach must be given. This field is **required.**
- **Personal Data:** Select the personal data that was leaked. This field is **required.**
- **Special Categories of Personal Data:** Select the special categories of which data was leaked.
- **Name Data Processor:** Who was the data processor of the data that was leaked.
- **Outsourced Data Processing:** Checkbox, set to ‘TRUE’ if the data was sent to a third party to be processed.
- **Sub-Data Processor:** Checkbox, set to ‘TRUE’ if there was another data processor with more responsibility.

- **Preventative Measures:** Which measures were taken to prevent this data breach from happening.
- **Consequences to CIA of Data:** The consequences of the breach to the Availability, Integrity and/or Confidentially of the data.
- **Consequences of Personal Data Breach:** Select the consequences of the leaked personal data.
- **Person(s) Involved:** Select one or more group(s) of persons involved in this data breach.
- **Description Persons Involved:** A description of the persons involved can be given here.
- **# Data Registers Involved:** Enter the number of data registers that are involved. Databases, Datasets and Data entities are some examples.
- **Minimum # of Persons Involved:** The minimum number of persons that are involved with this data breach.
- **Maximum # of Persons Involved:** The maximum number of persons that are involved with this data breach.
- **Persons in other EU-countries Involved:** Checkbox, set to 'TRUE' if there are other persons from other countries from the European Union are involved.

Notifications

- **Authorities Notified:** Checkbox, set to 'TRUE' if the national authorities have been notified.
    - **Date Authorities Notified** becomes available when **Authorities Notified** is set to 'TRUE'. Users can fill in the date and time they notified their authorities.
- **International Authorities Notified:** Checkbox, set to 'TRUE' if the international authorities have been notified.
    - **Name of International Authorities** becomes available when **International Authorities Notified** is set to 'TRUE'. Users can fill in the name of the international authorities they notified.
- **Which EU Country:** The country from the international authorities that were notified for this data breach.
- **Cross-border Processing:** Checkbox, set to 'TRUE' if the data controller or processor are from to different states.
- **Notification to Persons Involved:** Checkbox, set to 'TRUE' if persons affected by breach are notified.
    - **Date Persons Involved Notified** becomes available when **Notification to Persons Involved** is set to 'TRUE'. The date that they were notified can be registered here.
    - **Description Notification Persons Involved** becomes available when **Notification to Persons Involved** is set to 'TRUE'**.** A description of the notification sends to the persons involved can be given here.
    - **Means of Communication:** Which communication method was used to notify other persons.
    - **# of Persons Notified:** The number of persons notified for this data breach.
- **Reason no Notification:** A field to select the reason why not all the involved persons are notified.
- **Explanation no Notification:** Stays active when **Notification to Persons Involved** is 'FALSE'. In this field you can give a textual explanation of why the persons involved were not notified.
- **Secondary Notification:** A checkbox to select when a second notification to affected persons by this data breach is sent.
    - **Date of Notification** becomes available when **Secondary Notification** is set to 'TRUE'. The date that the second group of involved persons was notified.
    - **Description Notification Persons Involved** becomes available when **Secondary Notification** is set to 'TRUE'. A description of the notification send can be registered here.

Contact Details

- **Chamber of Commerce Registration nr.:** The Chamber of Commerce number from an involved organization in the data breach.
- **Name of the Organization:** The name of the involved organization.
- **Address:** The address of the involved organization.
- **Zip Code:** The zip code of the involved organization.
- **City:** The city in which the involved organization is located.
- **Active in Which Sector:** The sector in which the involved organization is active.

Additional Information

- **Follow-up Description:** A field for Event Responsible or Event Assessor to leave some additional information about the data breach.
- **Comments:** A field for the Event Responsible or Event Assessor to leave a comment for other users that can open the event.

3.4. Link Measures of Improvement

Users can add Event MoIs to the events with the '**Measures of improvement'**-tab. To add a new Event MoI to the event, users need to click on the "**Add MoI**"-button (figure 11).

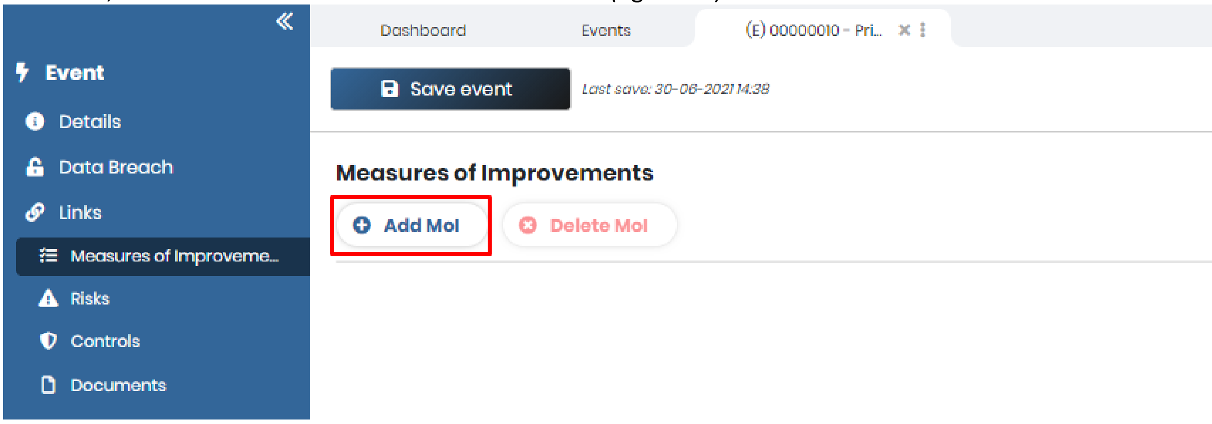


Figure 11: Adding a MoI to an Event

When clicking on the "Add MoI"-button, the regular MoI screen appears. For further MoI instructions please consult the BIM Manual. To delete linked MoI's, click on the MoI you want to delete to select it. After that, click on the "Delete MoI"-button.

3.5. **Link Risks and controls**

Under ‘Links’ in the side menu, it is possible for the user to link Risks and Controls to the event (see “A” in figure 12).

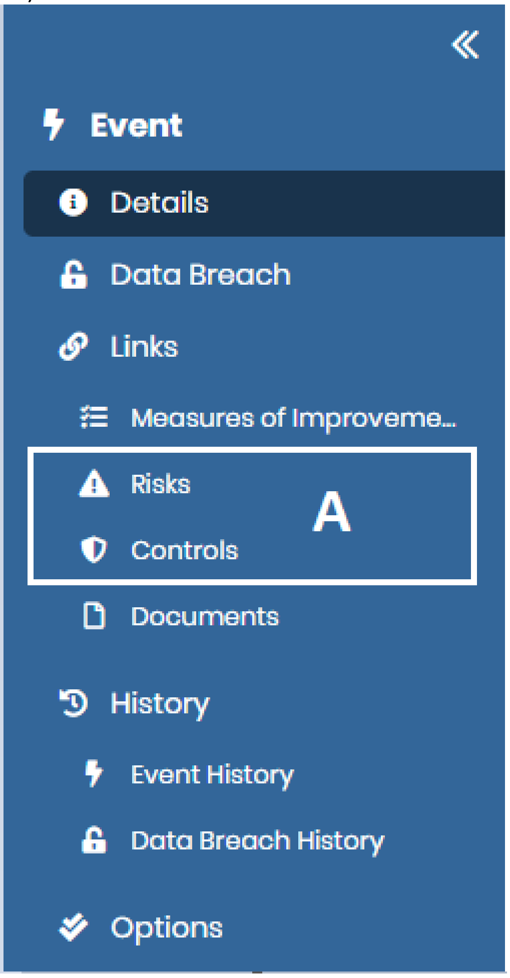


Figure 12: Link risks and controls

The Linked Risks screen is divided into two parts, Linked Risks(see "A" figure 13) and Linkable Risks(see "B" figure 15). The Risks that are shown in "Linkable Risks" depends on two variables.
It depends on the status of the event and what rights the user has in the Risk module.

1. Risks can only be linked in the status:
   - Awaiting acceptance
   - Awaiting improvements
2. And Risks can only be linked if the Event user has also a Risk (un)restricted Admin or Writer role.

To help the user find the correct Risk with the search field (see "C" figure 13). If there more Linkable Risks, please navigate through all pages with Risks (see "D" figure 13). To link a Risk, the user can drag and drop a Risk from the Linkable risks to Linked risks. You can also press on the arrow of a risk link it (see "E" figure 13). T

Figure 13: Link Risks to the event

To edit linked Risks, click on the ‘edit’ button for all linked Risks (see “F” figure 13). This is also possible per risk. When editing a Risk, the user can select the failure type and give a comments why this risk is applied to this Event (see figure 14).

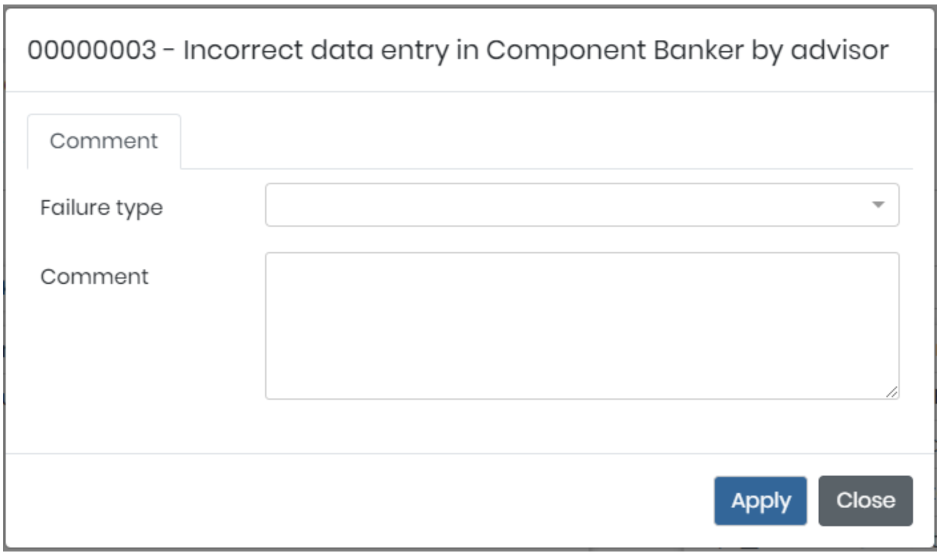


Figure 14: Risk Failure Types

Controls can also be linked to the Event. This works the same as for linked risks. Go to “Links” and then select “Controls”. Searching and linking controls works the same as for Risks.

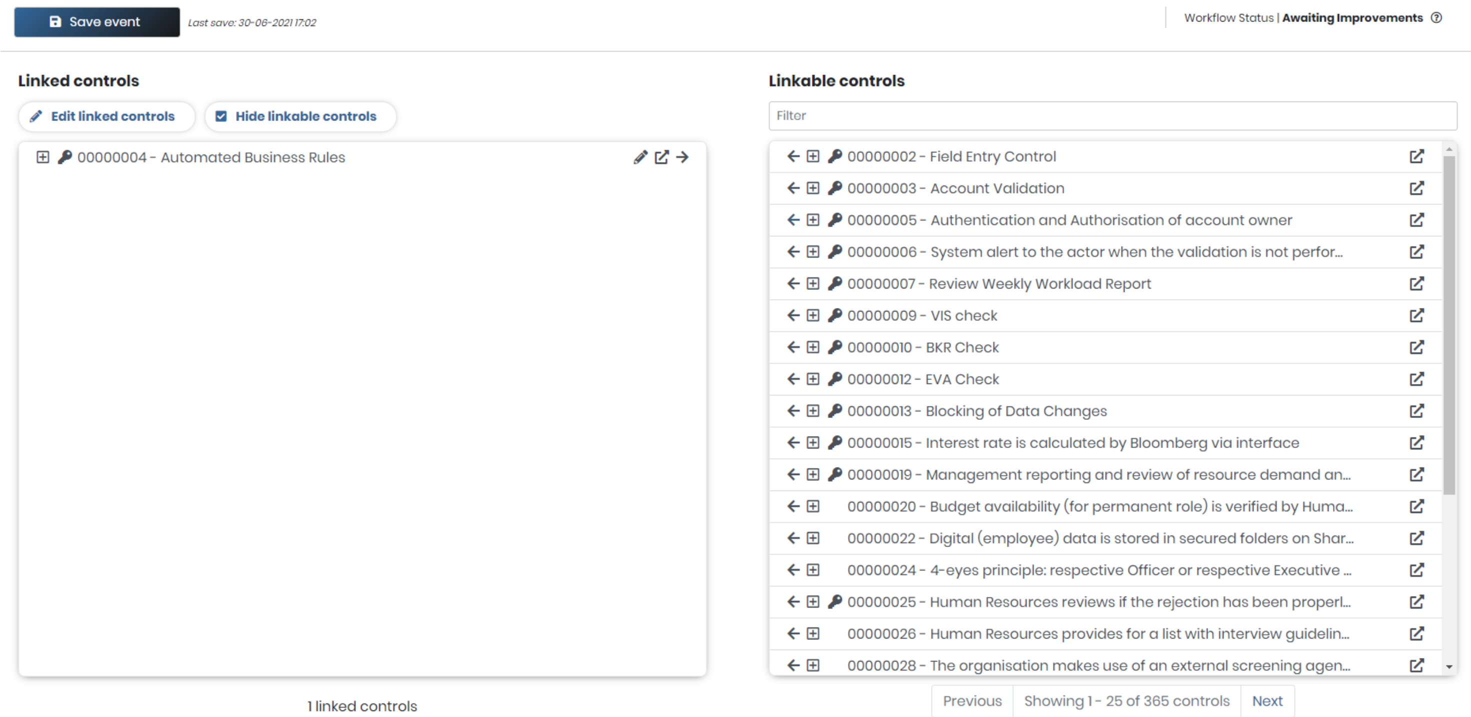


Figure 15: link Controls to the event

4. Defining the standing data

Standing data is used when filling in the details. For Events, all standing data for ‘Events’ must be filled in. First open Standing Data (see “Standing Data” in figure 16).

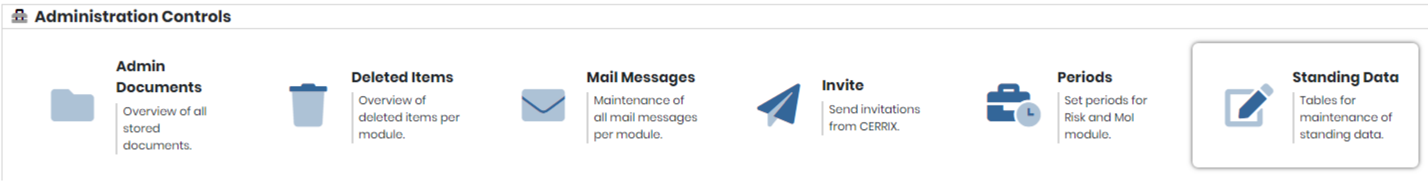


Figure 16: Standing Data

The standing data for consists of 7 fields for Events and 10 for data breaches. These are all available under the Events branche (see figure 17).

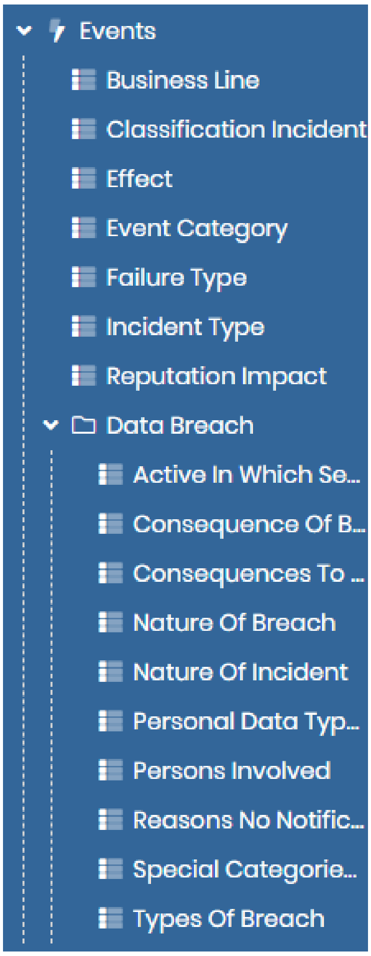


Figure 17: Events Standing Data

Maintaining Standing Data Fields

In the side menu is shown that the Standing Data of the field "**Business Line**" is currently opened. The overview screen gives the option to add a business line. This can be done by clicking on the "**Add**"-button (figure 18). After adding the business line, you must fill in a name and abbreviation in order to save it. You can delete a business line if it is not in use in any event. Editing a business line can be done by clicking on the business line in the menu, changing the name and/or abbreviation, and clicking on save.

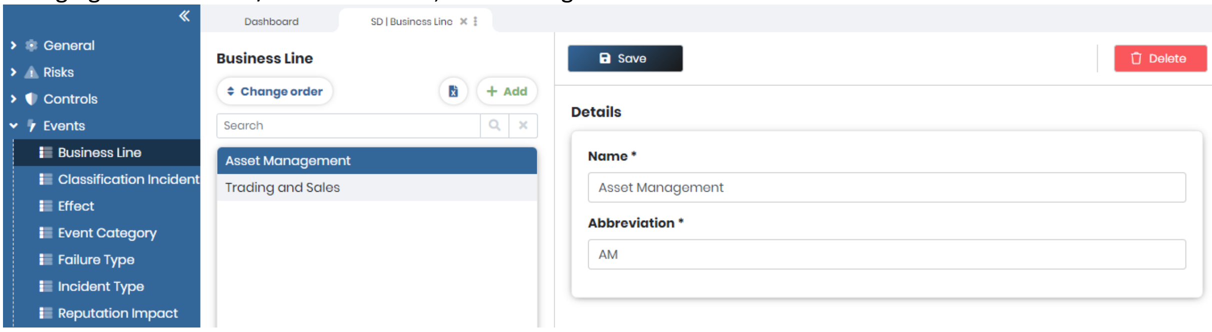


Figure 18: Business Line

Apart from adding editing and deleting, it is also possible to export the business lines. This can be done by clicking on the **File**-button left from the "**Add**"-button. The export generates an excel file. You can also change the order in which the Business lines are shown. This can be done by clicking on "**Change order**", dragging the business lines in a new order and clicking on save.

When one of the standing data items is opened, the following actions are possible:

1. **Add new:** Click on the "Add" icon, a menu opens where a name can be given. Depending on the kind of data, a color and value can also be given.
2. **Edit:** To edit data, click on the title of the data that you want to edit and click on save after changing the data.
3. **Change order:** To change the order of the standing data, click on "Change order" and click on "Complete order" after sorting the order to the new preferences.
4. **Export data:** Click on the excel-file icon to make an export per standing data item. Depending on the kind of data, the color code and value are also exported.

In the example below is shown how to maintain one of the Standing Data fields.

Event Category

The field "Event category" is also integrated in the risk module. This means that changes to this field also affect the field in the risk module.