**GUIDE**

# DORA – Incident reporting

FINANSINSPEKTIONEN

**14/10/2026**

Version 1.3

# CONTENT


Requirements 3

Submit an incident 4

- Flowchart 5
- Initial notification 6
- Affected entities 7
- Save and submit the report 7
- Intermediate report 9
- Final report 11

Revise an incident 13

- Flowchart for revising a report 15

Reclassify or revoke an incident 16

- Reclassification 16
- Revocation 16

Report Significant Cyber Threats 17

- Resume the report 17

Other information 18

- Sheet descriptions 18
- Date and time 18
- Filter by a Reference code 19

# Requirements

A person who is going to submit incident reports and reports of significant cyber threats needs to register an account in the Reporting Portal and have authorisation delegated to their account from a registered signatory of the company.

Please see the guides for the Reporting Portal for more information.

The authorisation ”DORA incident och cyberhot” is delegated to the user, for the company that is submitting the report (*submitting entity*). If there are any other companies affected by the incident (*affected entity*), no authorisation is necessary, only for the submitting company. However, affected companies should be entered into fields 1.4, 1.5 and 1.6. For more information about aggregating reporting of affected companies, please see page 7.

Submitting a report also requires access to the inbox for the email address entered in the contact form. This is to have access to the email notification containing important information, automatically sent from FIDAC.

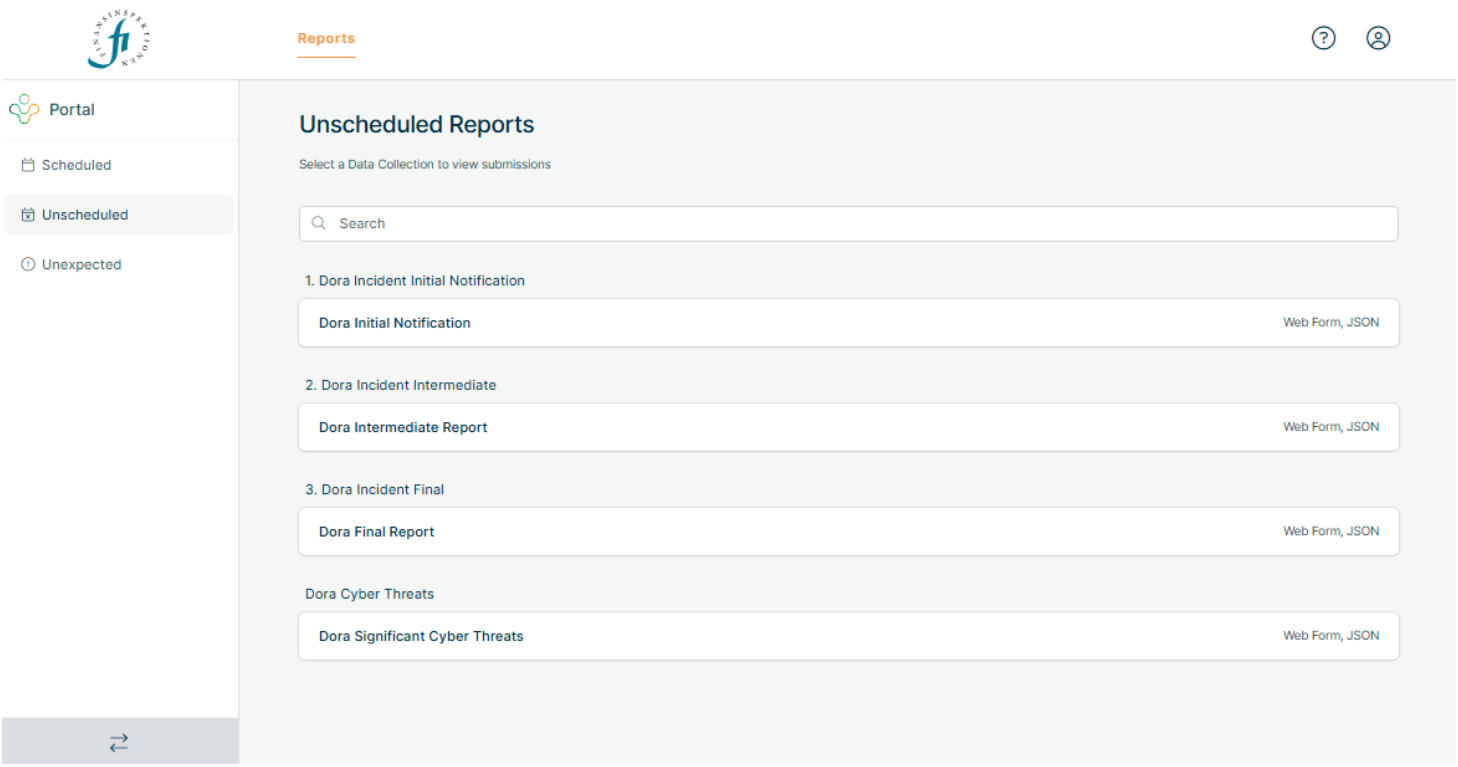
Please see the guide for FIDAC for more information.

# Submit an incident

The incident report according to the DORA directive is divided in three separate reporting modules in FIDAC:

- **Dora_initial**
  The module should be submitted as soon as possible but within 4 hours after the incident has been classified as major, and 24 hours at the latest after the company was made aware of the incident.
- **Dora_intermediate**
  The module should be submitted within 72 hours after the initial report was submitted.
- **Dora_final**
  The module should be submitted within one month after the intermediate report was submitted.

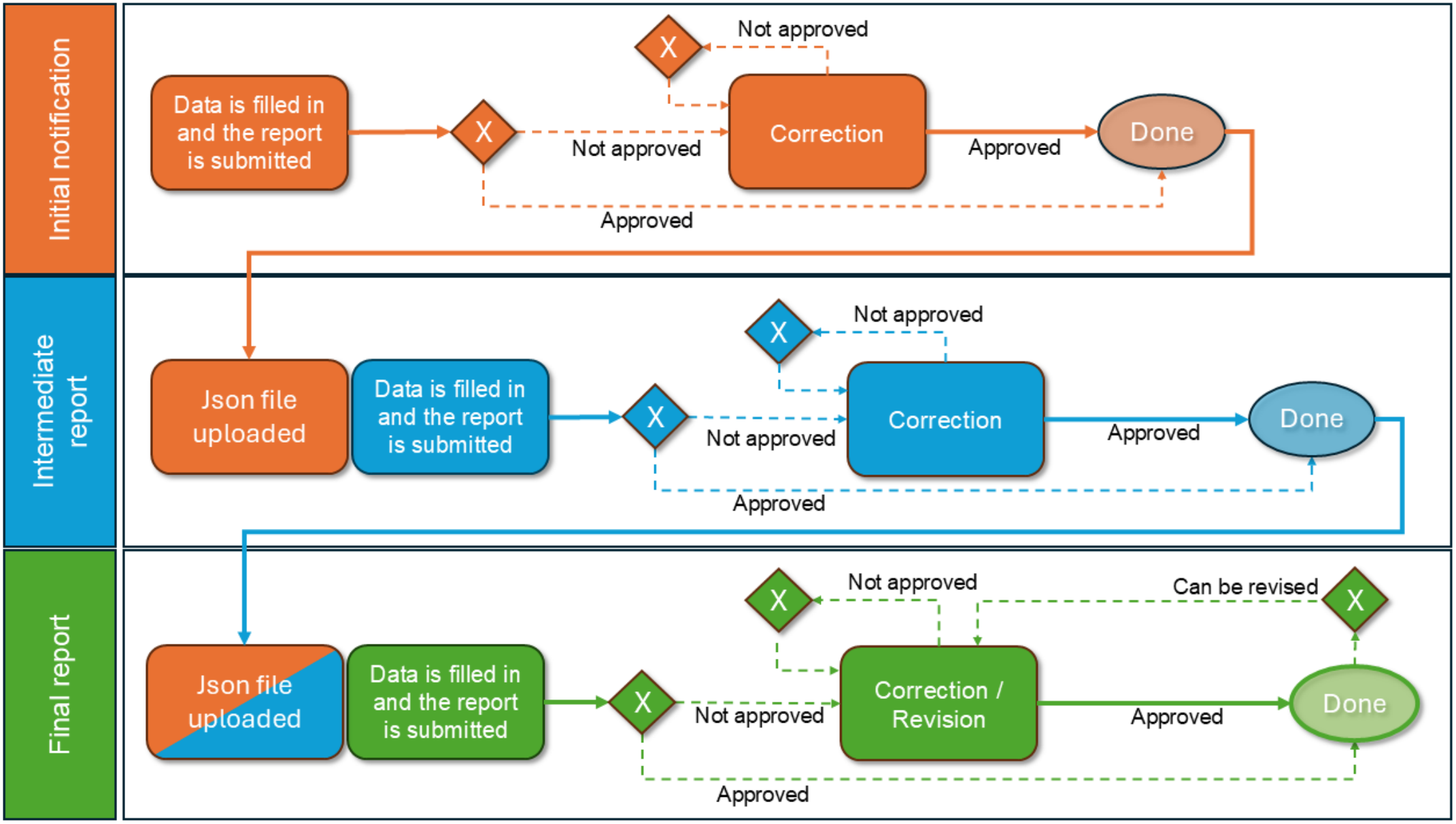
The reporting modules are divided, named and numbered via *Unscheduled* in the menu in FIDAC, like the below screenshot.




To submit a new incident report, select *1. Dora Incident Initial Report* and then *Add New Report* in the top right corner. A form will then open.

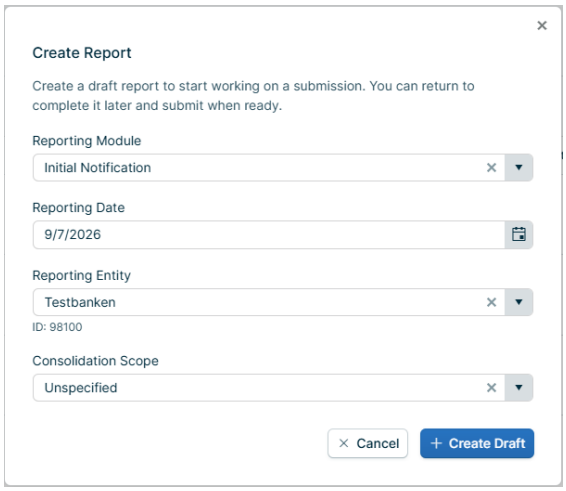
Please see the flowchart on the next page, illustrating reporting of all three incident modules.

## FLOWCHART


Initial notification
Data is filled in and the report is submitted
X
Not approved
Correction
Approved
Done
Not approved
Approved
Intermediate report
Json file uploaded
Data is filled in and the report is submitted
X
Not approved
Correction
Approved
Done
Not approved
Approved
Final report
Json file uploaded
Data is filled in and the report is submitted
X
Not approved
Correction / Revision
Approved
Done
Not approved
Can be revised
Approved

## INITIAL NOTIFICATION

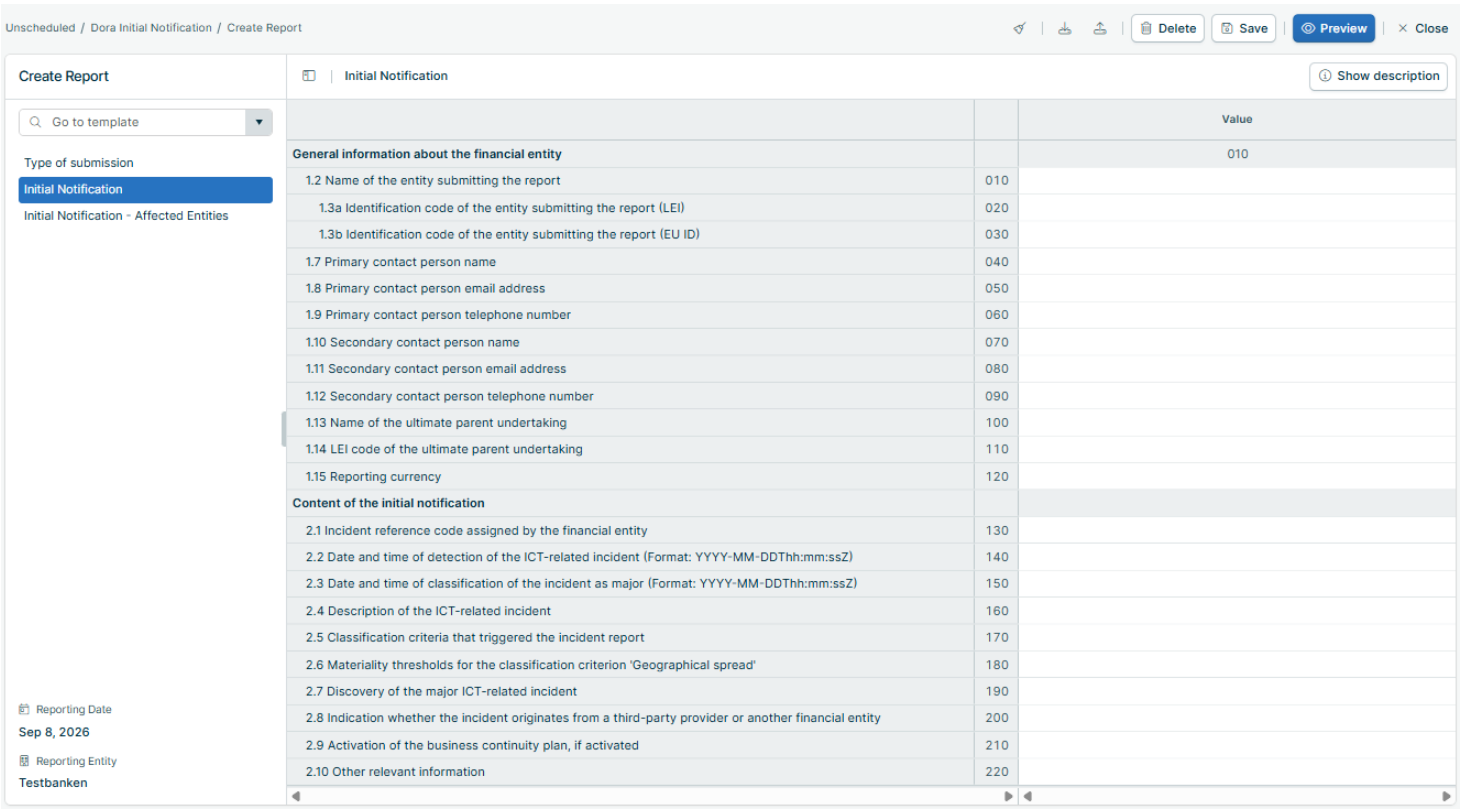
Select *DORA - Initial notification*, click Add *New Report* to start a report. Enter the date of the incident and select the entity that will submit the report. The entities displayed are determined by the user's permissions in the Reporting Portal.




Click *Create Draft* to open the form, start by by clicking *Type of submission* and select *initial_notification*. *Major_incident_reclassified_as_non-major* is only selected after the initial notification has been submitted and if the incident is no longer classified as major.

| | 1.1 Type of submission |
|---|---|
| | 010 |
| 010 | |

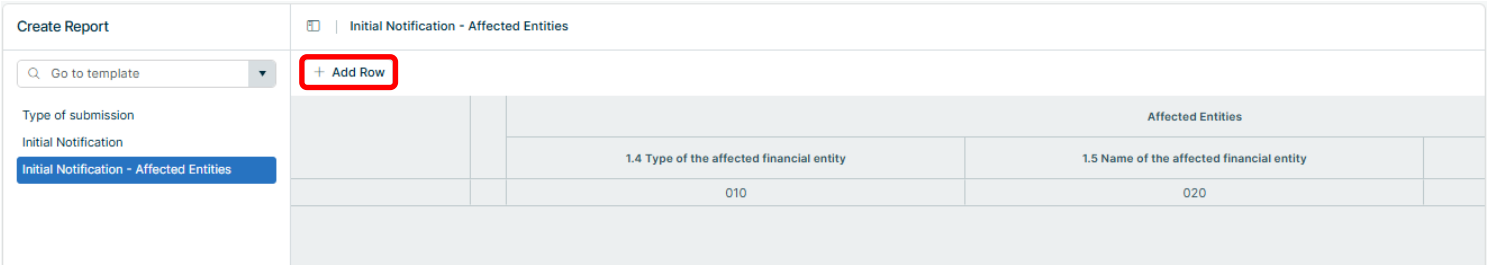
Continue by selecting *Dora Initial notification* in the menu.



## AFFECTED ENTITIES

Rows must be added manually in this tab.

Aggregated reporting is used when a single report is submitted for several financial entities affected by the same incident.
Add one row for each financial entity covered by the aggregated report.




At least one row must be provided. For the reporting entity, specify the type of financial entity (1.4) and LEI code (1.6). If other financial entities are covered by the report, specify the type (1.4), name (1.5), and LEI code (1.6) for each entity.




## SAVE AND SUBMIT THE REPORT

The report can be saved as a draft and resumed at a later time. Click *Save* to save the draft, the close the form. Click the *Draft* tab, then click *Continue* to resume the report.

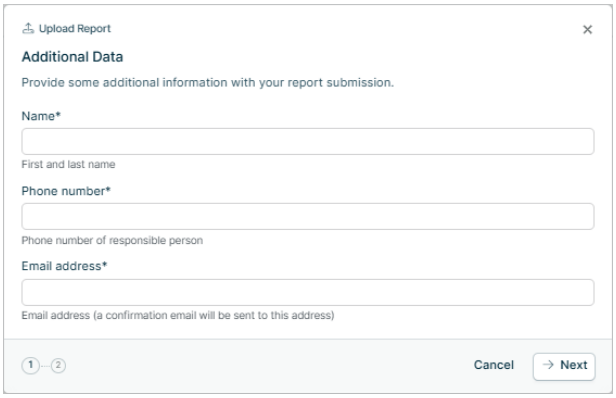
Once the report is completed, click symbol for *Download* to save the report as a JSON file which will be reused for the next reporting module.




Finish by clicking *Preview* in the top right corner. If something is missing or has been incorrectly entered according to the schema validation, those fields will be marked in red. Correct any errors, click *Preview* again and then *Submit*.

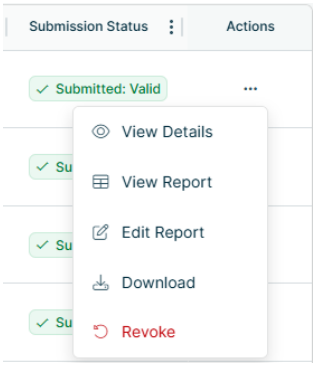



Enter the contact information and submit the report. The entered email address will receive an email notification which contain information about the report and a unique reference code.




It is also possible to download the JSON file in the next step. It is recommended to review the contact information.

The JSON file can also be downloaded via the option available in the *Actions* column to the far right of the submission row:




**Email notification**
When the report has been submitted, an email notification will automatically be sent from FIDAC, to the email address entered in the contact form. The email contains information about the report that was approved or encountered any validation errors, and details about the submission.

The details of the report are shown in the example below.
It is important to save the reference code, marked in bold:

**Details about the submission:**

- Financial entity ID: 98100
- Financial entity name: Testbanken
- Data collection: 1. Dora Incident Initial Report
- Module version: dora_initial_v1
- Submission ID: 2026-0427-dc73-de58
- Reporting date: April 27, 2026
- Submission timestamp: April 27, 2026 08:37:40
- **Reference code: CAFIX0427dc73de58**

The reference code is used in the next two reporting modules, to keep the reports (Initial, Intermediate and Final) together. When the reference code is used in the Intermediate and Final reports, the same code will be included in the email notifications for those reports. In addition, the reference code is also included in the subject line of the email.

## INTERMEDIATE REPORT

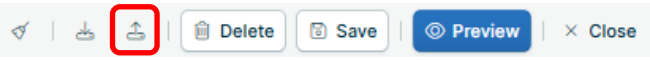
Then select *DORA - Intermediate Report* och click *Add New Report* to open the form. Click *Upload* in the form and select the JSON file you previously downloaded. To utilize the upload functionality with the information from the initial report in the intermediate report, you need to upload the JSON file before you start filling in subsequent parts of the intermediate report.

Before uploading the file, open it in a text editor and update the reporting date (if necessary). The “schemaRef” also needs to be changed from:

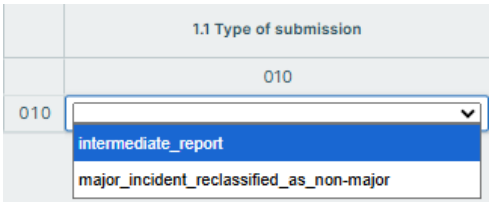
https://schemas.fi.se/esma/dora/v2/dora_**initial**_schema.json

To:

https://schemas.fi.se/esma/dora/v2/dora_**intermediate**_schema.json




The form is automatically filled with the data from the Initial notification, including the selected company. Before you start entering data, you must change the value for field *Type of submission*, from *initial_notification* to *intermediate_report*:

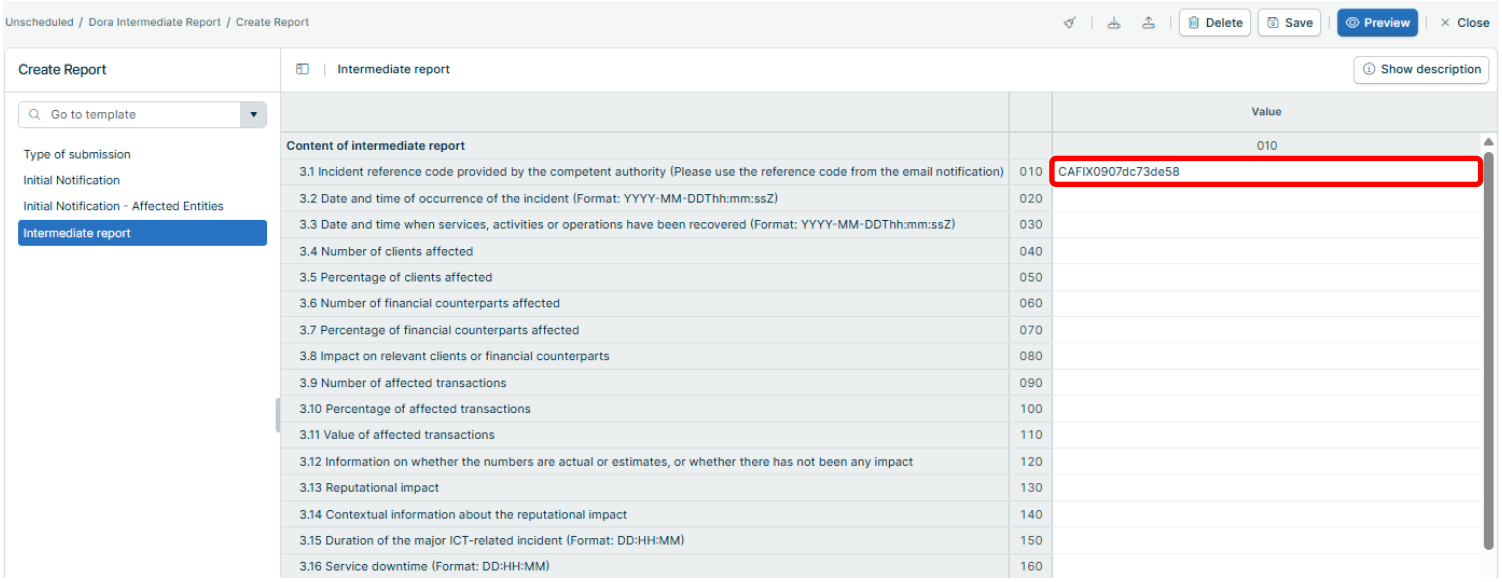



Select *Dora Initial notification*, the data from that submission will be available. If any data needs to be amended, go ahead and do so here.



**The reference code**

Select *DORA - Intermediate report* to coninue the reporting. It is important that the reference code, from the email notification, is entered in field 3.1:




A validation rule will check to make sure that the entered reference code corresponds to the previous submission Initial notification. The validation rule will be triggered after the Intermediate report has been submitted, if the entered reference code is not correct. If that happens, please make sure that the correct reference code has been entered and that there is no space included in the field.

Complete the rest of the fields for the Intermediate report, click *Preview* and then submit the report.

## FINAL REPORT

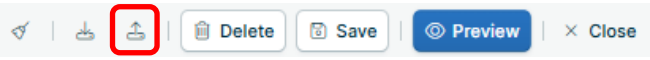
Select the *DORA - Final report* och click *Add New Report* to open the form. Click *Upload* in the form and select the previously downloaded JSON file from the Intermediate report.

Before uploading the file, open it in a text editor and update the reporting date (if necessary). The “schemaRef” also needs to be changed from:

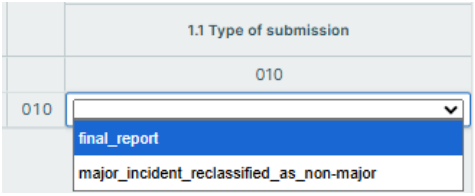
https://schemas.fi.se/esma/dora/v2/dora_**intermediate**_schema.json

to:

https://schemas.fi.se/esma/dora/v2/dora_**final**_schema.json




The form is automatically filled with the data from the Initial notification and Intermediate report, including the selected company. Before you start entering data, you must change the value for field 1.1. *Type of submission*, from *intermediate_report* to *final_report*:




If you select *Dora Initial report* or *Dora Intermediate report*, the data from those submissions will be available. If any data needs to be amended, go ahead and do so here.

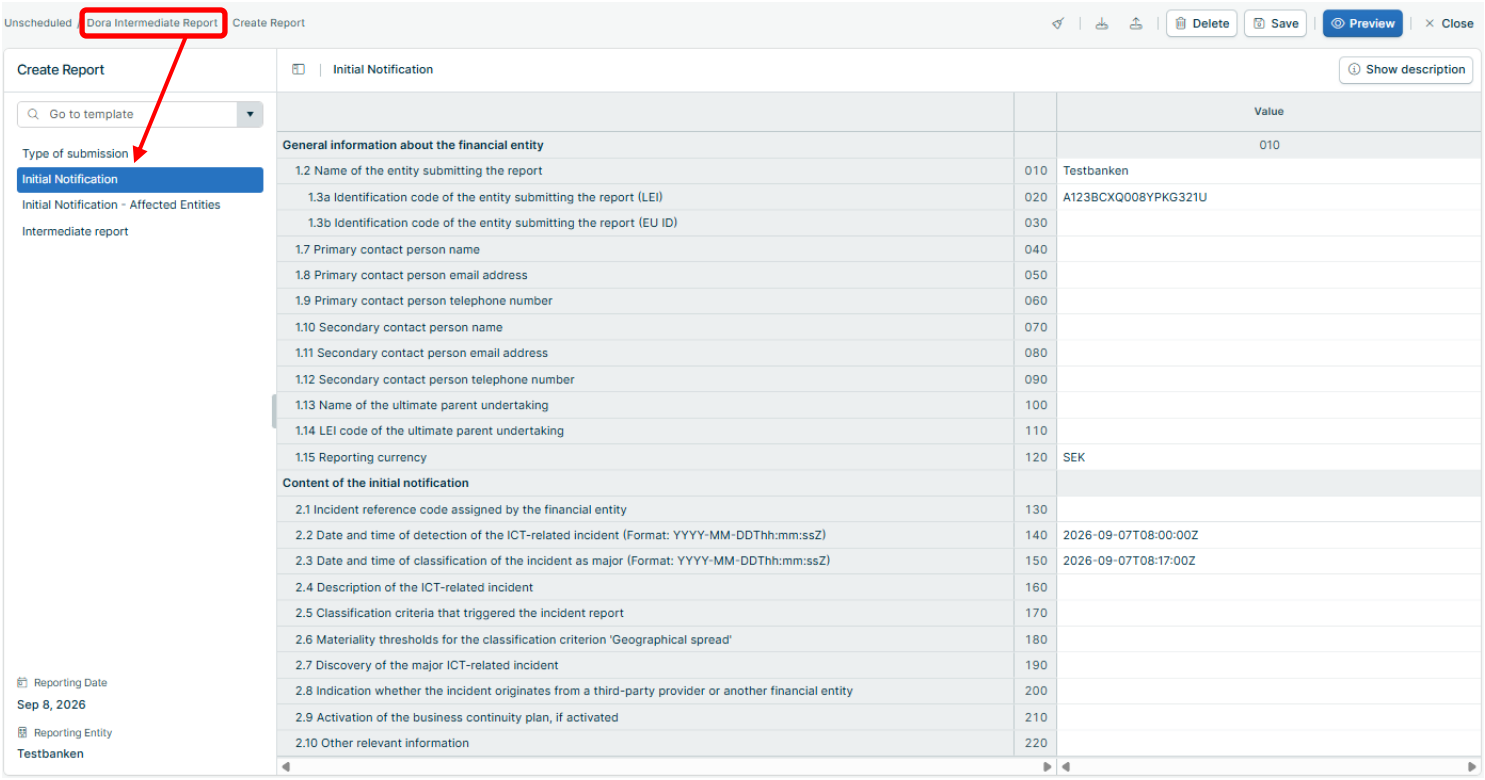


Complete the rest of the fields for the *Dora Final report*, click *Preview* and then submit the report.



# Revise an incident

The procedure to revise an incident report is somewhat different than for other reports in FIDAC. If there is need to revise an Initial report, then it must be done when submitting the Intermediate report, in sheet *Initial report*.




In the same way, if the Intermediate report must be revised, it is done when submitting the Final report, in sheet *Intermediate report*.

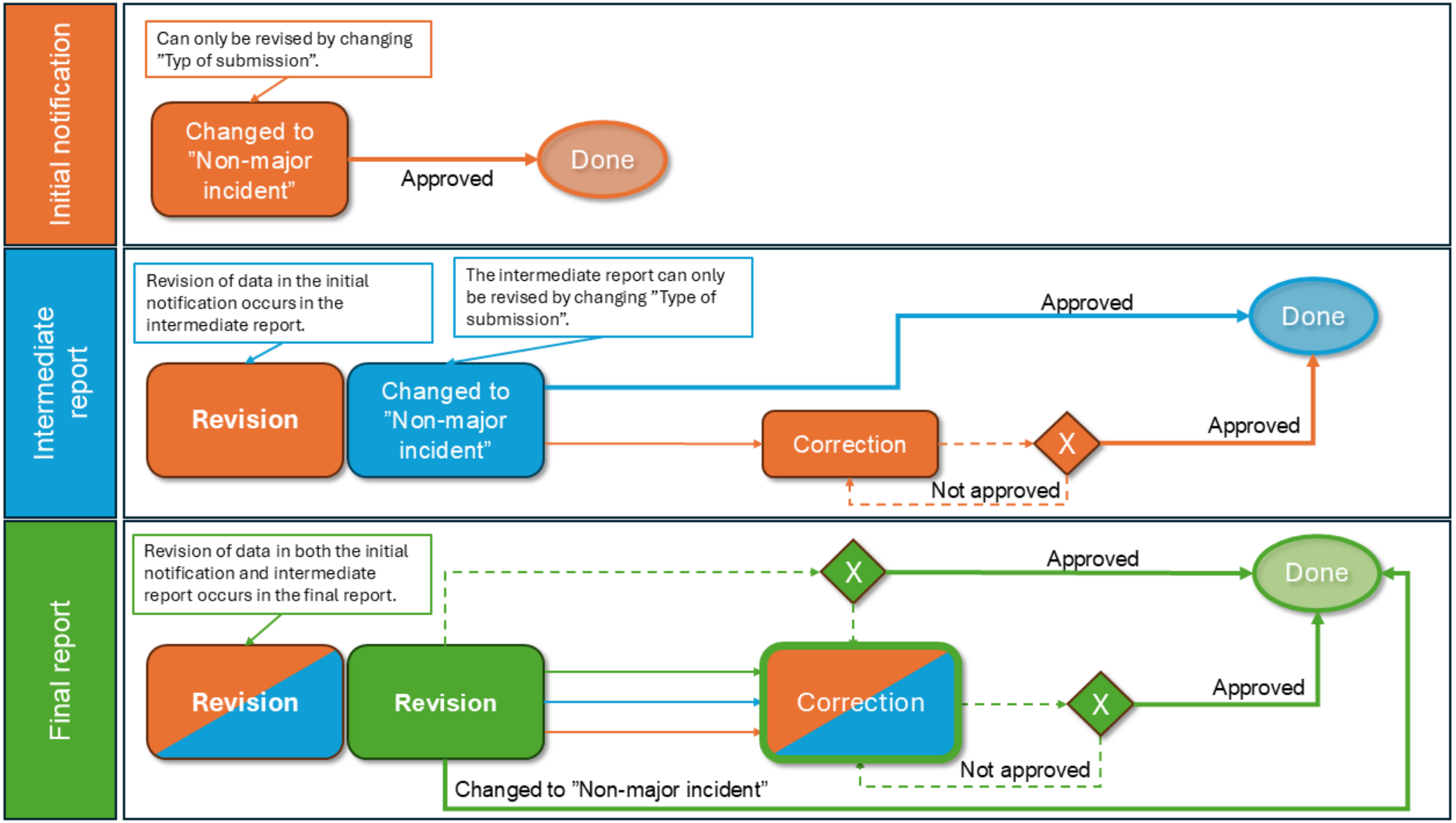



The Final report can be revised without limitation.

There is however the possibility to revise both the Initial and Intermediate reports directly, and that is by reclassifying them as *major_incident_reclassification_as_non-major*, in field 1.1. Reclassification should only be selected if the incident no longer is considered as major.

Please see the flowchart on the next page, illustrating revision of all three incident modules.

## FLOWCHART FOR REVISING A REPORT



# Reclassify or revoke an incident

## RECLASSIFICATION

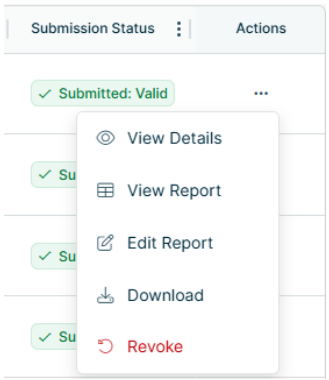
First and foremost, an incident should be reclassified as *major_incident_reclassification_as_non-major*. However, reclassification is not a viable option, then the incident can be deleted.

Field 2.10 (Other relevant information) is mandatory when reclassifying a report. Click *Preview* and submit the report.

## REVOCATION

If a mistake for example has been made, such as the same incident has been submitted in two different Initial notifications with the same data, then one of them can be revoked.

For the report that is to be revoked, navigate to column *Actions* to the right and select *Revoke*.

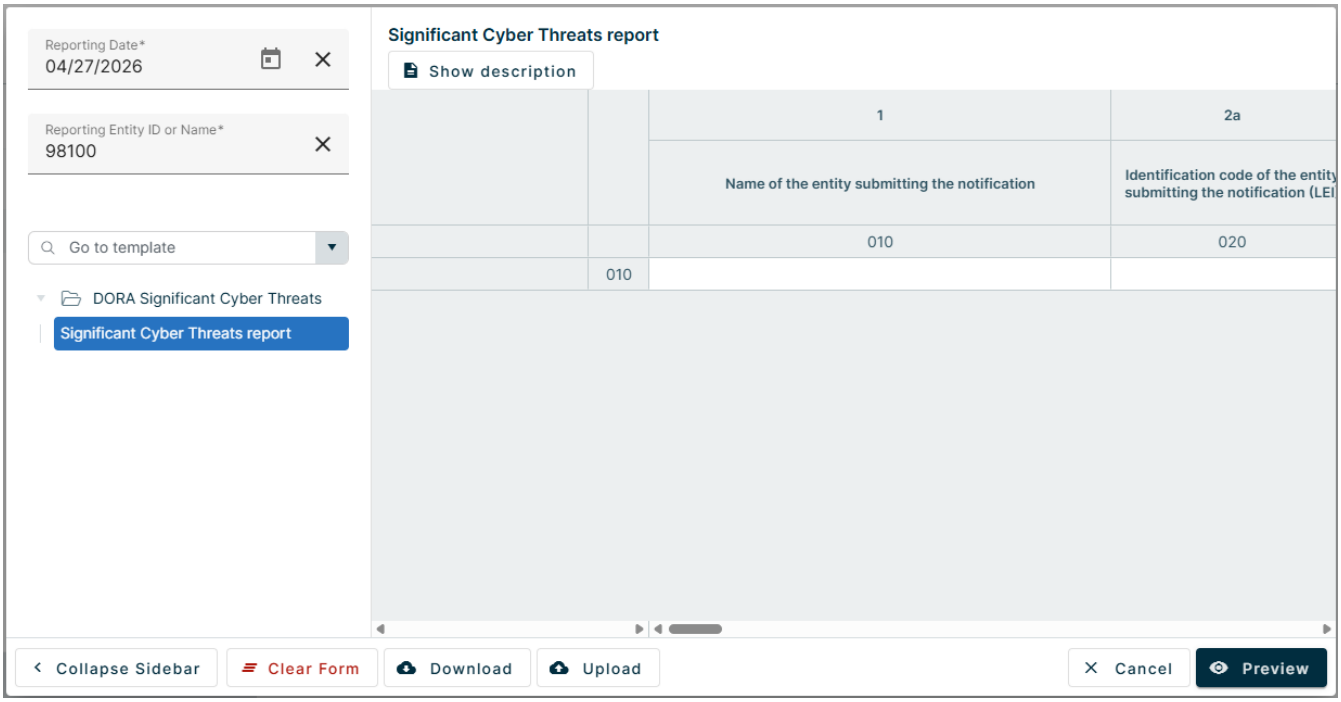



Enter a reason for revoking the report and click *Revoke*. The status symbol for the submission will change to ”Submitted: Processing”, then change to “Submitted: Valid”. I the column *Revision Status* it will now say ”Revoked” and an email notification will be sent to the email address entered when first submitting the report.

# Report Significant Cyber Threats

The report for Significant Cyber Threats according to the DORA directive is submitted in a separate reporting module in FIDAC. Select *Unscheduled* in the menu in FIDAC, select *Significant cyber threat* and click *Add New Report* in the top right corner to open the form.

The report itself is only one sheet. Click *Reporting Entity ID or Name* and select the company submitting the report. Data can now be entered into the fields.




Finish by clicking *Preview* in the bottom right corner. If something is missing or has been incorrectly entered (schema validation), those fields will be marked in red. Correct the fields, click *Preview* again and then *Report*.An email notification will be sent to the email address entered in the contact form.

Unlike the incident reports, there is no reference code used for Significant Cyber Threats since it is only one single reporting module.

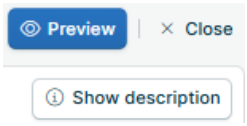
## RESUME THE REPORT

The downloaded JSON file can also be used to resume the report at a later time. If the report has been partially finished, save the JSON file by clicking *Download* and then close the form. At a later time, start a new report and click *Upload*, the saved data will automatically be filled in and you can continute. Once the remaining fields are completed, submit the report.

# Other information

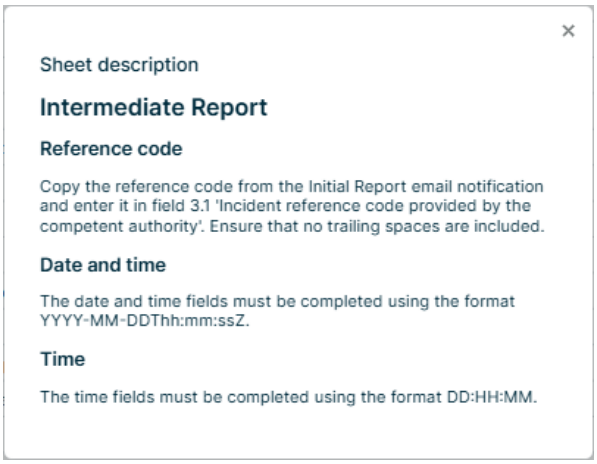
## SHEET DESCRIPTIONS

For each report, there is a description available in certain sheets, accessable in the top left corner of the form:




The information displayed is specific to the selected tab, but applies to the entire report (for example, date and time format). There are also specific descriptions. The example below describes how the reference code is used in the current tab.

Unfortunetaly, the information is only available in Swedish.




## DATE AND TIME

The format for date and time is quite specific. Date consists of year, month and day which are separated with a hyphen, followed by a T. Time consists of hours, minutes and seconds, which are separated by colon, followed by a Z. Broken down it looks like this:

YYYY-MM-DD T hh:mm:ssZ

Fields with date and time have to follow this format. An example could look like this:

2025-03-10T09:42:00Z

**UTC**

Z means ”zero offset” and is referencing UTC (Coordinated Universal Time). This means that time is according to timezone 0, which means that the time for an incident should subtract one hour for wintertime (Sweden, UTC +1) and two hours for daylight-saving time (Sweden, UTC +2). If the incident originated in another country than Sweden, find out the time zone for that country (according to UTC) and subtract or add hours accodringly. An example:

| | |
|---|---|
| Time of incident: | 09:42:00 |
| Time of incident according to UTC (wintertime): | 08:42:00 |
| Time of incident according to UTC (daylight-saving time): | 07:42:00 |

Fields consisting of only time are simpler, the format is days, hours and minutes, separated by colon:

DD:HH:MM

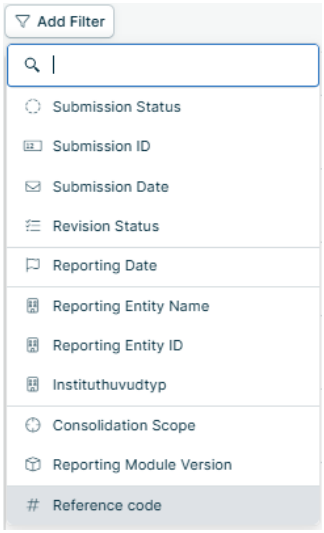
Nothing more is needed. Hours can be entered up to 23 and minutes up to 59, a day is represented by initial an 01. An example could look like this:

01:23:59

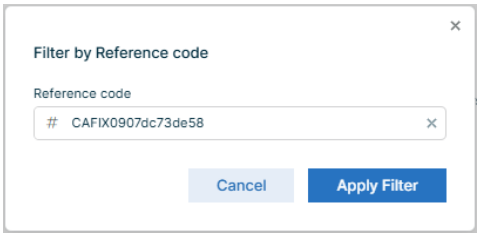
## FILTER BY A REFERENCE CODE

For parts of the final report, it is possible to filter by a reference code. The filter refers to field 3.1 in the respective report and returns results if the code has been reported.

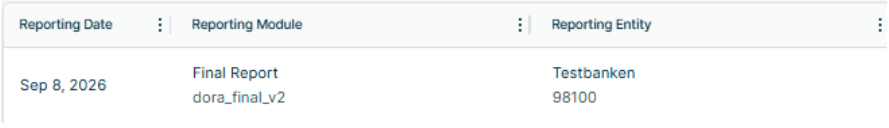
Click *Add filter* and then *Reference code* at the bottom of the list:



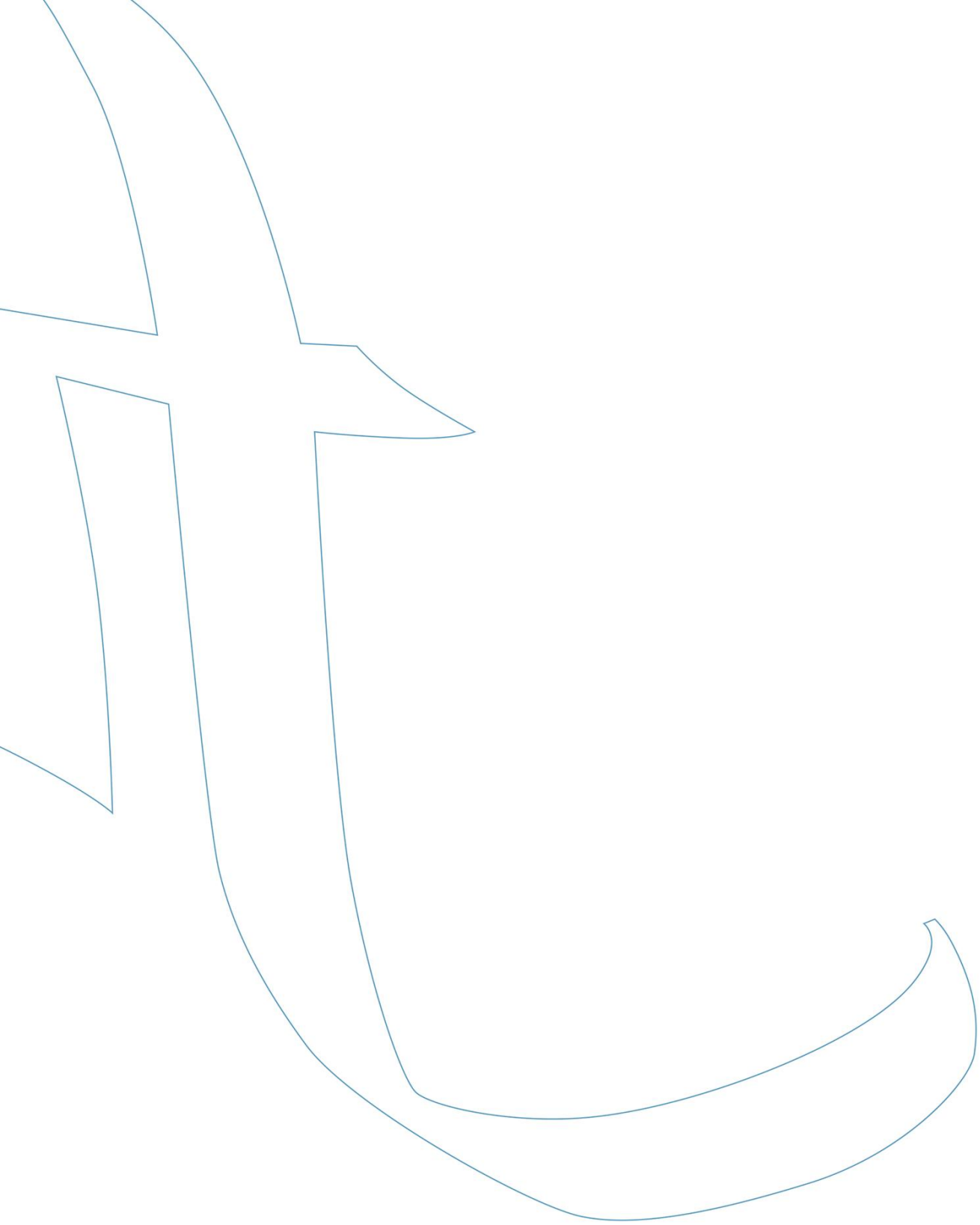

Click **Enter value**, enter the reference code and apply the filter.




The result will filter for the report containing the specified reference code.




For questions about this guide, please contact: reporting@fi.se



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

**www.fi.se**