



## **GUIDE**

# **DORA – Incident reporting**

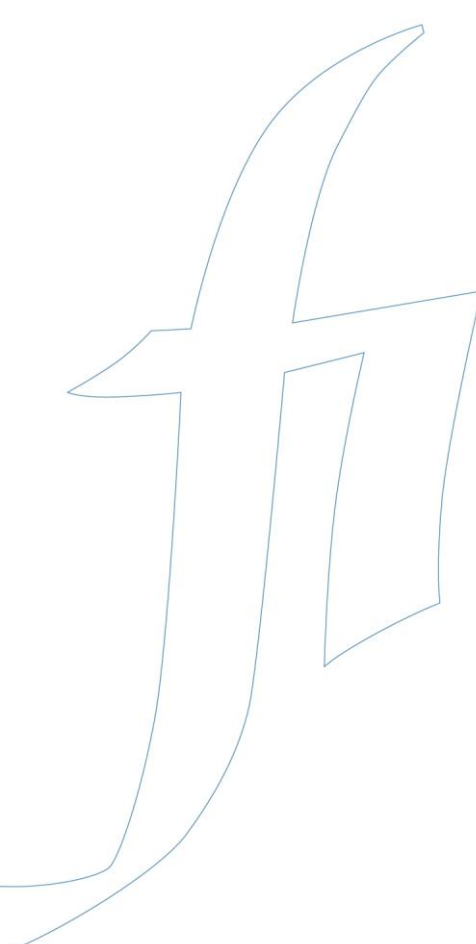
---

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 field 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.

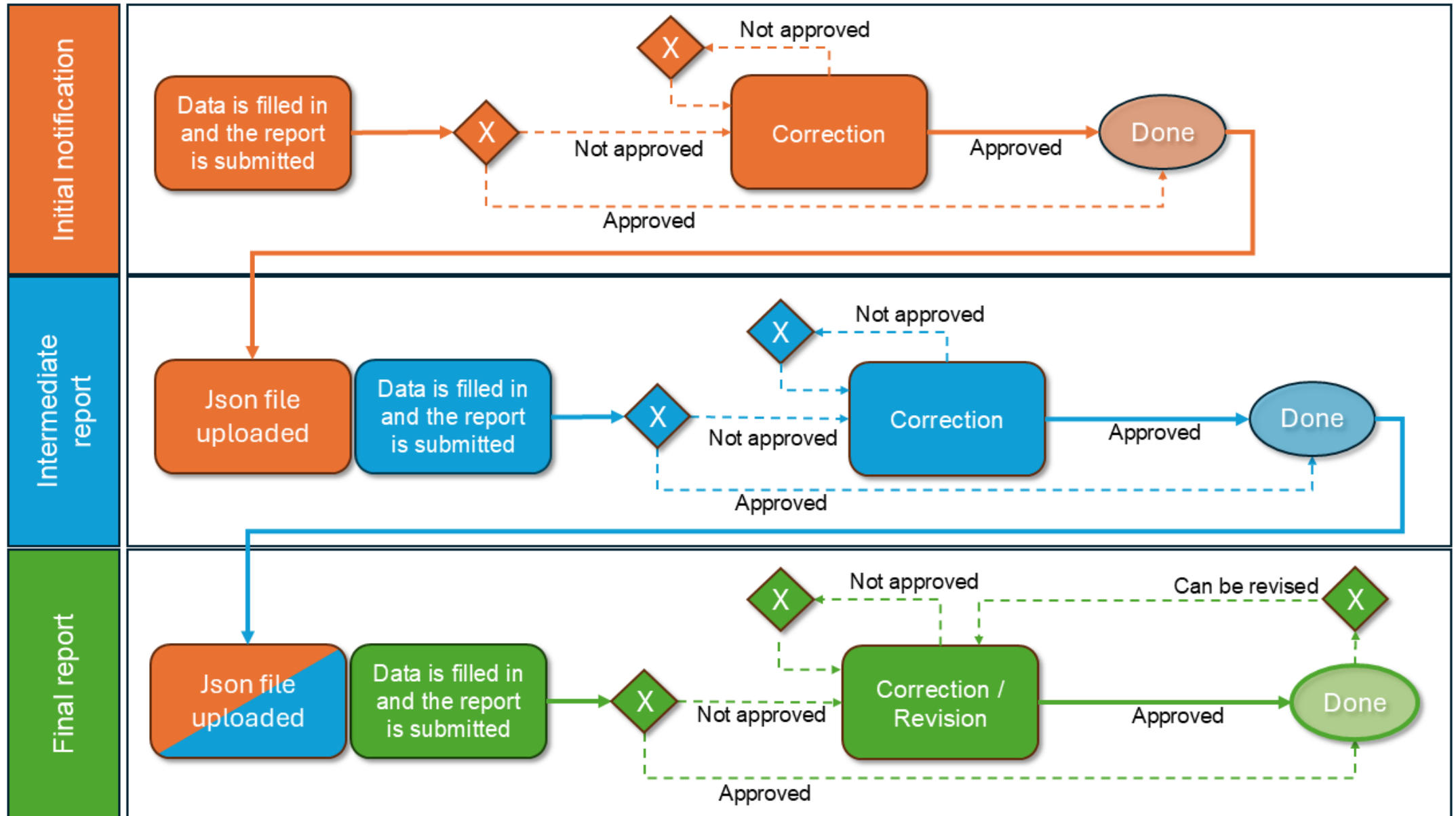
The reporting modules are divided, named and numbered via *Unscheduled* in the menu in FIDAC, like the below screenshot.

The screenshot displays the 'Unscheduled Reports' section of the FIDAC portal. On the left, a sidebar contains a 'Portal' header and three menu items: 'Scheduled', 'Unscheduled' (which is highlighted), and 'Unexpected'. The main content area is titled 'Unscheduled Reports' and includes a search bar. Below the search bar, there are four report categories, each with a list of report types and their corresponding formats:

| Report Category                       | Report Type                    | Format         |
|---------------------------------------|--------------------------------|----------------|
| 1. Dora Incident Initial Notification | Dora Initial Notification      | Web Form, JSON |
| 2. Dora Incident Intermediate         | Dora Intermediate Report       | Web Form, JSON |
| 3. Dora Incident Final                | Dora Final Report              | Web Form, JSON |
| Dora Cyber Threats                    | Dora Significant Cyber Threats | Web Form, JSON |

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.



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.

Create Report

Create a draft report to start working on a submission. You can return to complete it later and submit when ready.

Reporting Module

Initial Notification

Reporting Date

9/7/2026

Reporting Entity

Testbanken

ID: 98100

Consolidation Scope

Unspecified

Cancel

Create Draft

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.

Unscheduled / Dora Initial Notification / Create Report

Create Report

Initial Notification

Show description

Go to template

Type of submission

Initial Notification

Initial Notification - Affected Entities

|                                                                                                        |     | Value |
|--------------------------------------------------------------------------------------------------------|-----|-------|
| General information about the financial entity                                                         |     | 010   |
| 1.2 Name of the entity submitting the report                                                           | 010 |       |
| 1.3a Identification code of the entity submitting the report (LEI)                                     | 020 |       |
| 1.3b Identification code of the entity submitting the report (EU ID)                                   | 030 |       |
| 1.7 Primary contact person name                                                                        | 040 |       |
| 1.8 Primary contact person email address                                                               | 050 |       |
| 1.9 Primary contact person telephone number                                                            | 060 |       |
| 1.10 Secondary contact person name                                                                     | 070 |       |
| 1.11 Secondary contact person email address                                                            | 080 |       |
| 1.12 Secondary contact person telephone number                                                         | 090 |       |
| 1.13 Name of the ultimate parent undertaking                                                           | 100 |       |
| 1.14 LEI code of the ultimate parent undertaking                                                       | 110 |       |
| 1.15 Reporting currency                                                                                | 120 |       |
| Content of the initial notification                                                                    |     |       |
| 2.1 Incident reference code assigned by the financial entity                                           | 130 |       |
| 2.2 Date and time of detection of the ICT-related incident (Format: YYYY-MM-DDThh:mm:ssZ)              | 140 |       |
| 2.3 Date and time of classification of the incident as major (Format: YYYY-MM-DDThh:mm:ssZ)            | 150 |       |
| 2.4 Description of the ICT-related incident                                                            | 160 |       |
| 2.5 Classification criteria that triggered the incident report                                         | 170 |       |
| 2.6 Materiality thresholds for the classification criterion 'Geographical spread'                      | 180 |       |
| 2.7 Discovery of the major ICT-related incident                                                        | 190 |       |
| 2.8 Indication whether the incident originates from a third-party provider or another financial entity | 200 |       |
| 2.9 Activation of the business continuity plan, if activated                                           | 210 |       |
| 2.10 Other relevant information                                                                        | 220 |       |

Reporting Date

Sep 8, 2026

Reporting Entity

Testbanken

## 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.

| Affected Entities                         |                                           |
|-------------------------------------------|-------------------------------------------|
| 1.4 Type of the affected financial entity | 1.5 Name of the affected financial entity |
| 010                                       | 020                                       |

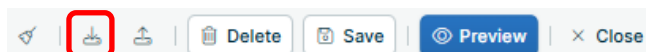
At least one row must be provided. For the reporting entity, specify the type of financial entity (1.4) and LEI code (1.6). If other financial entities are covered by the report, specify the type (1.4), name (1.5), and LEI code (1.6) for each entity.

| Affected Entities                         |                                           |
|-------------------------------------------|-------------------------------------------|
| 1.4 Type of the affected financial entity | 1.5 Name of the affected financial entity |
| 010                                       | 020                                       |
| 10                                        |                                           |
| 20                                        |                                           |

## 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, then 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 contains information about the report and a unique reference code.

**Upload Report**

**Additional Data**

Provide some additional information with your report submission.

**Name\***  
First and last name

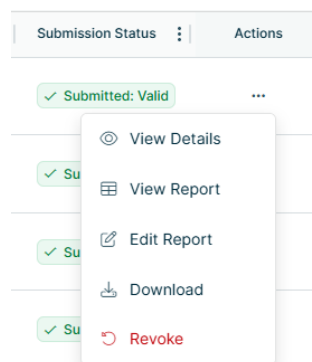
**Phone number\***  
Phone number of responsible person

**Email address\***  
Email address (a confirmation email will be sent to this address)

1 2 Cancel → Next

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 download 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 contain information about the report was approved or encountered any validation errors, and details about the submission.

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

#### Details about the submission:

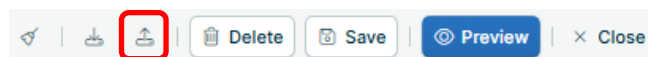
- Financial entity ID: 98100
- Financial entity name: Testbanken
- Data collection: 1. Dora Incident Initial Report
- Module version: dora\_initial\_v1
- Submission ID: 2026-0427-dc73-de58
- Reporting date: April 27, 2026
- Submission timestamp: April 27, 2026 08:37:40
- Reference code: CAFIX0427dc73de58**

The reference code is used in the next two reporting modules, in order 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.



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*:

| 1.1 Type of submission |                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------|
|                        | 010                                                                                                              |
| 010                    | <div> <input type="text"/> </div> <div> intermediate_report<br/> major_incident_reclassified_as_non-major </div> |

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.

Unscheduled / Dora Intermediate Report / Create Report

Delete
Save
Preview
Close

Create Report

Initial Notification
Show description

Go to template

Type of submission

Initial Notification
Initial Notification - Affected Entities
Intermediate report

|                                                                                             |     | Value                |
|---------------------------------------------------------------------------------------------|-----|----------------------|
| General information about the financial entity                                              |     |                      |
|                                                                                             |     | 010                  |
| 1.2 Name of the entity submitting the report                                                | 010 | Testbanken           |
| 1.3a Identification code of the entity submitting the report (LEI)                          | 020 | A123BCXQ008YPKG3271U |
| 1.3b Identification code of the entity submitting the report (EU ID)                        | 030 |                      |
| 1.7 Primary contact person name                                                             | 040 |                      |
| 1.8 Primary contact person email address                                                    | 050 |                      |
| 1.9 Primary contact person telephone number                                                 | 060 |                      |
| 1.10 Secondary contact person name                                                          | 070 |                      |
| 1.11 Secondary contact person email address                                                 | 080 |                      |
| 1.12 Secondary contact person telephone number                                              | 090 |                      |
| 1.13 Name of the ultimate parent undertaking                                                | 100 |                      |
| 1.14 LEI code of the ultimate parent undertaking                                            | 110 |                      |
| 1.15 Reporting currency                                                                     | 120 | SEK                  |
| Content of the initial notification                                                         |     |                      |
| 2.1 Incident reference code assigned by the financial entity                                | 130 |                      |
| 2.2 Date and time of detection of the ICT-related incident (Format: YYYY-MM-DDThh:mm:ssZ)   | 140 | 2026-09-07T08:00:00Z |
| 2.3 Date and time of classification of the incident as major (Format: YYYY-MM-DDThh:mm:ssZ) | 150 | 2026-09-07T08:07:00Z |
| 2.4 Description of the ICT-related incident                                                 | 160 |                      |

### The reference code

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

Unscheduled / Dora Intermediate Report / Create Report

Create Report

Go to template

Type of submission

Initial Notification

Initial Notification - Affected Entities

Intermediate report

Intermediate report

Show description

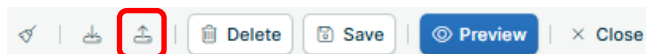
|                                                                                                                             |     | Value             |
|-----------------------------------------------------------------------------------------------------------------------------|-----|-------------------|
| <b>Content of intermediate report</b>                                                                                       |     |                   |
| 3.1 Incident reference code provided by the competent authority (Please use the reference code from the email notification) | 010 | CAFIX0907dc73de58 |
| 3.2 Date and time of occurrence of the incident (Format: YYYY-MM-DDThh:mm:ssZ)                                              | 020 |                   |
| 3.3 Date and time when services, activities or operations have been recovered (Format: YYYY-MM-DDThh:mm:ssZ)                | 030 |                   |
| 3.4 Number of clients affected                                                                                              | 040 |                   |
| 3.5 Percentage of clients affected                                                                                          | 050 |                   |
| 3.6 Number of financial counterparts affected                                                                               | 060 |                   |
| 3.7 Percentage of financial counterparts affected                                                                           | 070 |                   |
| 3.8 Impact on relevant clients or financial counterparts                                                                    | 080 |                   |
| 3.9 Number of affected transactions                                                                                         | 090 |                   |
| 3.10 Percentage of affected transactions                                                                                    | 100 |                   |
| 3.11 Value of affected transactions                                                                                         | 110 |                   |
| 3.12 Information on whether the numbers are actual or estimates, or whether there has not been any impact                   | 120 |                   |
| 3.13 Reputational impact                                                                                                    | 130 |                   |
| 3.14 Contextual information about the reputational impact                                                                   | 140 |                   |
| 3.15 Duration of the major ICT-related incident (Format: DD:HH:MM)                                                          | 150 |                   |
| 3.16 Service downtime (Format: DD:HH:MM)                                                                                    | 160 |                   |

A validation rule will check to make sure that the entered reference code is corresponding 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.



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*:

| 1.1 Type of submission |                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------|
|                        | 010                                                                                                  |
| 010                    | <div> <div></div> <div>final_report</div> <div>major_incident_reclassified_as_non-major</div> </div> |

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.

Unscheduled / Dora Final Report / Create Report

Delete

Save

Preview

Close

Create Report

Intermediate report

Show description

Go to template

Type of submission

Initial Notification

Initial Notification - Affected Entities

Intermediate report

Final report

|                                                                                                                             |     | Value             |
|-----------------------------------------------------------------------------------------------------------------------------|-----|-------------------|
| Content of intermediate report                                                                                              |     |                   |
|                                                                                                                             | 010 | 010               |
| 3.1 Incident reference code provided by the competent authority (Please use the reference code from the email notification) | 010 | CAFIX0907dc73de58 |
| 3.2 Date and time of occurrence of the incident (Format: YYYY-MM-DDThh:mm:ssZ)                                              | 020 |                   |
| 3.3 Date and time when services, activities or operations have been recovered (Format: YYYY-MM-DDThh:mm:ssZ)                | 030 |                   |
| 3.4 Number of clients affected                                                                                              | 040 |                   |
| 3.5 Percentage of clients affected                                                                                          | 050 |                   |
| 3.6 Number of financial counterparts affected                                                                               | 060 |                   |
| 3.7 Percentage of financial counterparts affected                                                                           | 070 |                   |
| 3.8 Impact on relevant clients or financial counterparts                                                                    | 080 |                   |
| 3.9 Number of affected transactions                                                                                         | 090 |                   |
| 3.10 Percentage of affected transactions                                                                                    | 100 |                   |
| 3.11 Value of affected transactions                                                                                         | 110 |                   |
| 3.12 Information on whether the numbers are actual or estimates, or whether there has not been any impact                   | 120 |                   |
| 3.13 Reputational impact                                                                                                    | 130 |                   |
| 3.14 Contextual information about the reputational impact                                                                   | 140 |                   |
| 3.15 Duration of the major ICT-related incident (Format: DD:HH:MM)                                                          | 150 |                   |
| 3.16 Service downtime (Format: DD:HH:MM)                                                                                    | 160 |                   |

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

Unscheduled / Dora Final Report / Create Report

✂ | 📄 | 📤 | 🗑 Delete | 💾 Save | 🔍 Preview | ✕ Close

Create Report

📄 | Final report

Show description

🔍 Go to template ▼

Type of submission  
Initial Notification  
Initial Notification - Affected Entities  
Intermediate report  
Final report

|                                                                                                                          |     | Value |
|--------------------------------------------------------------------------------------------------------------------------|-----|-------|
| Content of final report                                                                                                  |     | 010   |
| 4.1 High-level classification of root causes of the incident                                                             | 010 |       |
| 4.2 Detailed classification of root causes of the incident                                                               | 020 |       |
| 4.3 Additional classification of root causes of the incident                                                             | 030 |       |
| 4.4 Other types of root cause types                                                                                      | 040 |       |
| 4.5 Information about the root causes of the incident                                                                    | 050 |       |
| 4.6 Incident resolution                                                                                                  | 060 |       |
| 4.7 Date and time when the incident root cause was addressed                                                             | 070 |       |
| 4.8 Date and time when the incident was resolved                                                                         | 080 |       |
| 4.9 Information if the permanent resolution date of the incidents differs from the initially planned implementation date | 090 |       |
| 4.10 Assessment of risk to critical functions for resolution purposes                                                    | 100 |       |
| 4.11 Information relevant for resolution authorities                                                                     | 110 |       |
| 4.12 Materiality threshold for the classification criterion 'Economic impact'                                            | 120 |       |
| 4.13 Amount of gross direct and indirect costs and losses                                                                | 130 |       |
| 4.14 Amount of financial recoveries                                                                                      | 140 |       |
| 4.15 Information on whether the non-major incidents have been recurring                                                  | 150 |       |
| 4.16 Date and time of occurrence of recurring incidents                                                                  | 160 |       |

# 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 has to be done when submitting the Intermediate report, in sheet Initial report.

Unscheduled **Dora Intermediate Report** Create Report

Create Report

Go to template

Type of submission

Initial Notification

Initial Notification - Affected Entities

Intermediate report

Reporting Date

Sep 8, 2026

Reporting Entity

Testbanken

Initial Notification

Show description

|                                                                                                        |     | Value                |
|--------------------------------------------------------------------------------------------------------|-----|----------------------|
| <b>General information about the financial entity</b>                                                  |     |                      |
| 1.2 Name of the entity submitting the report                                                           | 010 | Testbanken           |
| 1.3a Identification code of the entity submitting the report (LEI)                                     | 020 | A123BCXQ008YPKG321U  |
| 1.3b Identification code of the entity submitting the report (EU ID)                                   | 030 |                      |
| 1.7 Primary contact person name                                                                        | 040 |                      |
| 1.8 Primary contact person email address                                                               | 050 |                      |
| 1.9 Primary contact person telephone number                                                            | 060 |                      |
| 1.10 Secondary contact person name                                                                     | 070 |                      |
| 1.11 Secondary contact person email address                                                            | 080 |                      |
| 1.12 Secondary contact person telephone number                                                         | 090 |                      |
| 1.13 Name of the ultimate parent undertaking                                                           | 100 |                      |
| 1.14 LEI code of the ultimate parent undertaking                                                       | 110 |                      |
| 1.15 Reporting currency                                                                                | 120 | SEK                  |
| <b>Content of the initial notification</b>                                                             |     |                      |
| 2.1 Incident reference code assigned by the financial entity                                           | 130 |                      |
| 2.2 Date and time of detection of the ICT-related incident (Format: YYYY-MM-DDThh:mm:ssZ)              | 140 | 2026-09-07T08:00:00Z |
| 2.3 Date and time of classification of the incident as major (Format: YYYY-MM-DDThh:mm:ssZ)            | 150 | 2026-09-07T08:17:00Z |
| 2.4 Description of the ICT-related incident                                                            | 160 |                      |
| 2.5 Classification criteria that triggered the incident report                                         | 170 |                      |
| 2.6 Materiality thresholds for the classification criterion 'Geographical spread'                      | 180 |                      |
| 2.7 Discovery of the major ICT-related incident                                                        | 190 |                      |
| 2.8 Indication whether the incident originates from a third-party provider or another financial entity | 200 |                      |
| 2.9 Activation of the business continuity plan, if activated                                           | 210 |                      |
| 2.10 Other relevant information                                                                        | 220 |                      |

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

Unscheduled **Dora Final Report** Create Report

Create Report

Go to template

Type of submission

Initial Notification

Initial Notification - Affected Entities

Intermediate report

Final report

Intermediate report

Show description

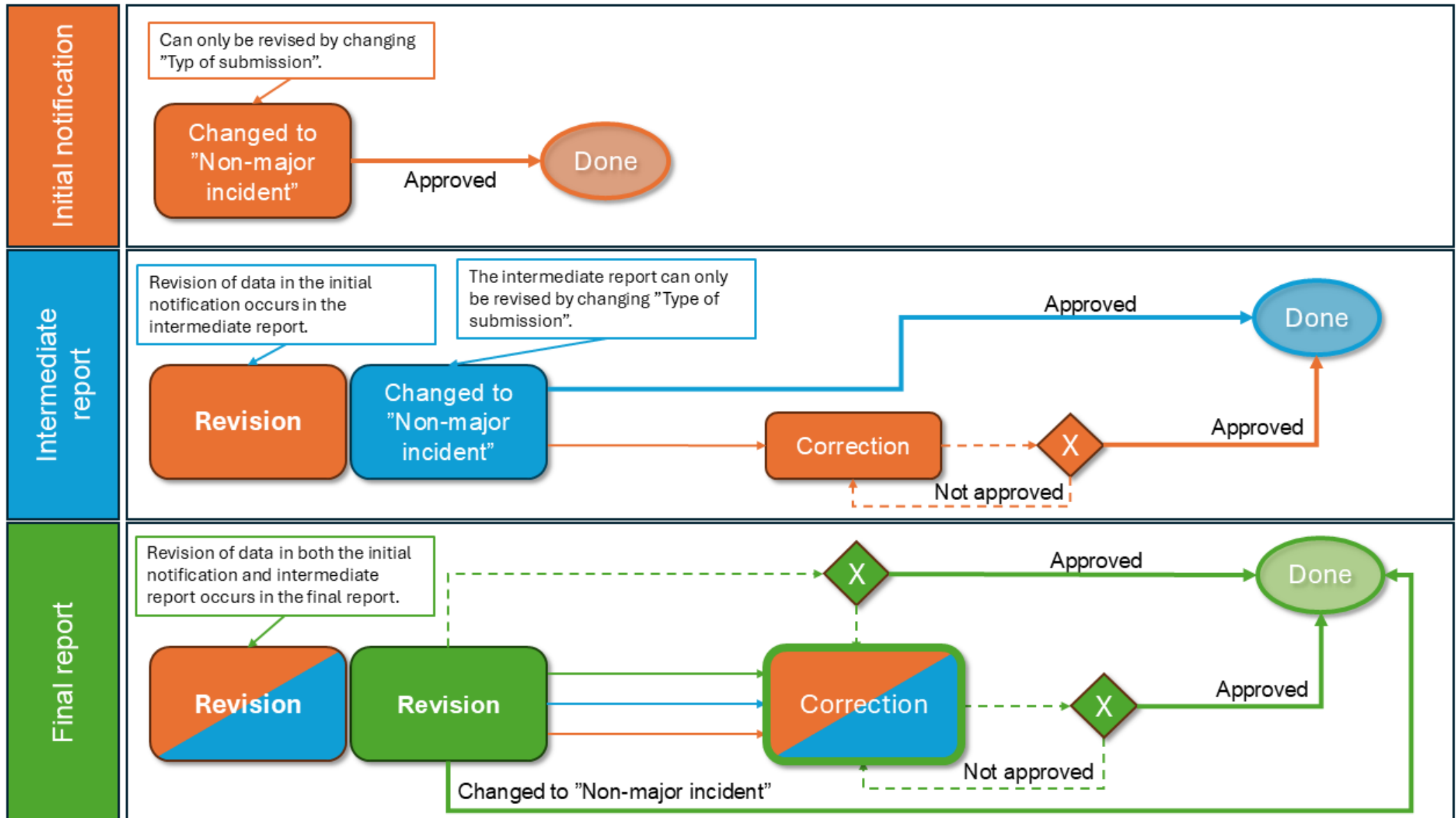
|                                                                                                                             |     | Value             |
|-----------------------------------------------------------------------------------------------------------------------------|-----|-------------------|
| <b>Content of intermediate report</b>                                                                                       |     |                   |
| 3.1 Incident reference code provided by the competent authority (Please use the reference code from the email notification) | 010 | CAFIX0907dc73de58 |
| 3.2 Date and time of occurrence of the incident (Format: YYYY-MM-DDThh:mm:ssZ)                                              | 020 |                   |
| 3.3 Date and time when services, activities or operations have been recovered (Format: YYYY-MM-DDThh:mm:ssZ)                | 030 |                   |
| 3.4 Number of clients affected                                                                                              | 040 |                   |
| 3.5 Percentage of clients affected                                                                                          | 050 |                   |
| 3.6 Number of financial counterparts affected                                                                               | 060 |                   |
| 3.7 Percentage of financial counterparts affected                                                                           | 070 |                   |
| 3.8 Impact on relevant clients or financial counterparts                                                                    | 080 |                   |
| 3.9 Number of affected transactions                                                                                         | 090 |                   |
| 3.10 Percentage of affected transactions                                                                                    | 100 |                   |
| 3.11 Value of affected transactions                                                                                         | 110 |                   |
| 3.12 Information on whether the numbers are actual or estimates, or whether there has not been any impact                   | 120 |                   |
| 3.13 Reputational impact                                                                                                    | 130 |                   |
| 3.14 Contextual information about the reputational impact                                                                   | 140 |                   |
| 3.15 Duration of the major ICT-related incident (Format: DD:HH:MM)                                                          | 150 |                   |
| 3.16 Service downtime (Format: DD:HH:MM)                                                                                    | 160 |                   |

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

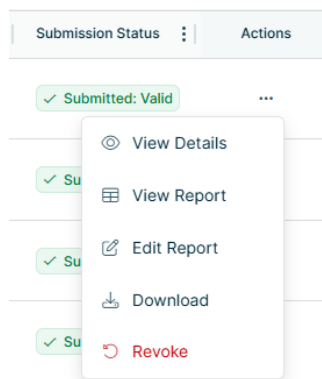
First and foremost, an incident should be reclassified as *major\_incident\_reclassification\_as\_non-major*. However, is reclassification is not a viable option, then the incident can be deleted.

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". In 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.

**Significant Cyber Threats report**

Show description

|  |     | 1                                              | 2a                                                                  |
|--|-----|------------------------------------------------|---------------------------------------------------------------------|
|  |     | Name of the entity submitting the notification | Identification code of the entity submitting the notification (LEI) |
|  |     | 010                                            | 020                                                                 |
|  | 010 |                                                |                                                                     |

Go to template

DORA Significant Cyber Threats

Significant Cyber Threats report

< Collapse Sidebar

Clear Form

Download

Upload

X Cancel

Preview

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.

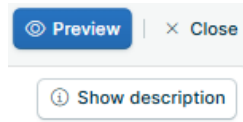
## RESUME THE REPORT

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 continue. Once the remaining fields are completed, submit the report.

## Other information

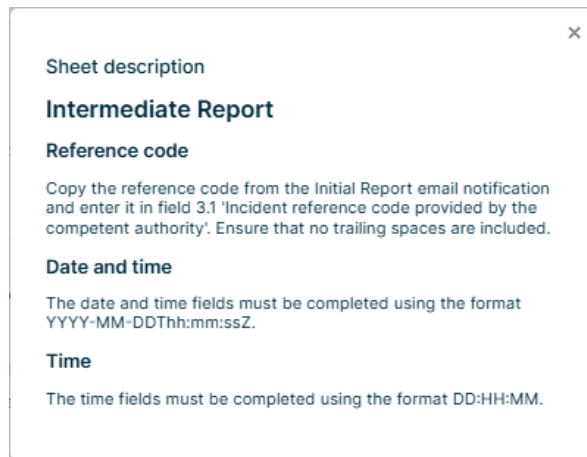
### SHEET DESCRIPTIONS

For each report, there is a description available in certain sheets, accessible 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.

Unfortunately, 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 accordingly. 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:

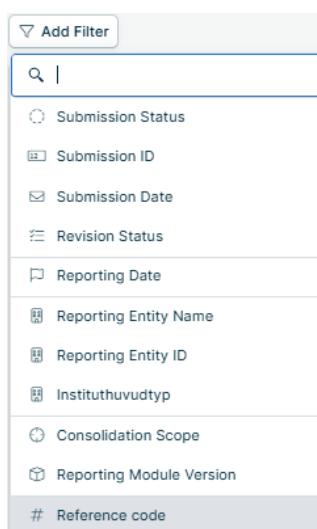
01:23:59

### 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.

| Reporting Date | Reporting Module              | Reporting Entity    |
|----------------|-------------------------------|---------------------|
| Sep 8, 2026    | Final Report<br>dora_final_v2 | Testbanken<br>98100 |

For questions about this guide, please contact: [reporting@fi.se](mailto: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](http://www.fi.se)**