



Banc Ceannais na hÉireann  
Central Bank of Ireland

Eurosystem

# Guide to Submitting DORA Major ICT-related Incident and Significant Cyber Threat Report(s) on the Central Bank of Ireland Portal

# Contents

<b>1 Glossary of Terms &amp; Abbreviations .....</b>	<b>4</b>
<b>2 Checklist .....</b>	<b>5</b>
<b>3 Overview .....</b>	<b>6</b>
3.1 Purpose of This Guidance .....	6
<b>4 Portal Information .....</b>	<b>7</b>
4.1 Inactivity.....	7
4.2 Internet Browser.....	7
4.3 Logging In .....	7
4.4 User Permissions.....	7
<b>5 Major ICT-related Incident Reporting .....</b>	<b>9</b>
5.1 How to Submit an Initial DORA Major ICT-related Notification.....	9
5.1.1 Complete the Reporting Template.....	9
5.1.2 Create a New Major Incident Report on the Portal .....	9
5.1.3 Naming Convention for the DORA Major Incident Report.....	11
5.1.4 Submission of a DORA Major Incident Report on the Portal.....	12
5.1.5 Incident Reference Code.....	15
5.2 How to submit an Intermediate DORA Major Incident Report .....	16
5.2.1 Complete the Reporting Template.....	16
5.2.2 Submit the Intermediate Report on the Portal.....	17
5.3 How to submit a Final DORA Major Incident Report.....	20
5.3.1 Complete the Reporting Template.....	20
5.3.2 Submit the Final Report on the Portal.....	20
5.4 How to Reclassify a Major Incident as Non-major .....	23
5.4.1 Complete the Reporting Template.....	23
5.4.2 Submit the Major Incident Reclassified as Non-major Report on the Portal...	24
5.5 Submitting a DORA Major Incident Report where there are two (or more) separate incidents on the same day .....	27

5.6 Common Validation Errors .....	28
<b>6 Significant Cyber Threat Reporting .....</b>	<b>29</b>
6.1 Complete the Reporting Template .....	29
6.2 Submit a DORA Significant Cyber Threat on the Portal.....	29
6.3 Naming Convention for the DORA Significant Cyber Threat Report.....	34
<b>7 FAQ.....</b>	<b>35</b>
7.1 What happens if I get an error message on the Portal when uploading a report? .	35
7.2 What do I do if I'm unable to access the Portal? .....	35
7.3 What do I do if my submission is rejected on the Portal?.....	35
7.4 Can I make an update to my initial notification, intermediary report, or final report?.....	37
7.5 I am unable to edit a cell in the reporting template .....	37
<b>Annex: Validation Rules .....</b>	<b>38</b>

# 1 Glossary of Terms & Abbreviations

<b>Term</b>	<b>Description</b>
<b>C Code</b>	The financial entity's number that is used for the Portal
<b>Central Bank</b>	The Central Bank of Ireland
<b>DORA</b>	Digital Operational Resilience Act (DORA) ( <a href="#">Regulation (EU) 2022/2554</a> )
<b>ICT</b>	Information and Communication Technology
<b>LEI</b>	Legal Entity Identifier
<b>Portal</b>	The Central Bank of Ireland Portal used to submit major ICT-related incident and significant cyber threat reports <a href="#">here</a>
<b>Reporting Template</b>	The major ICT-related incident reporting template or significant cyber threat reporting template that are available on the Central Bank of Ireland's DORA webpage <a href="#">here</a>

## 2 Checklist

When submitting a major ICT-related incident or significant cyber threat report on the Central Bank of Ireland (Central Bank) Portal, the following checklist may be of assistance.

- The relevant reporting template provided [here](#) on the DORA webpage on the Central Bank's website has been used.
- All mandatory fields have been populated in the reporting template.
- All conditional mandatory fields have been populated in the reporting template, where required. (Note, a number of fields become mandatory based on the preceding answers provided. The reporting instructions tab of the reporting template outlines such fields).
- The name of the reporting template adheres to the naming convention. [Please see here for more details on the naming convention.](#)
- The correct type of submission (i.e. initial notification, intermediate report, final report or major incident reclassified as non-major) has been selected in field 1.1 of the incident reporting template and matches the report type selected on the "Load a file" page of the Central Bank [Portal](#) (the Portal).
- The user has the necessary access permissions to submit the reporting template on the Portal. [Please see here for more details on Portal user permissions.](#)
- Following the submission of an initial notification, when submitting an intermediate report, final report or major incident reclassified as non-major report for the same incident, on the "Load a file" page of the Portal the "First file being submitted for this incident" tick box is unchecked and the correct corresponding "Report Reference" is selected. This ensures that the report being submitted is linked to the relevant preceding report submitted in respect of the incident. [Please see here for more details on the submission process.](#)
- When submitting an intermediate report or final report, the relevant incident reference code has been populated in field 3.1 of the incident reporting template, where applicable. [Please see here for more details.](#)
- The user is aware of alternative methods of submitting the reporting template in the event that the entity's or Central Bank's systems are unavailable. (Note, if experiencing technical issues with the Portal, please email [onlinereturns@centralbank.ie](mailto:onlinereturns@centralbank.ie) or call 01 224 4545. If unable to submit an incident or significant cyber threat report, please contact the relevant supervisory team in the Central Bank using existing communication channels). Once any technical/operational issues have been resolved, the expectation is that the incident or significant cyber threat report will be submitted on the Portal as soon as practicable.

# 3 Overview

## 3.1 Purpose of This Guidance

This document provides systems guidance for financial entities subject to the Digital Operational Resilience Act (DORA)<sup>1</sup> in relation to submitting major ICT-related incident reports and significant cyber threat reports on the [Portal](#).

The information contained in this guidance applies to financial entities in scope of DORA where the Central Bank is the designated competent authority, and should be read in combination with other relevant documentation and legislative texts concerning DORA incident and cyber threat reporting.<sup>2</sup>

When submitting a major ICT-related incident or significant cyber threat report, in scope financial entities must use the relevant reporting template provided [here](#) on the DORA webpage of the Central Bank's website.

**It is important to note that validation rules apply to the structure of the reporting template. This means that when populating the reporting template, the structure and formatting of same must not be altered.** For more information on the validation rules, please refer to the annex.

In this guidance, examples of the successful and unsuccessful submission of a major ICT-related incident report and significant cyber threat report on the Portal are provided.

With regard to the Portal, it is the responsibility of the financial entity's administrator to manage user access to same. For users not familiar with the Portal, information and related guidance documents are available on the Central Bank's website [here](#).

---

<sup>1</sup> [Regulation \(EU\) 2022/2554](#).

<sup>2</sup> For instance, the Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and the Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat (the draft version is available [here](#)).

## 4 Portal Information

### 4.1 Inactivity

A Portal login session times out after eight hours of inactivity, at which point the user is required to login again (including using the second factor method). When the user is finished using the Portal, it is recommended that the user exit the system using the logout link under “Account Settings” in the top right corner of the screen.

### 4.2 Internet Browser

As explained in the Browser Support Section of the Portal, the Portal should work with any modern, standards-based browser. The Central Bank does not require, or recommend, any particular browser as the Central Bank’s websites and public-facing applications support the current versions of all major browsers. Testing is concentrated on the most commonly used browsers. At this time, this specifically includes Chrome and Edge.

### 4.3 Logging In

The [Getting Started](#) Help section of the Central Bank’s website provides information on how to register for and login to the Portal, including setting up second factor authentication.

### 4.4 User Permissions

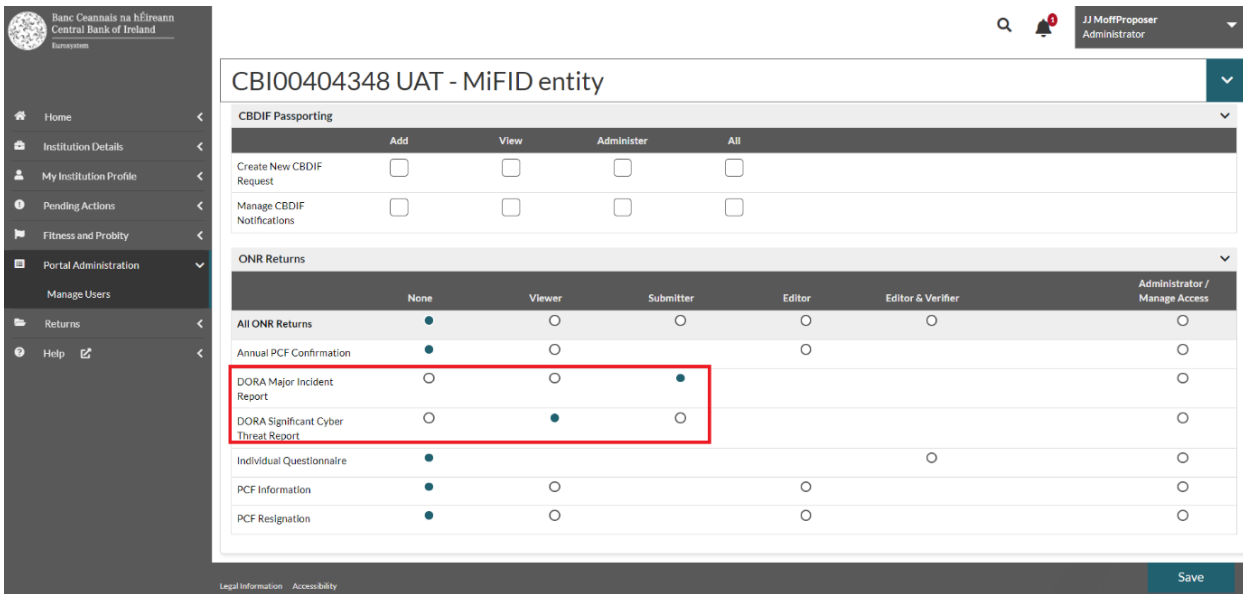
Portal administrators automatically have permission to view/submit a DORA major ICT-related incident or significant cyber threat report.

The administrator can assign permissions to non-administrator users via the Portal administrator tab.

Go to “Portal Administration” > “Manage Users” > Select the relevant user > Select “Actions” > “Manage Permissions”.

User Type	Person Name	Person Code	E-mail	User Status	Last Login	Actions
User	John Doe	UA0300630	john.doe@gmail.ie	Linked	--	Actions
Admin	JJ MuffProposer	UA0300594	james.mofftt@centralbank.ie	Linked	--	Actions
User	James MuffApplicant	UA0300591	jimmy1@example.com	Added	--	Actions

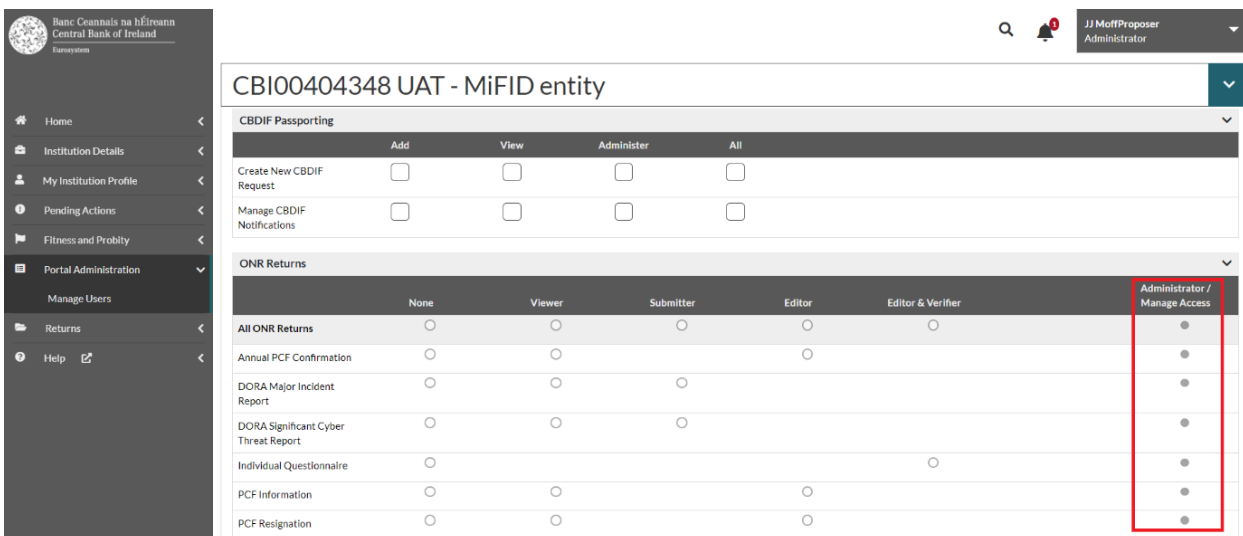
Scroll to the bottom of the page and locate ONR Returns. From this section, viewer or submitter access can be chosen.



In the above example, the user has submitter access for major ICT-related incident reports and viewer access for significant cyber threat reports.

A submitter has the ability to both submit reports and view previously submitted reports. A viewer can only view previously submitted reports. Select the required level of access and then click “Save”.

The administrator has access to all reports as indicated by the grey shaded circles highlighted in the red box below.



**If you cannot see the Returns tab, please note the below:**

Portal administrators should activate their permissions via the Portal administrator tab. The Portal administrator receives automatic access to all return/report types, however in the scenario where the “View/Edit” option is not displayed, the following action should be taken:

Go to “Portal Administration” > “Manage Users” > Select the relevant user > Select “Actions” > “Manage Permissions” > Scroll to the bottom of the permission page and select “Save”. Once saved, best practice is to clear the browser history and to log in again. The “Returns” menu item should then appear.



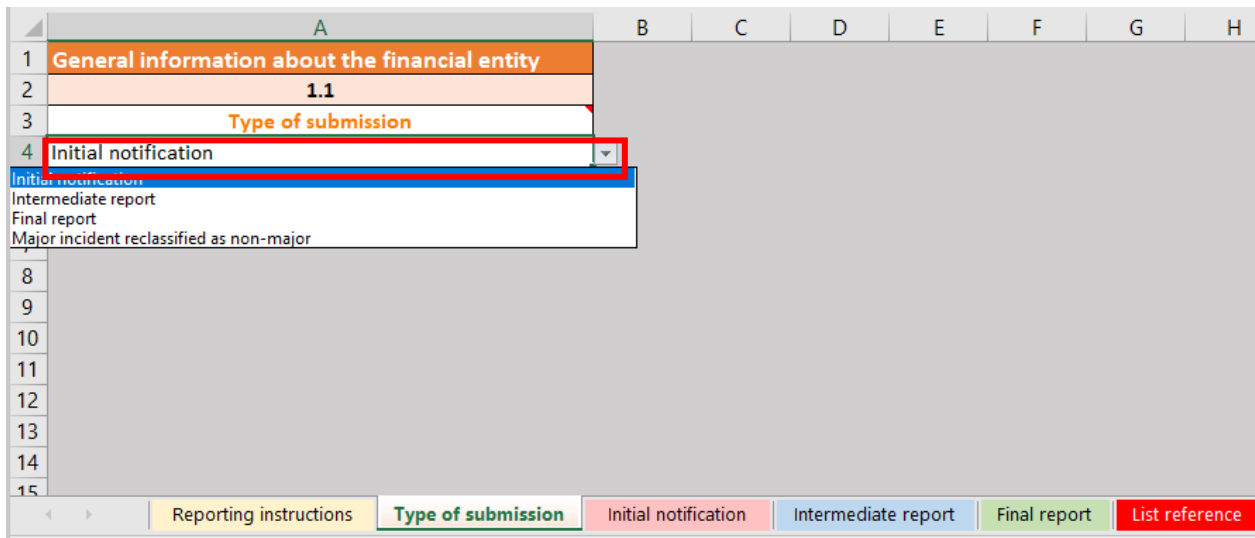
# 5 Major ICT-related Incident Reporting

## 5.1 How to Submit an Initial DORA Major ICT-related Notification

### 5.1.1 Complete the Reporting Template

As already noted, the reporting templates are available [here](#) on the DORA webpage of the Central Bank’s website.

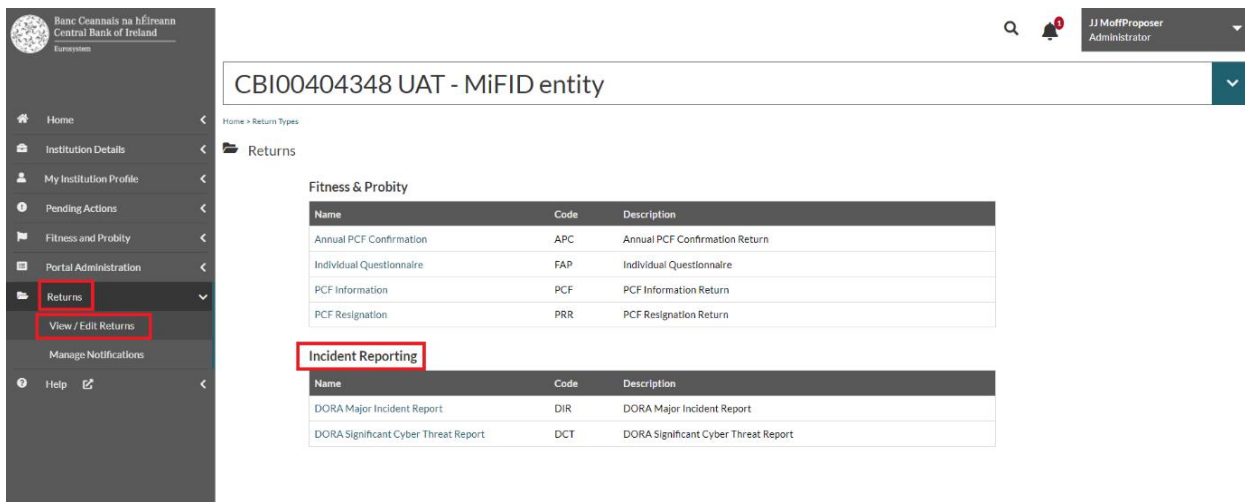
For field 1.1 of the DORA incident reporting template, ensure that type of submission selected is “Initial notification”.



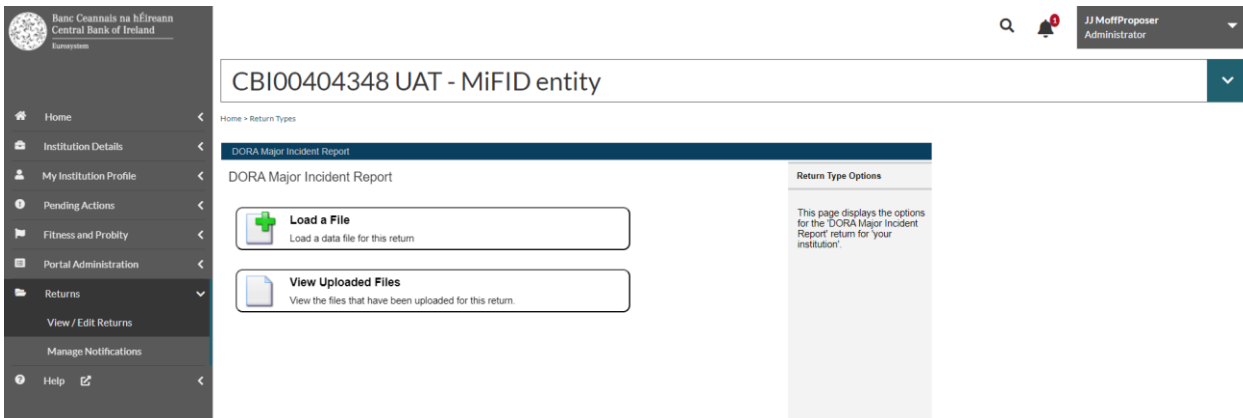
Ensure that all mandatory and conditional mandatory fields for the initial notification are populated in the reporting template, and that name of same adheres to the naming convention (see section 5.1.3 for more details).

### 5.1.2 Create a New Major Incident Report on the Portal

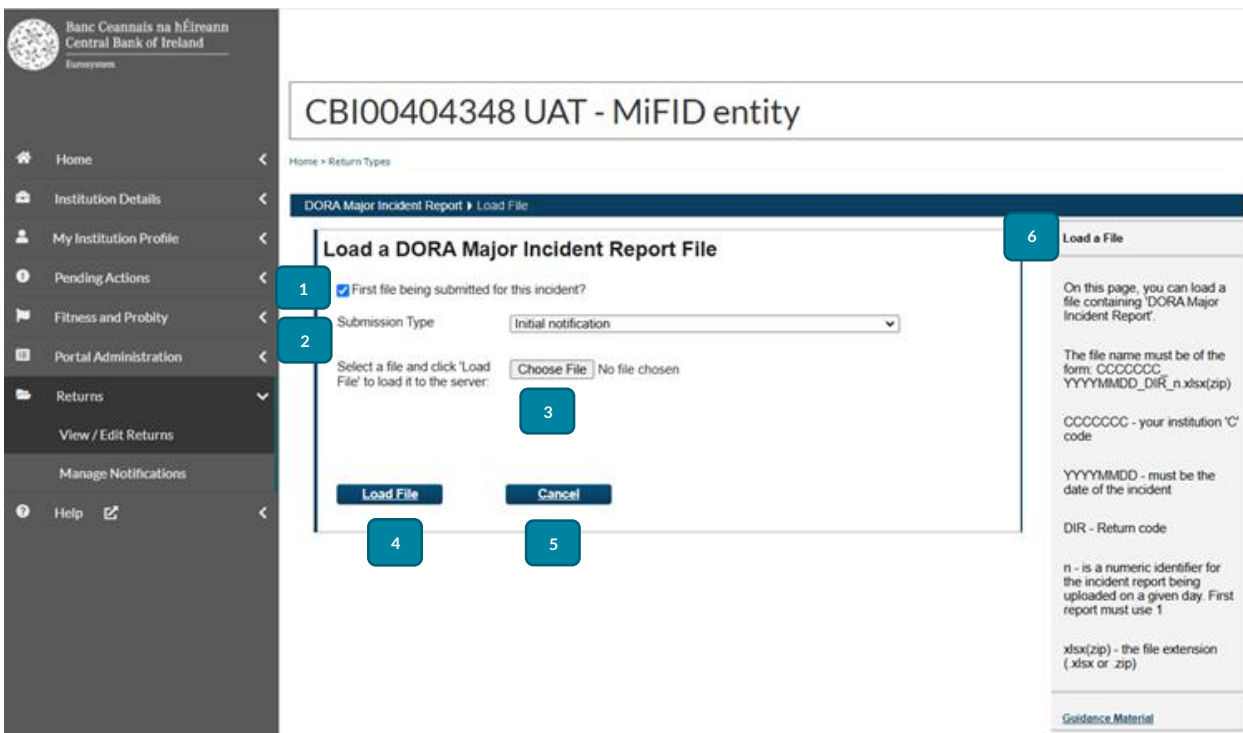
To submit a major ICT-related incident report, the user logs in to the Portal with their user details, navigates to the “Returns” tab and clicks “View / Edit Returns”. The reports are located under the Incident Reporting heading.



Click on the hyperlink for “DORA Major Incident Report”. This opens the report landing page where the user can load a file or view previously uploaded files.



Then navigate to “Returns” > “View / Edit Returns” > “DORA Major Incident Report” > “Load File”.



The Load a File screen allows the user to submit a DORA major incident report to the Central Bank.

**It is important to note that multiple reports will most likely be submitted for the same incident. Section 5.1.3 below provides information on how to name the first submission of an incident and how to link reports back to the first submission using the naming convention**

The elements of the Load a File screen above are explained as follows:

**1. First file being submitted for this incident**

This is a pre-ticked box which indicates that this is the first report being submitted in respect of an incident. As the box is pre-ticked upon loading the screen, no action is required.

Unticking the box allows the user to submit additional reports related to the first submission.

Note: if it is the first incident report being submitted, the tick box will not appear (as no previous submissions have been made).

## 2. Submission Type

When the user is submitting the first report for an incident, the relevant submission type of “Initial notification”, “Intermediate report” or “Final report” can be selected from the dropdown options.

## 3. Choose File

Pressing the “Choose File” button opens the user’s file explorer. From here, the relevant populated reporting template can be selected. As already noted, the reporting templates are available on the Central Bank’s website.

## 4. Load File

Where the reporting template adheres to the naming conventions (please section 5.1.3 for more details) and appears beside “Choose File,” click on the “Load File” button.

## 5. Cancel

Clicking on the “Cancel” button returns the user to the DORA Major Incident Report Portal screen.

### 5.1.3 Naming Convention for the DORA Major Incident Report

As per point 6 on the screenshot above, the reporting template must adhere to the following naming convention:

**CCCCCCC\_YYYYMMDD\_DIR\_n.xlsx(zip)**

Where:

**CCCCCCC** – is the financial entity’s C code.

(Note – this is the numerical section of the financial entity’s number preceded by “C” and NOT the institution number. Where the institution number is CBI0012345, the C Code will be C12345).

**YYYYMMDD** – is the date of the incident.

**DIR** – is the return code for DORA incident reports.

**n** – is the numeric identifier for the incident being reported on a given day. The first incident being reported in the day must use 1. This allows for more than one incident to be reported where such an incident occurs on the same date as another reported incident.

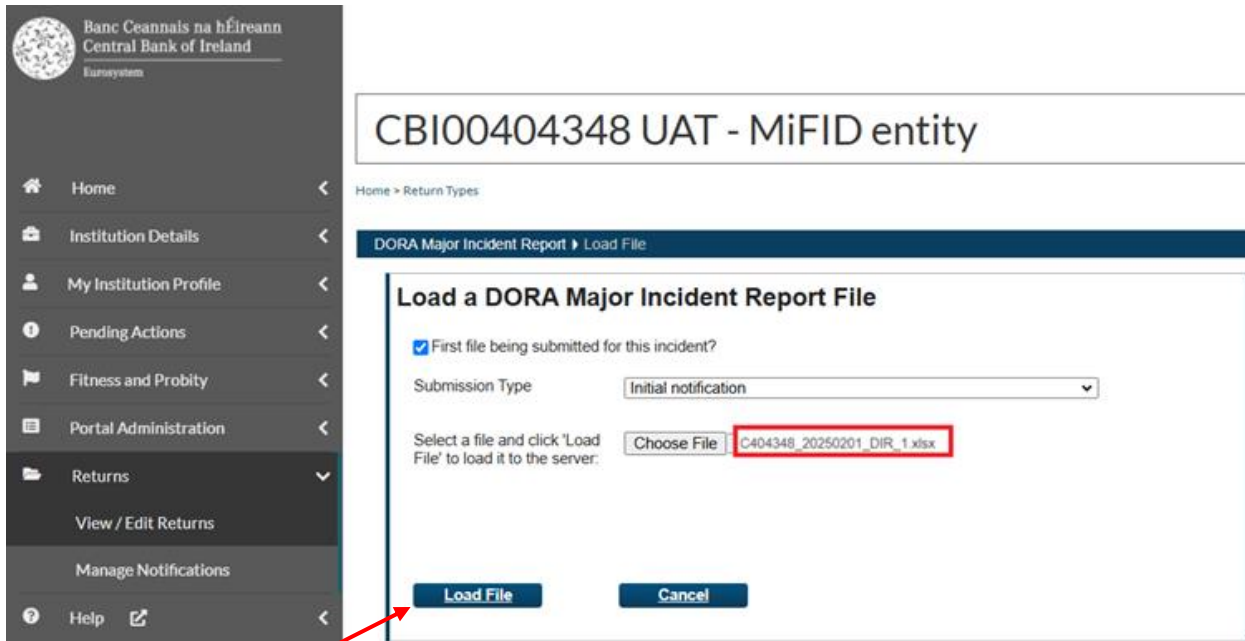
**xlsx(zip)** – is the file extension (.xlsx or .zip).

By way of example, if an incident occurred on 1 February 2025 in the institution CBI0012345 (and is the first incident to happen on that day), the reporting template should be named as follows:

**C12345\_20250201\_DIR\_1.xlsx**

### 5.1.4 Submission of a DORA Major Incident Report on the Portal

When the reporting template is chosen from the file explorer, it appears on screen as below.

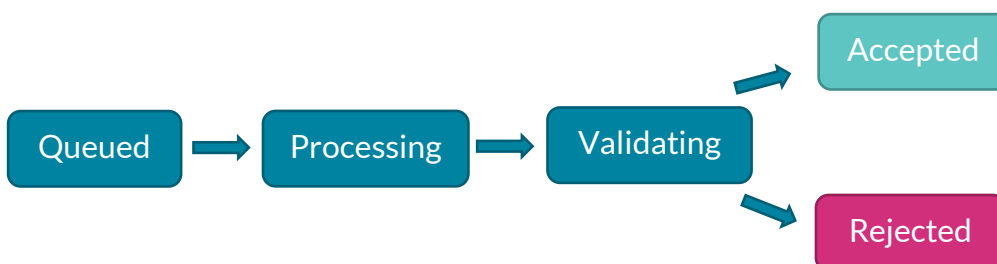


Select "Load File".

The File Upload Status screen appears as below.



The initial "File Status" appears as "Queued". The status progresses through the following identifiers:



Progressing through these identifiers is automatic and can be quick to the extent that they may only appear briefly on screen.

Website traffic depending, the majority of reports should be processed within five minutes.

### DORA Major Incident Report

File name:	C404348_20250201_DIR_1.xlsx
File status:	<b>Validating</b>
File size:	140876 bytes
Upload date:	23-Oct-2024 (09:54)
Processed date:	23-Oct-2024 (09:55)
Incident reference code:	C404348_20250201_1

[Back](#) [Refresh page](#)

Clicking on “Refresh Page” updates the user on the current file status.

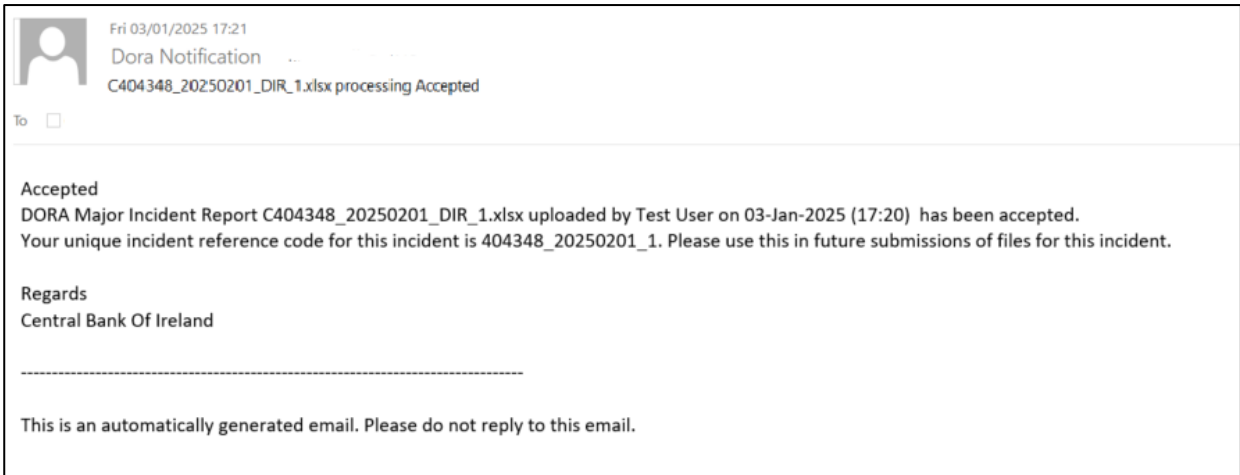
Upon the successful completion of the uploading process, the file status appears as “Accepted” and the processed date displayed.

### DORA Major Incident Report

File name:	C404348_20250201_DIR_1.xlsx
File status:	<b>Accepted</b>
File size:	140876 bytes
Upload date:	22-Oct-2024 (14:58)
Processed date:	<b>22-Oct-2024 (14:59)</b>
Incident reference code:	C404348_20250201_1

[Back](#) [Refresh page](#)

The user also receives a confirmation email detailing the outcome of the submission. This email is sent to the address that the user has registered with the Portal, and is only sent to the user that has submitted the report. An example of such a confirmation email is set out below.



On the Portal upload screen, clicking on “Back”, redirects the user to the “View Uploaded Files” screen, where the user can view all previously uploaded files, the submission type, who uploaded the file, date of upload and the status.

### DORA Major Incident Report

**File name:** C404348\_20250201\_DIR\_1.xlsx

**File status:** **Accepted**

**File size:** 140876 bytes

**Upload date:** 22-Oct-2024 (14:58)

**Processed date:** 22-Oct-2024 (14:59)

**Incident reference code:** C404348\_20250201\_1

Back
Refresh page

Banc Ceannais na hÉireann  
Central Bank of Ireland  
Eunessystem

- Home <
- Institution Details <
- My Institution Profile <
- Pending Actions <
- Fitness and Probity <
- Portal Administration <
- Returns >
  - View / Edit Returns
  - Manage Notifications
- Help <

## CBI00404348 UAT - MiFID entity

Home > Return Types

DORA Major Incident Report > View Files

### DORA Major Incident Report Files

File Name	Submission Type	Loaded By	Load Date	Processed Date	Status
C404348_20250303_DIR_1.xlsx	Final Report	JJ MottProposer	05-Nov-2024 (11:19)	05-Nov-2024 (11:20)	Rejected
C404348_20250302_DIR_1.xlsx	Final Report	JJ MottProposer	05-Nov-2024 (11:09)	05-Nov-2024 (11:10)	Accepted
C404348_20250301_DIR_1.xlsx	Intermediate Report	JJ MottProposer	06-Nov-2024 (09:14)	06-Nov-2024 (09:15)	Rejected
C404348_20250301_DIR_1.xlsx	Initial Notification	JJ MottProposer	06-Nov-2024 (09:13)	06-Nov-2024 (09:14)	Accepted
C404348_20250301_DIR_1.xlsx	Initial Notification	JJ MottProposer	05-Nov-2024 (18:25)	05-Nov-2024 (18:27)	Rejected
C404348_20250301_DIR_1.xlsx	Initial Notification	JJ MottProposer	05-Nov-2024 (18:23)	05-Nov-2024 (18:24)	Rejected
C404348_20250601_DIR_1.xlsx	Initial Notification	JJ MottProposer	05-Nov-2024 (18:06)	05-Nov-2024 (18:07)	Rejected
C404348_20250205_DIR_1.xlsx	Intermediate Report	JJ MottProposer	30-Oct-2024 (16:52)	30-Oct-2024 (16:52)	Rejected

Back to “Checklist”

The user can also access this screen from the main DORA Major Incident Report page.

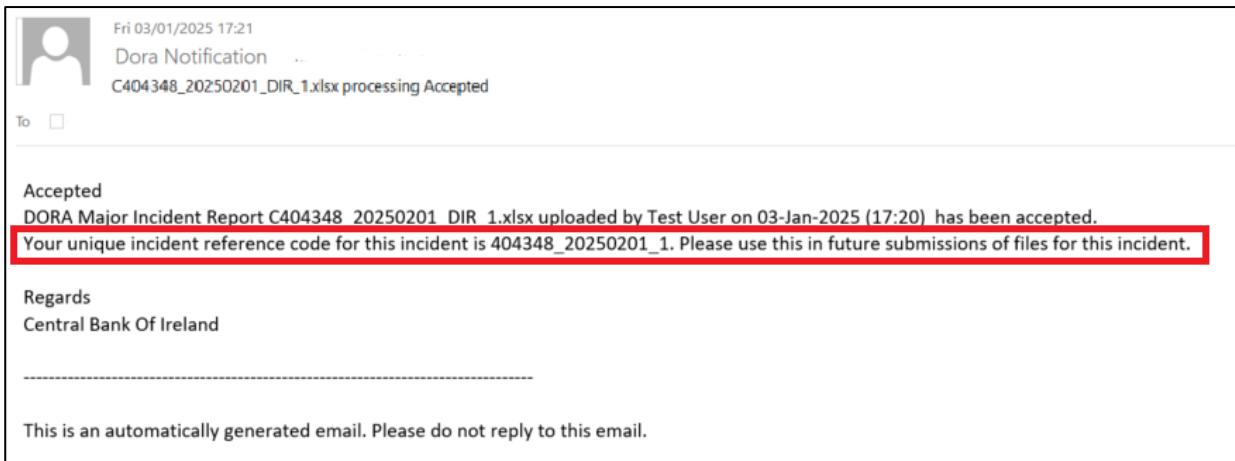


### 5.1.5 Incident Reference Code

The incident reference code is a unique reference code used to identify a major incident and is based on the naming convention for incident reports.

Upon the successful uploading of an initial notification on the Portal, the incident reference code is provided on the screen as per the below. This code is also included in the confirmation email sent to the user.





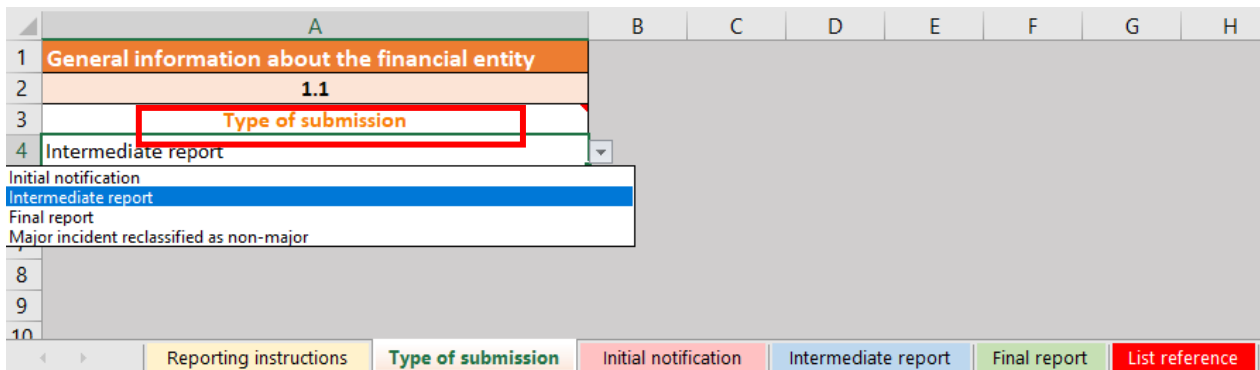
It is important to take note of the incident reference code as it is required when populating the intermediate or final reports (field 3.1 of the reporting template).

## 5.2 How to submit an Intermediate DORA Major Incident Report

### 5.2.1 Complete the Reporting Template

As already noted, the reporting templates are available on the DORA webpage of the Central Bank's website.

For field 1.1 of the DORA incident reporting template, ensure that type of submission selected is "Intermediate report".



Populate the relevant incident reference code in field 3.1 of the reporting template, as per the screenshot on the following page. As outlined in section 5.1.5 above, the incident reference code is displayed on the Portal upload screen for the initial notification, and is included in the confirmation email sent to the user following the successful submission of the initial notification on the Portal.

If you need to retrieve this code again, on the Portal navigate to: "Returns" > "View/Edit Returns" > "DORA Major Incident Report" > "View Uploaded Files" > Select the file.

#### KEY POINT TO NOTE

When inputting the incident reference code, do not copy and paste directly from the Portal webpage. First, copy to a word doc or notepad and then copy and paste from there. This is to avoid locking a cell on the reporting template.



Content of the intermediate report						
3.1	3.2	3.3	3.4	3.5	3.6	3.7
Incident reference code provided by the competent authority	Date and time of occurrence of the incident	Date and time when services, activities or operations have been recovered	Number of clients affected	Percentage of clients affected	Number of financial counterparts affected	Percentage of financial counterparts affected

Reporting instructions | Type of submission | Initial notification | **Intermediate report** | Final report | List reference

Ensure that all mandatory and conditional mandatory fields for the intermediate report are populated in the reporting template, and that name of same adheres to the naming convention (see section 5.1.3 above for more details).

### 5.2.2 Submit the Intermediate Report on the Portal

When submitting an intermediate report on the Portal, navigate to “Returns” > “View / Edit Returns” > “DORA Major Incident Report” > “Load File”.

As the intermediate report is typically not the first report submitted in response to a specific major incident,<sup>3</sup> (i.e. it is a follow-up report to the initial notification that has already been submitted), the user unticks the relevant box on the Portal screen as set out below.

<sup>3</sup> In a small number of cases where major incidents are quickly resolved, the intermediate or final report may be the first report submitted.

## DORA Major Incident Report ▶ Load File

## Load a DORA Major Incident Report File

 First file being submitted for this incident?Submission Reference Submission Type Select a file and click 'Load File' to load it to the server:  No file chosen

A dropdown menu option appears in respect of the Submission Reference.

When this dropdown is selected, a list of previously submitted reports is provided in descending order.

CBI00404348 UAT - MiFID entity

[Home](#) > [Return Types](#)

## DORA Major Incident Report ▶ Load File

## Load a DORA Major Incident Report File

 First file being submitted for this incident?

Submission Type

Select a file and click 'Load File' to load it to the server:

  
C404348\_20250302\_DIR\_1  
C404348\_20250301\_DIR\_1  
C404348\_20250206\_DIR\_1  
C404348\_20250205\_DIR\_1  
C404348\_20250203\_DIR\_1  
C404348\_20250202\_DIR\_1  
**C404348\_20250201\_DIR\_1**  
C404348\_20250102\_DIR\_1  
C404348\_20250101\_DIR\_1

Choose the desired report reference (the example above shows the selection of the report submitted previously in the guidance - C404348\_20250201\_DIR\_1, i.e. an incident that occurred on 1 February 2025).

When submitting a subsequent report, always choose the report reference that is associated with the incident on the original date that the incident occurred.

[Back to "Checklist"](#)

Next, choose “Intermediate report” as the Submission Type.

CBI00404348 UAT - MiFID entity

Home > Return Types

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

C404348\_20250201\_DIR\_1

Submission Type

Intermediate report

Select a file and click 'Load File' to load it to the server:

Initial notification

Intermediate report

Final report

Major incident reclassified as non-major

Load File

Cancel

Click on the “Choose File” button and select the relevant populated reporting template to be uploaded.

Ensure that the name of this file matches the report reference.

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

C404348\_20250201\_DIR\_1

Submission Type

Intermediate report

Select a file and click 'Load File' to load it to the server:

Choose File C404348\_20250201\_DIR\_1.xlsx

Load File

Cancel

Next, click on “Load File”.

The file status of the intermediate report then progresses through the status identifiers. When accepted, the intermediate report is displayed as a successfully uploaded file on the Portal and the user receives a confirmation email (see section 5.1.4 above for more information).

Back to “Checklist”

## 5.3 How to submit a Final DORA Major Incident Report

### 5.3.1 Complete the Reporting Template

As already noted, the reporting templates are available on the DORA webpage of the Central Bank's website.

For field 1.1 of the DORA incident reporting template, ensure that type of submission selected is "Final report".

The screenshot displays a spreadsheet interface for the DORA reporting template. The columns are labeled A through H. Row 1 is titled "General information about the financial entity". Row 2 contains the field identifier "1.1". Row 3 is labeled "Type of submission" and is highlighted with a red box. Row 4 shows a dropdown menu with the following options: "Final report", "Initial notification", "Intermediate report", "Final report", and "Major incident reclassified as non-major". The "Final report" option is selected and highlighted in blue. At the bottom of the spreadsheet, there is a navigation bar with several tabs: "Reporting instructions", "Type of submission" (highlighted with a red box), "Initial notification", "Intermediate report", "Final report", and "List reference".

Ensure that all mandatory and conditional mandatory fields for the final report are populated in the reporting template, and that name of same adheres to the naming convention (see section 5.1.3 above for more details).

### 5.3.2 Submit the Final Report on the Portal

When submitting the final report on the Portal, the process is similar to that of the intermediate report outlined above in section 5.2.

On the Portal, navigate to "Returns" > "View / Edit Returns" > "DORA Major Incident Report" > "Load File".

As the final report is typically not the first report submitted in response to a specific major incident, (i.e. it is a follow-up report to the initial notification and intermediate report that may have been submitted already), the user unticks the relevant box on the Portal screen as set out below.

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference: C404348\_20250201\_DIR\_1

Submission Type: Final report

Select a file and click 'Load File' to load it to the server:  No file chosen

A dropdown menu option appears in respect of the Submission Reference.

When the dropdown is selected, a list of previously submitted reports is provided in descending order.

CBI00404348 UAT - MiFID entity

Home > Return Types

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

**Submission Reference**

Submission Type

Select a file and click 'Load File' to load it to the server:

- C404348\_20250206\_DIR\_1
- C404348\_20250302\_DIR\_1
- C404348\_20250301\_DIR\_1
- C404348\_20250206\_DIR\_1
- C404348\_20250205\_DIR\_1
- C404348\_20250203\_DIR\_1
- C404348\_20250202\_DIR\_1
- C404348\_20250201\_DIR\_1**
- C404348\_20250102\_DIR\_1
- C404348\_20250101\_DIR\_1

Choose the desired Submission Reference (the example above shows the selection of the report submitted previously in the guidance – C404348\_20250201\_DIR\_1, i.e. an incident that occurred on 1 February 2025.)

**When submitting a subsequent report, always choose the report reference that is associated with the incident on the original date that the incident occurred.**

Next, choose “Final report” as the Submission Type.

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference: C404348\_20250201\_DIR\_1

Submission Type: Final report

Select a file and click 'Load File' to load it to the server:

Final report

Initial notification

Intermediate report

Final report

Major incident reclassified as non-major

Load File Cancel

Click on the “Choose File” button and select the relevant populated reporting template to be uploaded.

Ensure that the name of this file matches the submission reference.

DORA Major Incident Report ▶ Load File

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference: C404348\_20250201\_DIR\_1

Submission Type: Final report

Select a file and click 'Load File' to load it to the server:

Choose File C404348\_20250201\_DIR\_1.xlsx

Load File Cancel

Next, click on “Load File”.

The file status of the final report then progresses through the status identifiers. When accepted, the final report is displayed as a successfully uploaded file on the Portal and the user receives a confirmation email (see section 5.1.4 above for more information).

## 5.4 How to Reclassify a Major Incident as Non-major

### 5.4.1 Complete the Reporting Template

Where a major incident report has been successfully submitted on the Portal, but upon further assessment by the impacted financial entity it is determined that the incident reported as major at no time fulfilled the required classification criteria and materiality thresholds, the financial entity submits a major incident reclassified as non-major report.

As already noted, the reporting templates are available on the DORA webpage of the Central Bank’s website.

For field 1.1 of the DORA incident reporting template, ensure that type of submission selected is “Major incident reclassified as non-major”.

The screenshot shows a spreadsheet interface for the reporting template. Row 1 is titled 'General information about the financial entity'. Row 2 is labeled '1.1'. Row 3 is labeled 'Type of submission'. Row 4 shows a dropdown menu with the selected option 'Major incident reclassified as non-major'. Below the dropdown, a list of options is visible: 'Initial notification', 'Intermediate report', 'Final report', and 'Major incident reclassified as non-major'. At the bottom of the spreadsheet, a navigation bar contains buttons for 'Reporting instructions', 'Type of submission', 'Initial notification', 'Intermediate report', 'Final report', and 'List reference'. The 'Type of submission' button is highlighted with a red box.

Ensure that all mandatory and conditional mandatory fields for the major incident reclassified as non-major report are populated in the reporting template. For instance, in field 2.10 of the reporting template, the financial entity must provide a description of the reasons why the incident does not fulfil the criteria to be considered a major incident.

The screenshot shows a table with three columns. The first column is labeled '2.8' and contains the text 'Indication whether the incident originates from a third party provider or another financial entity'. The second column is labeled '2.9' and contains the text 'Activation of business continuity plan, if activated'. The third column is labeled '2.10' and contains a text box with the instruction 'Enter major incident reclassified as non-major details here'. The text box is highlighted with a red box. At the bottom of the spreadsheet, a navigation bar contains buttons for 'Reporting instructions', 'Type of submission', 'Initial notification', 'Intermediate report', 'Final report', and 'List reference'. The 'Initial notification' button is highlighted with a red box.

### 5.4.2 Submit the Major Incident Reclassified as Non-major Report on the Portal

When submitting the major incident reclassified as non-major report on the Portal, the process is similar to that of the initial notification, intermediate report and final report outlined in the preceding sections.

On the Portal, navigate to “Returns” > “View/Edit Returns” > “DORA Major Incident Report” > “Load File”.

As the major incident reclassified as non-major report is not the first report being submitted relating to a specific major incident, i.e. it is a follow-up report, the user unticks the relevant box on the Portal screen as set out below.

DORA Major Incident Report ▶ Load File

#### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

Submission Type

Select a file and click 'Load File' to load it to the server:  No file chosen

A dropdown menu option appears in respect of the Submission Reference.

When the dropdown is selected, a list of previously submitted reports is provided in descending order.



# CBI00404348 UAT - MiFID entity

Home > Return Types

DORA Major Incident Report ▶ Load File

## Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

Submission Type

Select a file and click 'Load File' to load it to the server.

Load File

C404348\_20250206\_DIR\_1

C404348\_20250302\_DIR\_1

C404348\_20250301\_DIR\_1

C404348\_20250206\_DIR\_1

C404348\_20250205\_DIR\_1

C404348\_20250203\_DIR\_1

C404348\_20250202\_DIR\_1

C404348\_20250201\_DIR\_1

C404348\_20250102\_DIR\_1

C404348\_20250101\_DIR\_1

Choose the desired Submission Reference (the example above shows the selection of the report submitted previously in the guidance – C404348\_20250201\_DIR\_1, i.e. an incident that occurred on 1 February 2025).

**When submitting a subsequent report, always choose the report reference that is associated with the incident on the original date that the incident occurred.**

Next, choose “Major incident reclassified as non-major” as the Submission Type.

Back to “Checklist”

# CBI00404348 UAT - MiFID entity

Home > Return Types

DORA Major Incident Report ▶ Load File

## Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

Submission Type

Select a file and click 'Load File' to load it to the server:

Initial notification  
Intermediate report  
Final report  
Major incident reclassified as non-major

Load File

Cancel

Click on the “Choose File” button and select the relevant populated reporting template to be uploaded.

Ensure that the name of this file matches the submission reference.

DORA Major Incident Report ▶ Load File

## Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Reference

Submission Type

Select a file and click 'Load File' to load it to the server:

Choose File

Load File

Cancel

Next, click on “Load File”.

Back to “Checklist”

The file status of the major incident reclassified as non-major report then progresses through the status identifiers. When accepted, the major incident reclassified as non-major report is displayed as a successfully uploaded file on the Portal and the user receives a confirmation email (see section 5.1.4 above for more information).

## 5.5 Submitting a DORA Major Incident Report where there are two (or more) separate incidents on the same day

As outlined earlier in section 5.1.3 of the guidance, the reporting template should adhere to the following naming convention:

CCCCCC\_YYYYMMDD\_DIR\_n.xlsx(zip)

The “n” is the numeric identifier for the incident report being uploaded on a given day.

E.g. If an incident occurred on 1 February 2025 in the financial entity CBI0012345, (and is the first incident) the reporting template should be saved as follows:

C12345\_20250201\_DIR\_1.xlsx

Here, “1” denotes that this is the first incident on this day for this financial entity.

If another, separate incident occurs in this financial entity later on this day (1 February 2025), which is not connected to the first incident, the “n” notation will be 2.

E.g. C12345\_20250201\_DIR\_2.xlsx

The screenshot shows a web interface for loading a DORA Major Incident Report file. At the top, there is a dark blue header with the text "DORA Major Incident Report ▶ Load File". Below this is a white box with a dark blue border containing the following elements:

- Load a DORA Major Incident Report File** (Section Header)
- First file being submitted for this incident?
- Submission Type: Initial (dropdown menu)
- Select a file and click 'Load File' to load it to the server: Choose File C404348\_20250201\_DIR\_2.xlsx (file name highlighted in a red box)
- Buttons: Load File and Cancel

It is important to note that the “n” notation does not reflect an initial notification, intermediate report or final report. It reflects that another separate incident(s) has occurred on the same day.

## 5.6 Common Validation Errors

The examples shown thus far in the guidance regarding the submission of DORA major incident reports on the Portal are ones that have been successfully submitted.

However, there may be instances where the submission of a report is rejected, or the user encounters errors when trying to upload a report on the Portal.

In order to avoid common validations errors, it is important to note the following:

1. Ensure that the C Code is correct and a capital C is used. In the below example, a lower case C is used, which results in an error message being displayed on the Portal screen.

DORA Major Incident Report ▶ Load File

---

### Load a DORA Major Incident Report File

First file being submitted for this incident?

Submission Type: Initial notification

Select a file and click 'Load File' to load it to the server: Choose File No file chosen

Institution Code 'c404348' is invalid.

Load File
Cancel

2. Ensure that the type of submission selected in field 1.1 (cell A4) of the reporting template matches the submission type selected on the Portal. In the below example, the submission types selected on the Portal and reporting template do not match, which results in an error message being displayed.

### DORA Major Incident Report

File name:	C404348_20250702_DIR_1.xlsx
File status:	Rejected
File size:	141377 bytes
Upload date:	07-Jan-2025 (15:26)
Processed date:	07-Jan-2025 (15:26)
Incident reference code:	C404348_20250702_1

Validation errors

Worksheet 'Type of submission', column 'Type of submission' cell 'A4' the Submission Type selected on screen does not match the Type of submission specified in the file

Back
Refresh page

# 6 Significant Cyber Threat Reporting

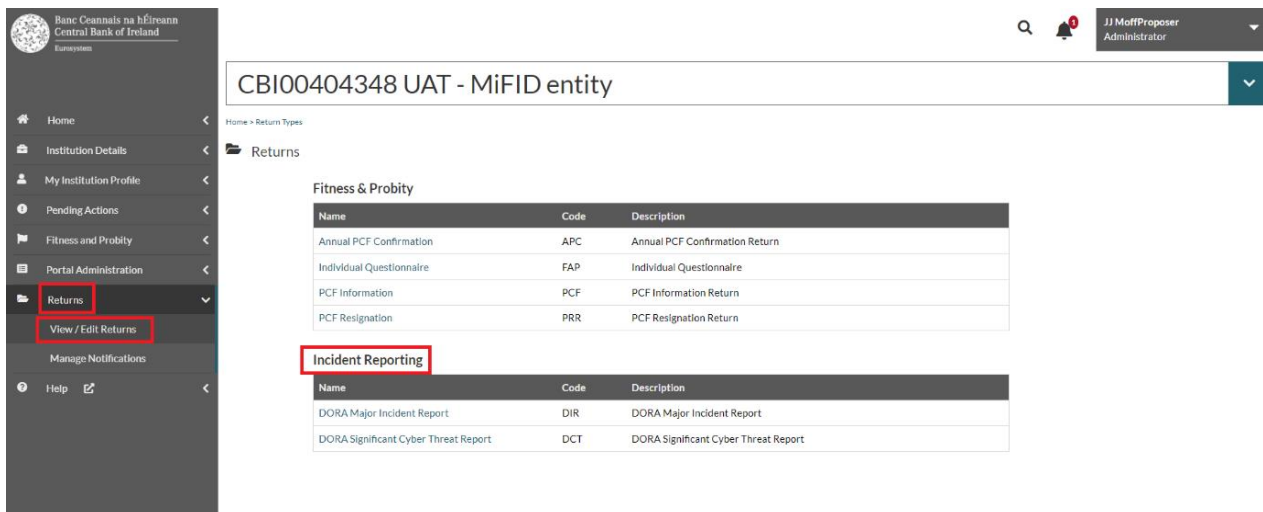
## 6.1 Complete the Reporting Template

As already noted, the reporting templates are available on the DORA webpage of the Central Bank’s website.

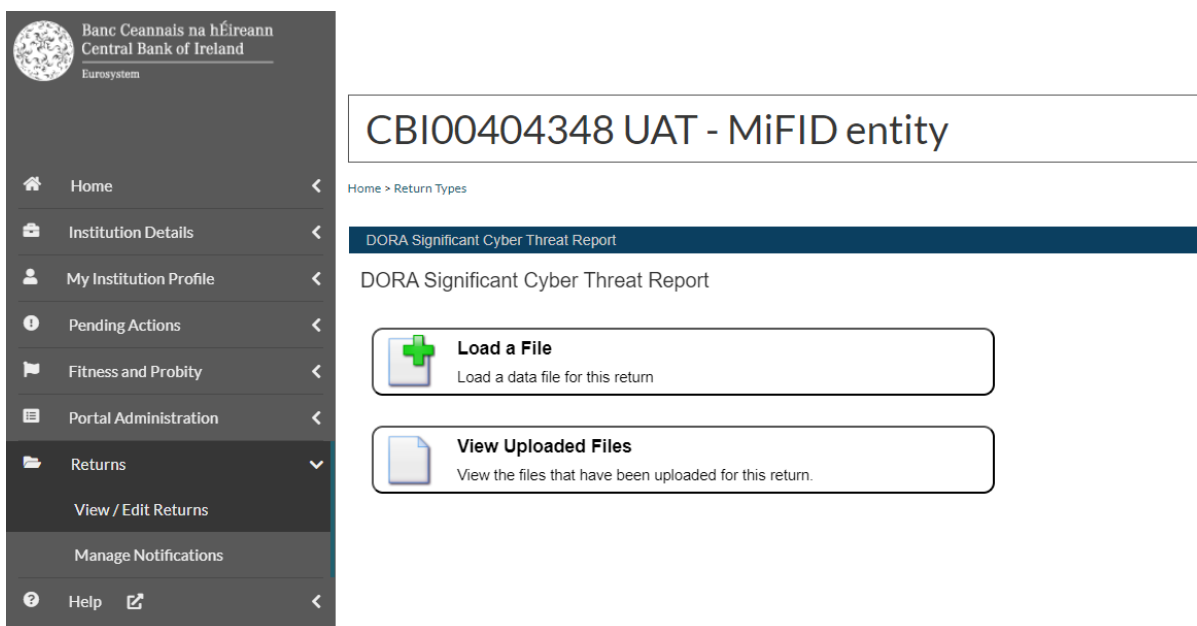
For the DORA significant cyber threats reporting template, ensure that all mandatory and conditional mandatory fields are populated in the reporting template, and that name of same adheres to the naming convention (see section 6.3 below for more details).

## 6.2 Submit a DORA Significant Cyber Threat on the Portal

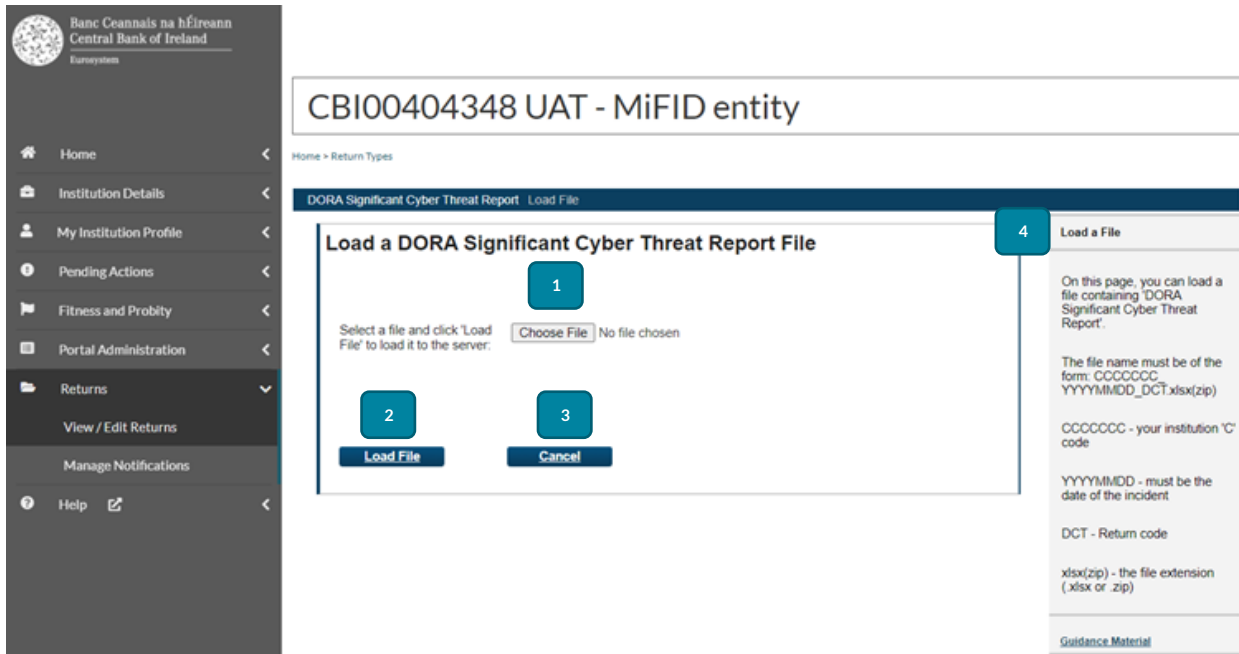
To submit a DORA significant cyber threat report, the user logs-in to the Portal with their user details, navigates to the “Returns” section and clicks “View/Edit Returns”. The reports are located under the Incident Reporting heading.



Click on the hyperlink for “DORA Significant Cyber Threat Report”. This opens the report landing page where the user can load a file or view previously uploaded files.



Then navigate to “Returns” > “View/Edit Returns” > “DORA Significant Cyber Threat Report” > “Load File”.

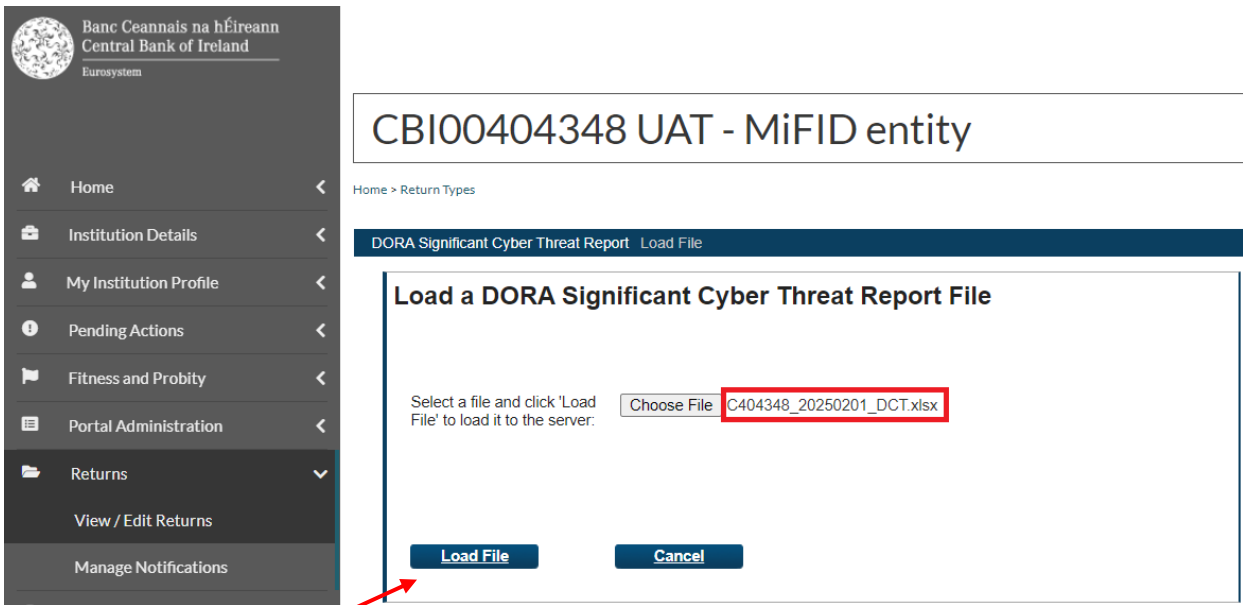


The Load a File screen allows the user to submit a DORA significant cyber threat report to the Central Bank.

The elements of the Load a File screen above are explained as follows:

1. Pressing the “Choose File” button opens the user’s File Explorer. From here the relevant populated reporting template can be selected.
2. When the reporting template appears beside “Choose File,” click on the “Load File” button.
3. Clicking on the “Cancel” button returns the user to the DORA significant cyber threat report Portal screen.
4. Ensure that the reporting template adheres to the naming convention (please see section 6.3 for more details).

When the reporting template is chosen from the file explorer, it appears on the Portal screen as below.

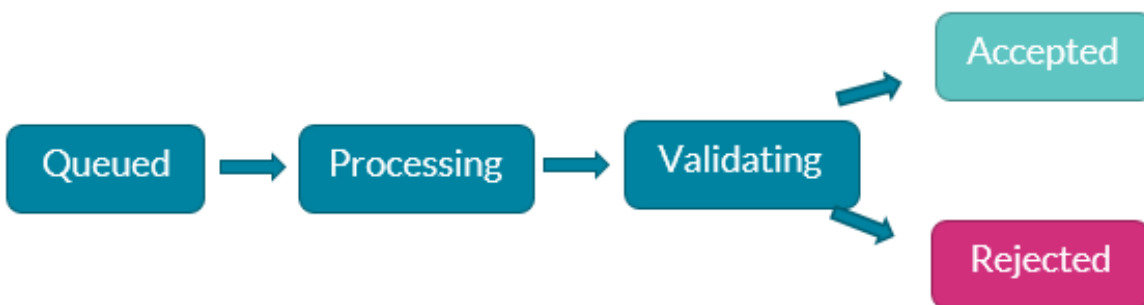


Select "Load File".

The File Upload Status screen appears as below.



The initial "File Status" is "Queued." The status progresses through the following identifiers:



Progressing through these identifiers is automatic and can be quick to the extent that they may only appear briefly on screen.


Website traffic depending, the majority of reports should be processed within 5 minutes.

DORA Significant Cyber Threat Report View Files ▶ 6ad7a27d-7297-ef11-81a9-005056872d79

### DORA Significant Cyber Threat Report

File name:	C404348_20250201_DCT.xlsx
File status:	<b>Queued</b>
File size:	80489 bytes
Upload date:	31-Oct-2024 (10:25)
Processed date:	N/A

[Back](#) [Refresh page](#)



Clicking “Refresh Page” updates the user on the current file status.

Upon the successful completion of the uploading process, the file status appears as “Accepted” and the processed date displayed.

DORA Significant Cyber Threat Report View Files ▶ c58cbb92-b197-ef11-81a9-005056872d79

### DORA Significant Cyber Threat Report

File name:	C404348_20250201_DCT.xlsx
File status:	<b>Accepted</b>
File size:	80506 bytes
Upload date:	31-Oct-2024 (17:57)
Processed date:	31-Oct-2024 (17:57)

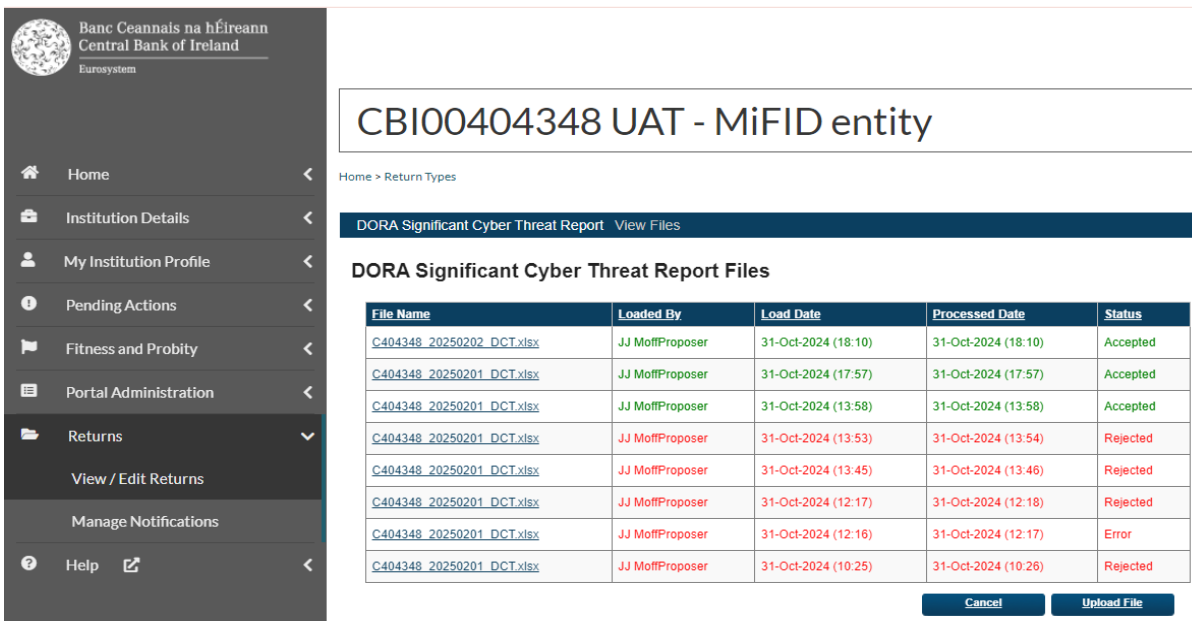
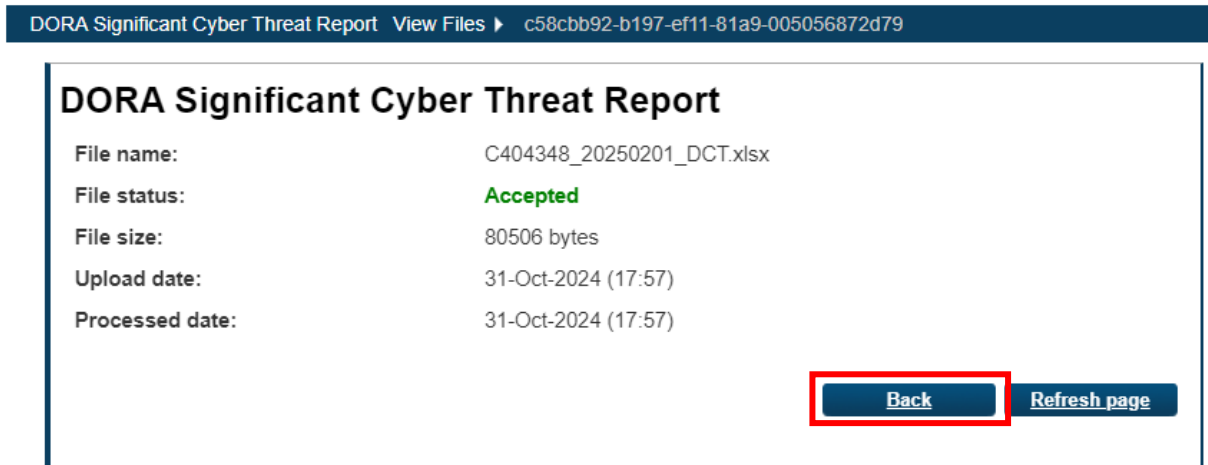
[Back](#) [Refresh page](#)

The user also receives a confirmation email detailing the outcome of the submission. The email is sent to the address which the user has registered with the Portal, and is only sent to the user that has submitted the DORA significant cyber threat report. An example of the confirmation email is set out below.





On the Portal upload screen, clicking on “Back”, redirects the user to the “View Uploaded Files” screen, where the user can view all previously uploaded files, the submission type, who uploaded file, date of upload and the status. The user can also access this page from the main DORA Significant Cyber Threat Report page.



Back to “Checklist”

## 6.3 Naming Convention for the DORA Significant Cyber Threat Report

The reporting template must adhere to the following naming convention:

**CCCCCCC\_YYYYMMDD\_DCT.xlsx(zip)**

Where:

**CCCCCCC** – is the financial entity’s C code.

(NOTE – this is the numerical section of the financial entity’s number preceded by “C” and NOT the institution number. Where the institution number is CBI0012345, your C Code will be C12345).

**YYYYMMDD** – is the date of the incident.

**DCT** – is the return code for DORA cyber threat reports.

**xlsx(zip)** - is the file extension (.xlsx or .zip).

By way of example, if the detection of a significant cyber threat occurred on 1 February 2025 in financial entity CBI0012345, the reporting template should be named as follows:

**C12345\_20250201\_DCT.xlsx**

## 7 FAQ

### 7.1 What happens if I get an error message on the Portal when uploading a report?

#### DORA Significant Cyber Threat Report

File name:	C404348_20250201_DCT.xlsx
File status:	<b>Error</b>
File size:	80490 bytes
Upload date:	31-Oct-2024 (12:16)
Processed date:	31-Oct-2024 (12:17)

[Back](#) [Refresh page](#)

An “Error” file status is different from a “Rejected” status. Please try to upload the report to the Portal again and if the error persists, contact the Central Bank helpline by emailing [onlinereturns@centralbank.ie](mailto:onlinereturns@centralbank.ie) or call 01 224 4545.

### 7.2 What do I do if I’m unable to access the Portal?

If you are experiencing technical issues with the Portal, please email [onlinereturns@centralbank.ie](mailto:onlinereturns@centralbank.ie) or call 01 224 4545.

For users not familiar with the Portal, information and related guidance documents are available on the Central Bank’s website at: <https://www.centralbank.ie/regulation/central-bank-portal>. The [Getting Started](#) Help section of the Central Bank’s website provides information on how to register for and log in to the Portal, including setting up second factor authentication.

If you are unable to submit an incident or significant cyber threat report, and/or are experiencing any other issues related to incident reporting, please contact your supervisory team in the Central Bank using existing communication channels.

Once any technical/operational issues have been resolved, the expectation is that the incident or significant cyber threat report will be submitted on the Portal as soon as practicable.

### 7.3 What do I do if my submission is rejected on the Portal?

The submission of a report may be rejected on the Portal for various reasons, including due to the non-entry of data in a mandatory field in the reporting template or where inconsistent submission types are selected in respect of the reporting template and Portal.

When a submission is rejected on the Portal, the user is presented with the validation errors and instructed as to what cell to amend in the reporting template to rectify the issue.

In the example set out below, the user did not enter data into a number of mandatory fields of the reporting template. To rectify this, the user needs to enter data into the fields of the reporting

template identified in the error message, and to upload the rectified reporting template to the Portal.

DORA Major Incident Report ▸ View Files ▸ a247d63e-e495-ef11-81a9-005056872d79

### DORA Major Incident Report

File name: C404348\_20250206\_DIR\_1.xlsx  
 File status: **Rejected**  
 File size: 141256 bytes  
 Upload date: 29-Oct-2024 (10:55)  
 Processed date: 29-Oct-2024 (10:55)  
 Incident reference code: C404348\_20250206\_1

**Validation errors**

Worksheet 'Initial notification', column 'Name of the entity submitting the report' is a mandatory field
Worksheet 'Initial notification', column 'Identification code of the entity submitting the report' is a mandatory field
Worksheet 'Initial notification', column 'LEI code of the financial entity affected' is a mandatory field
Worksheet 'Initial notification', column 'Primary contact person name' is a mandatory field
Worksheet 'Initial notification', column 'Primary contact person email' is a mandatory field
Worksheet 'Initial notification', column 'Primary contact person telephone' is a mandatory field
Worksheet 'Initial notification', column 'Second contact person name' is a mandatory field
Worksheet 'Initial notification', column 'Second contact person email' is a mandatory field

In the example set out below, the type of submission selected in field 1.1 (cell A4) of the reporting template does not match the submission type selected on the Portal, which results in an error message being displayed. To rectify this, the user needs to amend the type of submission selected in field 1.1 (cell A4) of the reporting template to match the submission type selected on the Portal, and upload the rectified reporting template to the Portal.

### DORA Major Incident Report

File name: C404348\_20250702\_DIR\_1.xlsx  
 File status: **Rejected**  
 File size: 141377 bytes  
 Upload date: 07-Jan-2025 (15:26)  
 Processed date: 07-Jan-2025 (15:26)  
 Incident reference code: C404348\_20250702\_1

**Validation errors**

Worksheet 'Type of submission', column 'Type of submission' cell 'A4' the Submission Type selected on screen does not match the Type of submission specified in the file

Back
Refresh page

In the example set out below, conditional mandatory fields in the intermediate report were not populated. These fields need to be populated in light of data provided in the initial notification. To rectify this, the user enters data into the conditional mandatory fields in the intermediate report that are identified in the error message, and uploads the rectified reporting template to the Portal.

### DORA Major Incident Report

**File name:** C404348\_20250301\_DIR\_1.xlsx

**File status:** Rejected

**File size:** 141442 bytes

**Upload date:** 06-Nov-2024 (09:14)

**Processed date:** 06-Nov-2024 (09:15)

**Incident reference code:** C404348\_20250301\_1

Validation errors

Worksheet 'Intermediate report', column 'Materiality thresholds for the classification criterion Data losses' is a conditional mandatory field
Worksheet 'Intermediate report', column 'Description of the data losses' is a conditional mandatory field

## 7.4 Can I make an update to my initial notification, intermediary report, or final report?

Yes, if the user has submitted an initial notification and it is accepted on the Portal, another initial notification can be submitted. Remember to untick the “First file being submitted for this incident” tick box on the Portal screen and upload the report with the same date. The same logic applies for the intermediate and final reports.

Note: reports do not need to be unlocked on the Portal.

## 7.5 I am unable to edit a cell in the reporting template

This can occur if data is copied and pasted from a webpage and entered into a cell of the reporting template. The user will see the below error message when they try to edit the cell.

	1.4	1.5	1.6	1.7
e ort	<b>Type of the affected financial entity</b>	<b>Name of the financial entity affected</b>	<b>LEI code of the financial entity affected</b>	<b>Primary contact person name</b>

Microsoft Excel

The cell or chart you're trying to change is on a protected sheet. To make a change, unprotect the sheet. You might be requested to enter a password.

If this occurs, you need to download a new reporting template from the Central Bank’s website and re-enter the data. The reporting template does not allow modifications to unprotected cells.

# Annex: Validation Rules

Validation Checks	Error Message
<b>General Checks</b>	
C code must be correct and using capital C - see section 5.6	Institution code 'C12345' is invalid
Filename must follow naming convention as outlined on screen - see section 5.1.3	File Format should be as follows: CCCCCC_YYYYMMDD_DIR_n.xlsx(zip) CCCCCC - your institution C-code YYYYMMDD - must be the date of the incident DIR - the DIR Return code n - numeric identifier xlsx - the file extension (.zip or .xlsx)
File type extension must be .xlsx or .zip - see section 5.1.3	File Format should be as follows: CCCCCC_YYYYMMDD_DIR_n.xlsx(zip) CCCCCC - your institution C-code YYYYMMDD - must be the date of the incident DIR - the DIR Return code n - numeric identifier xlsx - the file extension (.zip or .xlsx)
If the file extension is .zip it must contain .xlsx file	The compressed zip file doesn't contain allowed file type
File size must be less than 80MB	Uploaded file exceeds maximum permissible size of 80MB
<b>Reporting Template Checks</b>	
Published structured reporting template must be used	Multiple messages depending on structure alteration e.g.: The protected reporting template has been altered. The template text contained in worksheet '<tab name>', cell 'xn' is incorrect. Please use the reporting template that has been provided.
Submission Type selected on the Portal screen must match type of submission in selected in the reporting template - see sections 5.6 and 7.3	Worksheet 'Type of submission', column 'Type of submission' cell 'A4' the Submission Type selected on screen does not match the Type of submission specified in the file.
All fields must be completed in the reporting template using the correct type of data as specified in the Reporting Instructions tab of the template	Worksheet '<tab name>', '<column>' cell 'xn' + <text specific to the type of data to be captured>
All fields marked as mandatory in the Reporting Instructions tab of the reporting template must be completed - see section 7.3	Worksheet '<tab name>', column '<column name>' is a mandatory field
Fields marked as conditional mandatory "Yes, IF xyz" in the Reporting Instructions tab of the reporting template must be completed if the condition is met - see section 7.3	Worksheet '<tab name>', column '<column name>' is a conditional mandatory field
Either LEI or EU ID must be completed	Worksheet '<tab name>', column '<column name>' is a conditional mandatory field



Banc Ceannais na hÉireann  
Central Bank of Ireland

---

Eurosystem