INCIDENT REPORTING WITH CIRAS V2 MANUAL

Contents

CIRAS 2 Platform

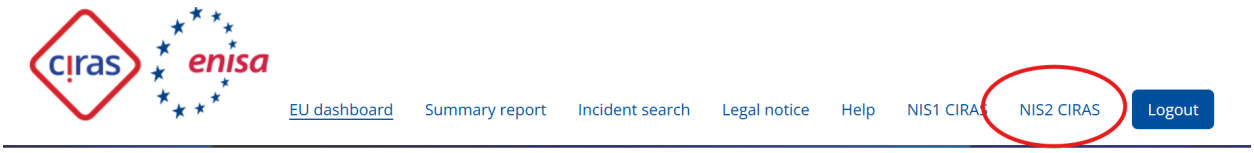
CIRAS 2 is evolution of CIRAS and follows the templates and the requirements set in NIS 2.

CIRAS page

https://ciras.enisa.europa.eu/

Accessing NIS 2 CIRAS

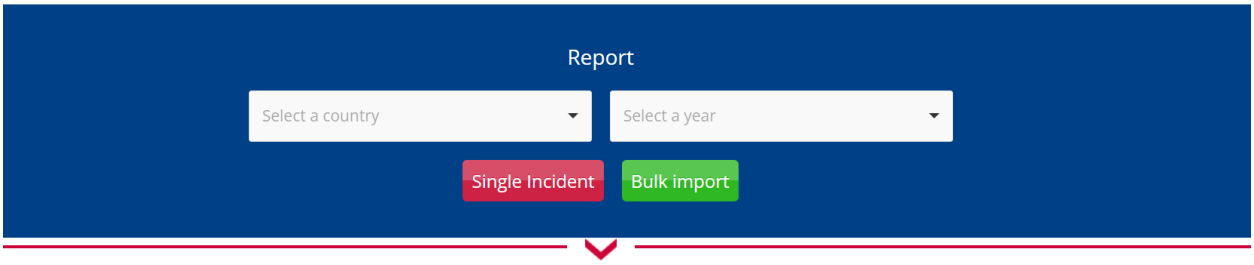
Go to CIRAS web page and click NIS 2 CIRAS, as indicated below.



Reporting process

A. Incident reporting process

Scroll down to until you reach the below picture



Select country and year for reporting and click start single incident or bulk import

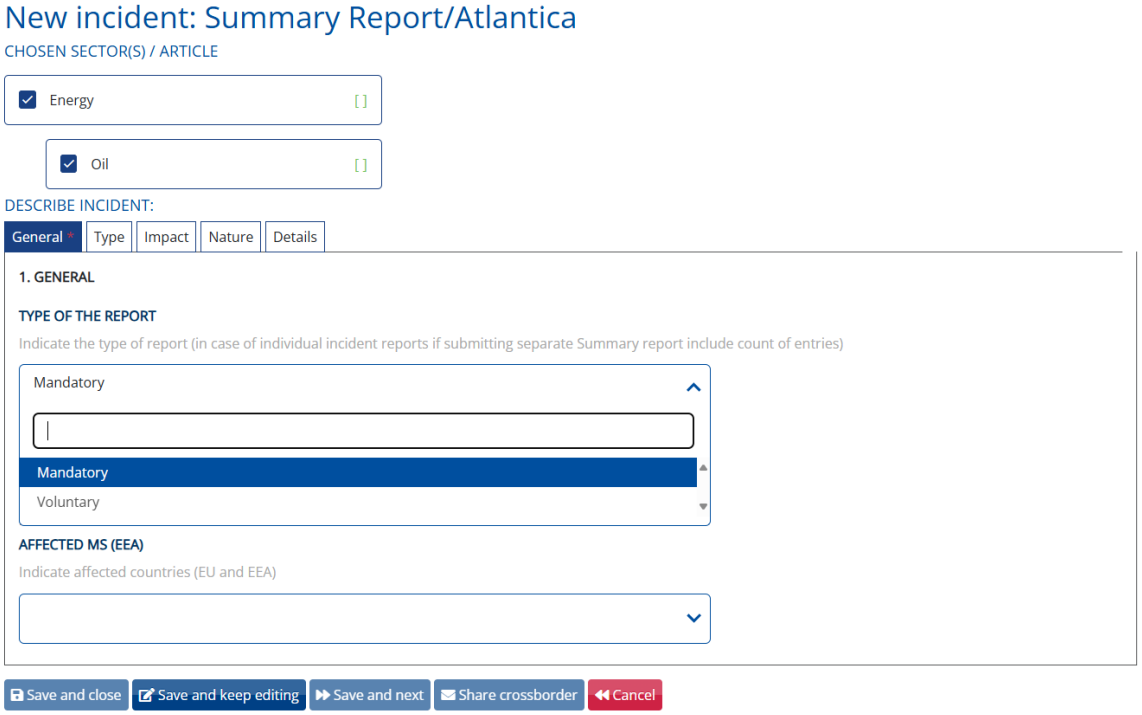
B. Single incident reporting procedure

All the sectors according to NIS 2 are available. In case a member state has more sectors to report on, please contact incidentreporting@enisa.europa.eu and we will add them for you.

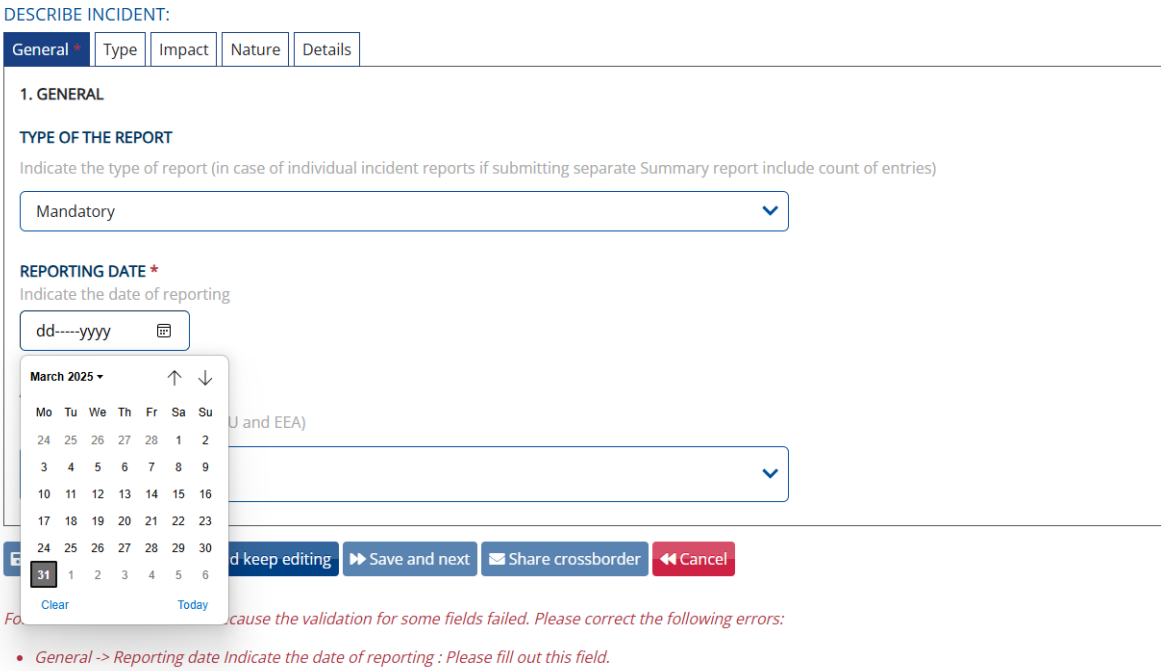
B.1. General TAB

B.1.1. Select the type of report

Options are: Voluntary or Mandatory. Only one option can be selected.

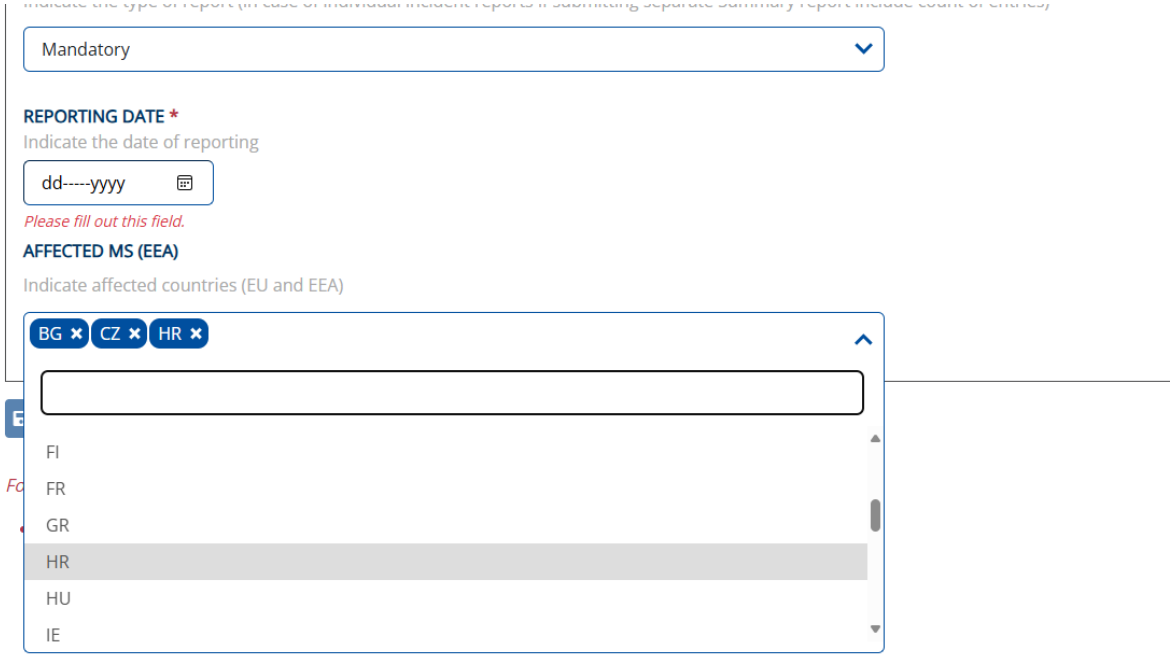


B.1.2. Select date



B.1.3. Select affected countries

Multiple countries can be selected

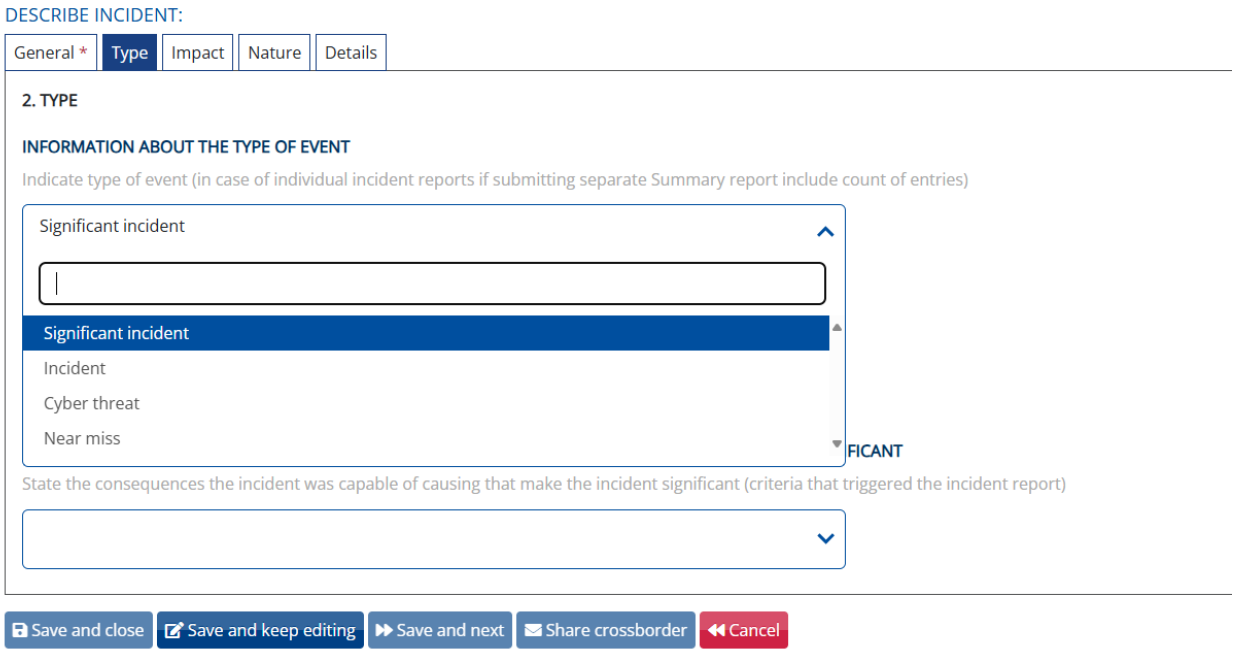


B.2. Incident type TAB

Information about the type of incident

Only one option can be selected.

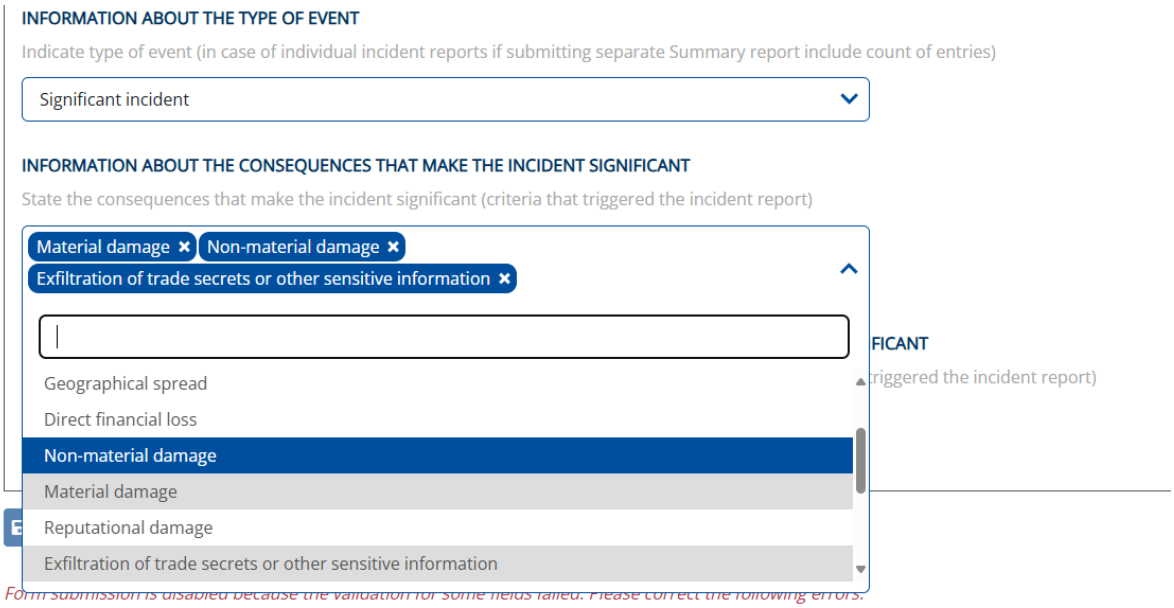
Based on this the other tabs IMPACT and NATURE might disappear.



B.2.1. Steps for significant incident

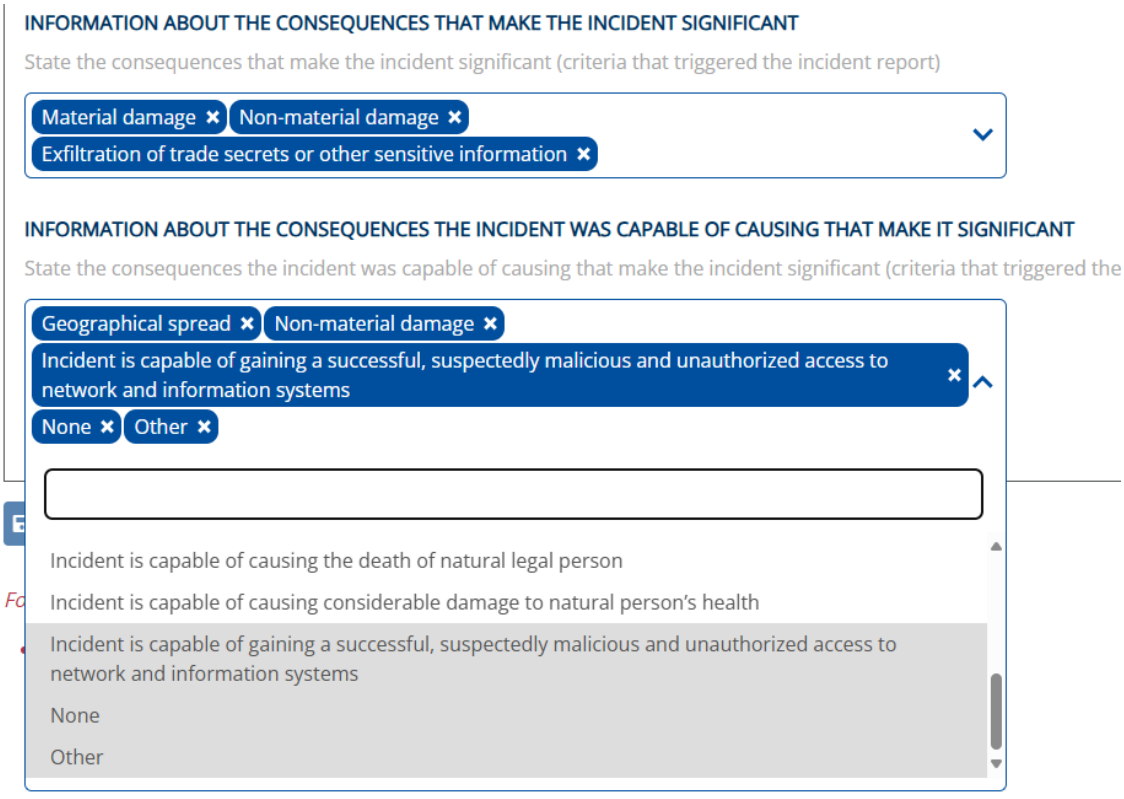
B.2.1.1. Information about the consequences that make the incident significant

Multiple options can be selected



B.2.1.2. Information about the consequences the incident was capable of causing that make it significant

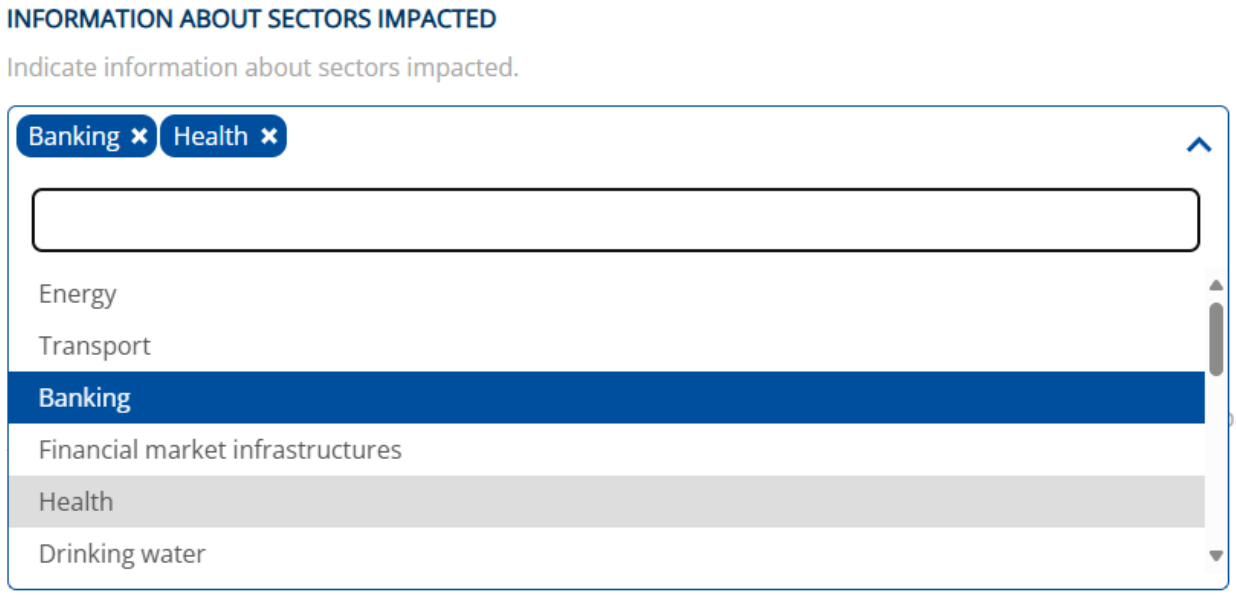
Multiple options can be selected



B.2.1.3. Impact TAB

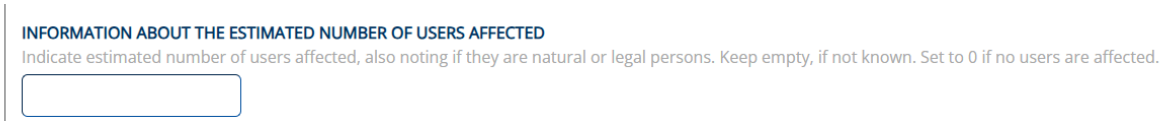
B.2.1.4. Information about sectors impacted

Multiple choices can be made



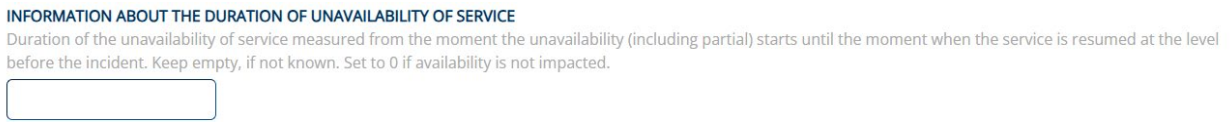
B.2.1.5. Information about the estimated number of users affected

Numbers only



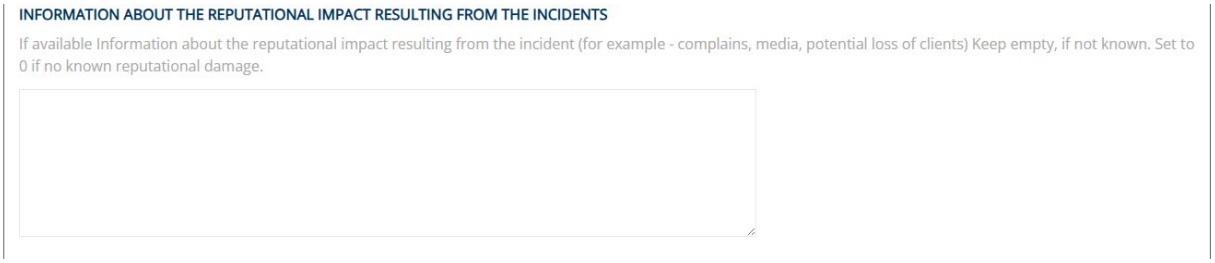
B.2.1.6. Information about the duration of the unavailability of the service

Numbers only



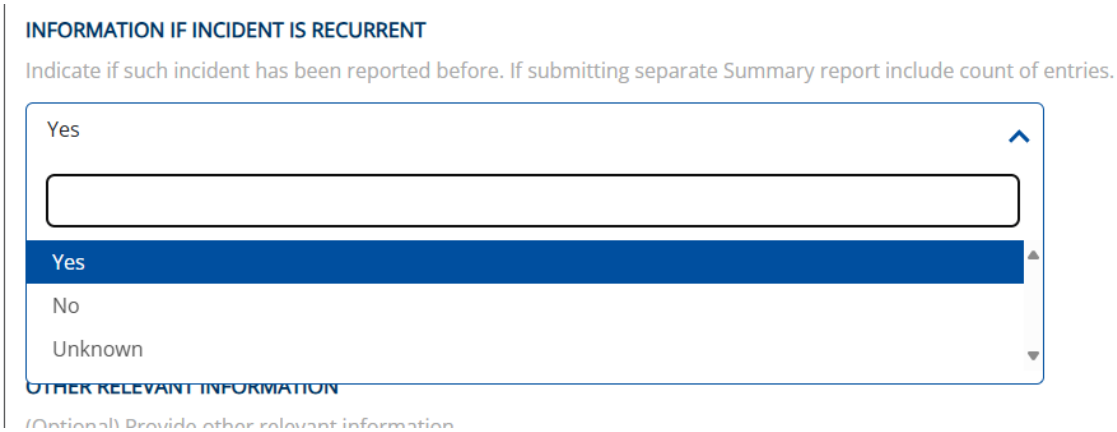
B.2.1.7. Information about the reputational impact resulting from the incidents

Text only



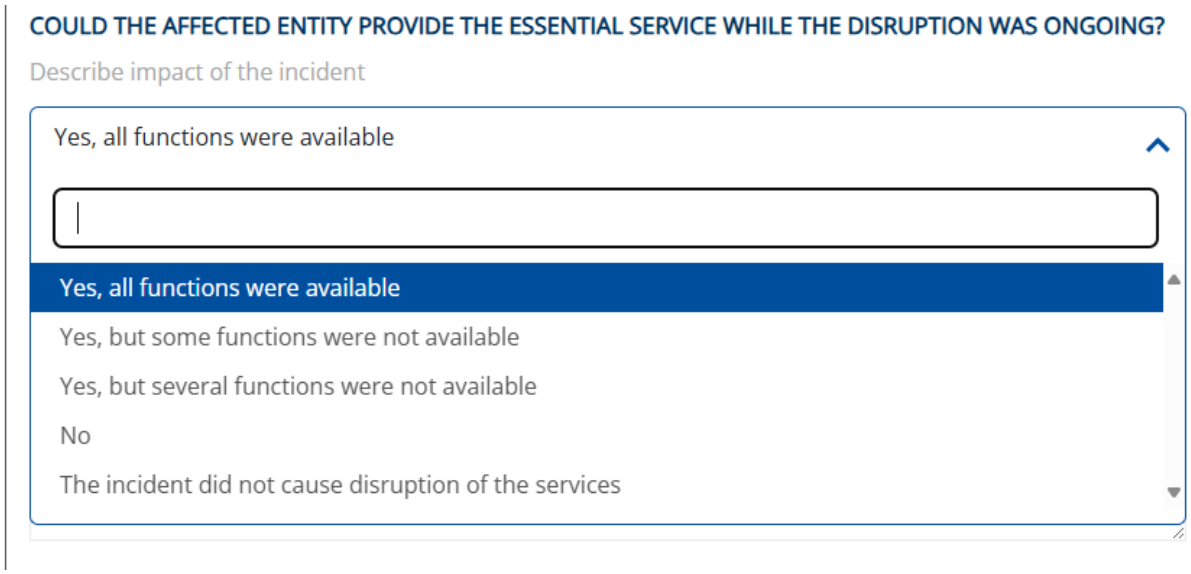
B.2.1.8. Information if the incident is recurrent

Only one option can be selected



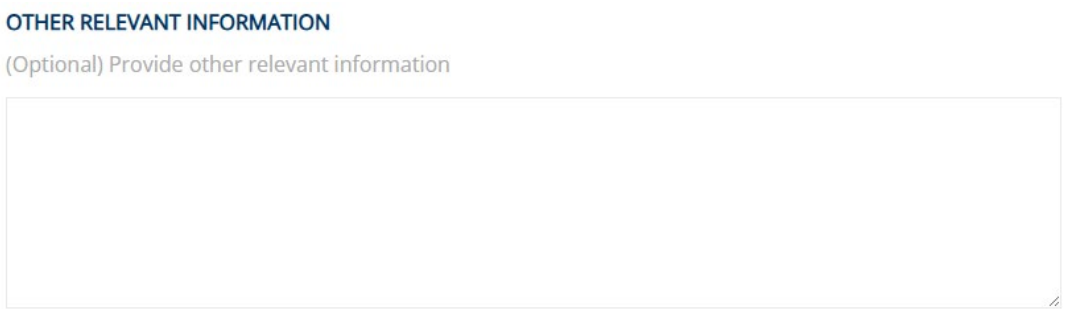
B.2.1.9. Could the affected entity provide the essential service while the disruption was ongoing?

Only one option can be selected

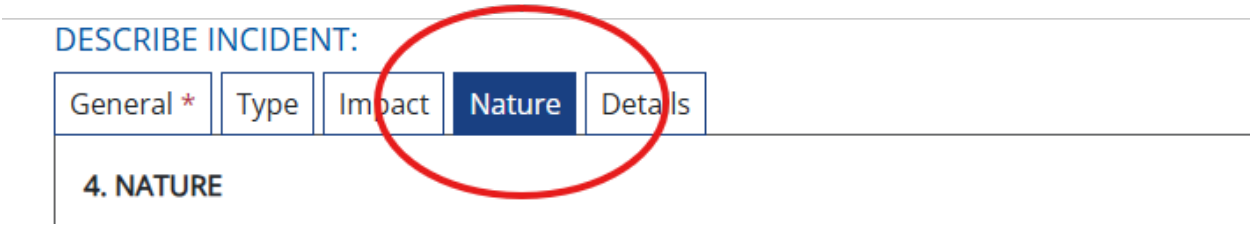


B.2.1.10. Other relevant information

Text only

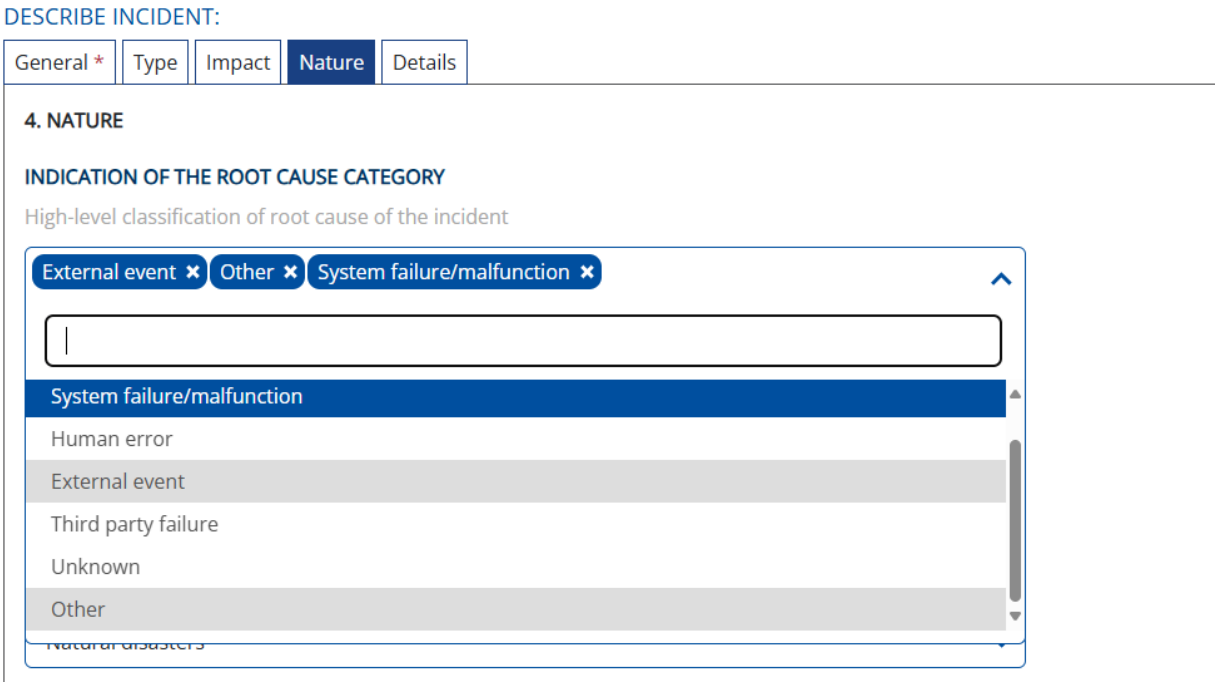


B.2.2. Nature of the incident TAB



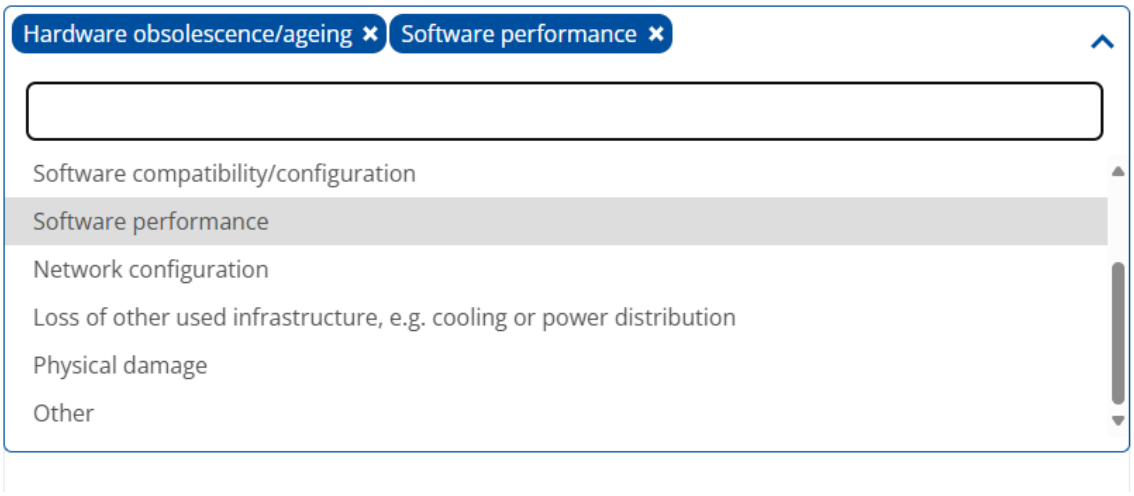
B.2.2.1. Indication of the root cause category

Multiple options can be selected



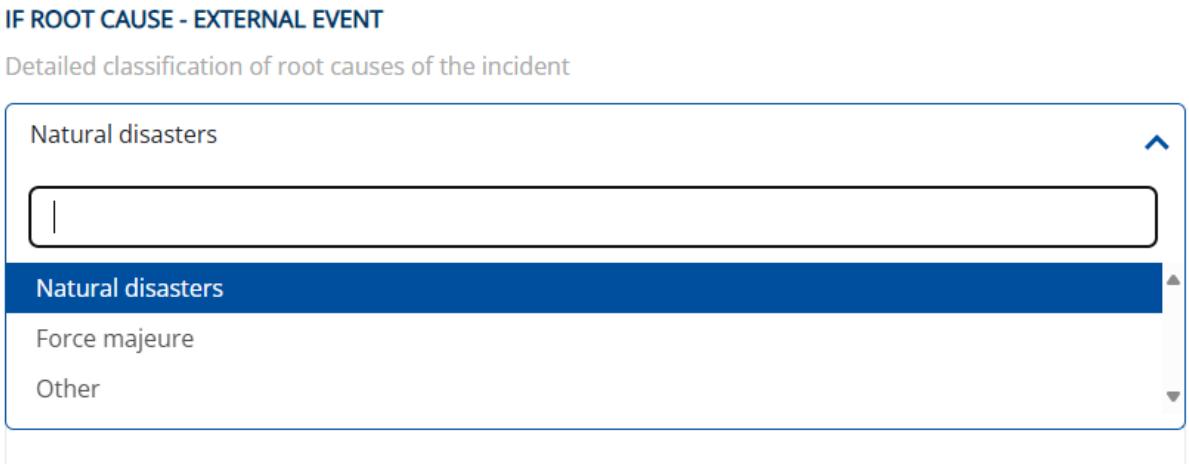
B.2.2.2. In case of system failure/malfunction

Multiple selections are possible



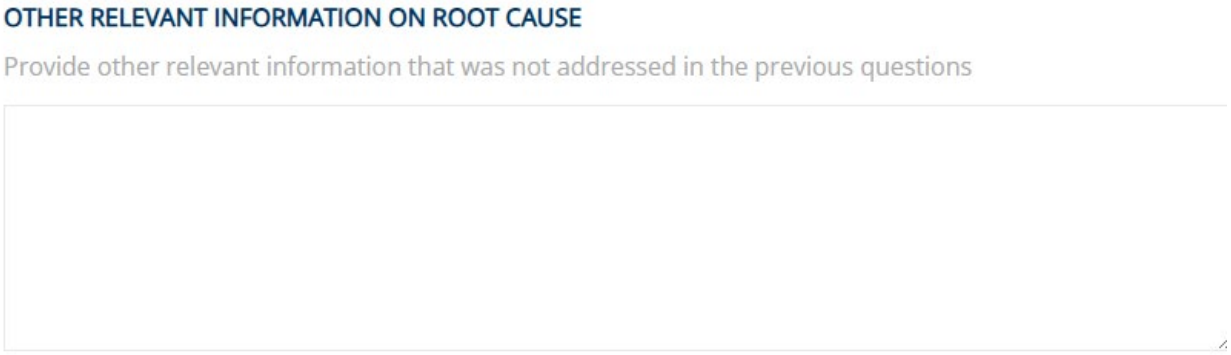
B.2.2.3. If root cause is external event

Only one option is possible

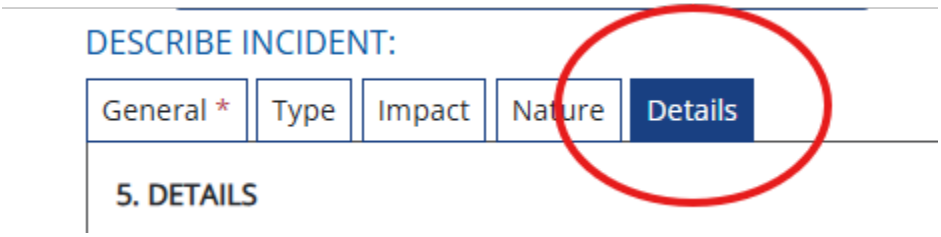


B.2.2.4. Other relevant information

Text field

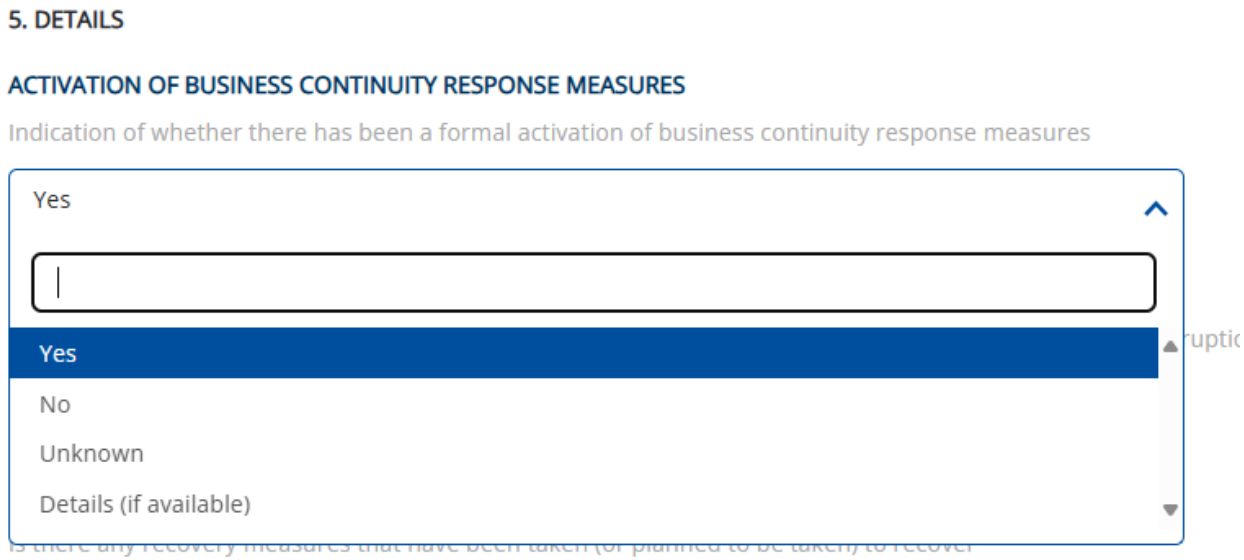


B.2.3. Details TAB



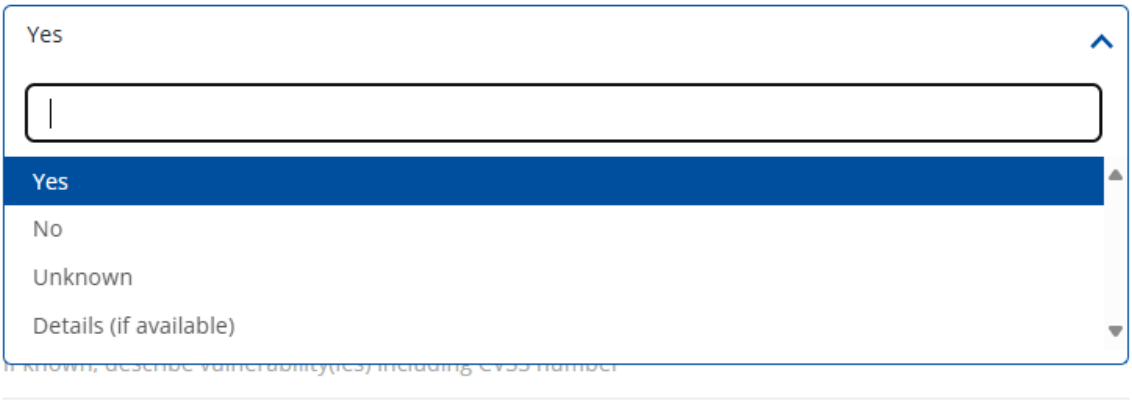
B.2.3.1. Activation of Business continuity response measures

Only one option is possible



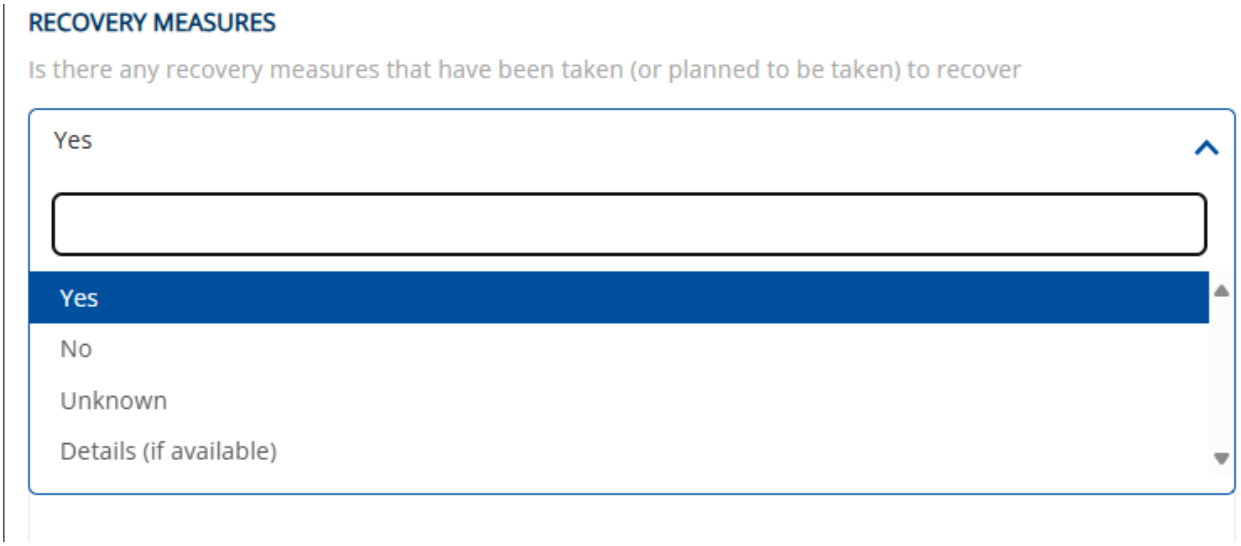
B.2.3.2. Follow up actions

Only one option is possible



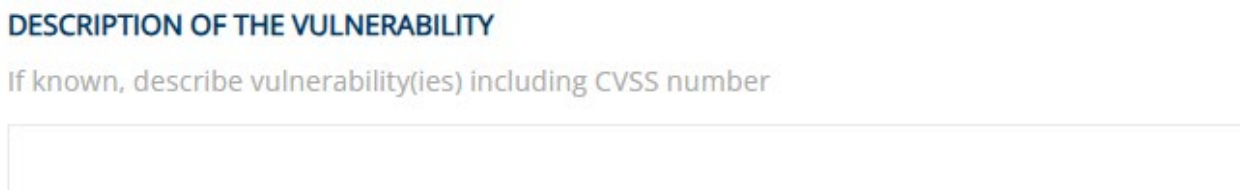
B.2.3.3. Recovery measures

Only one option is possible



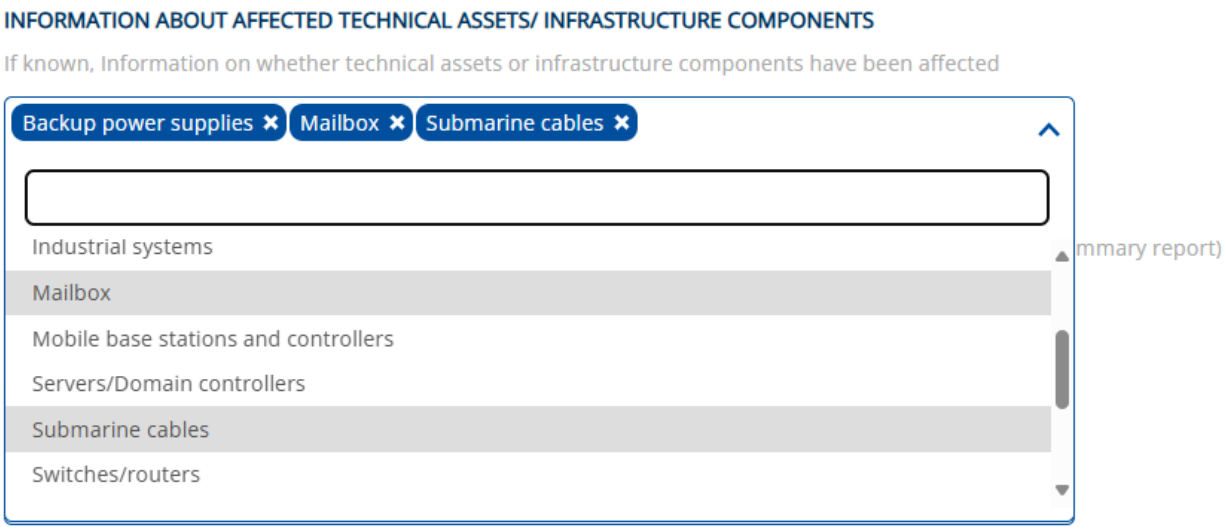
B.2.3.4. Description of the vulnerability

Text only



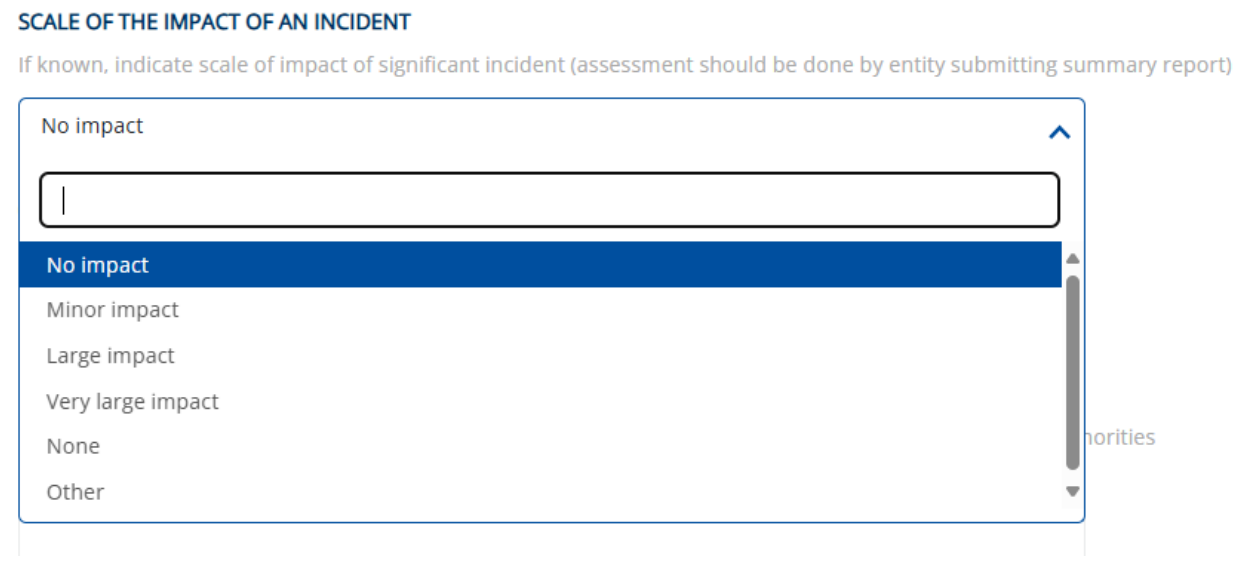
B.2.3.5. Information about affected technical assets/infrastructure components

Multiple selections are possible



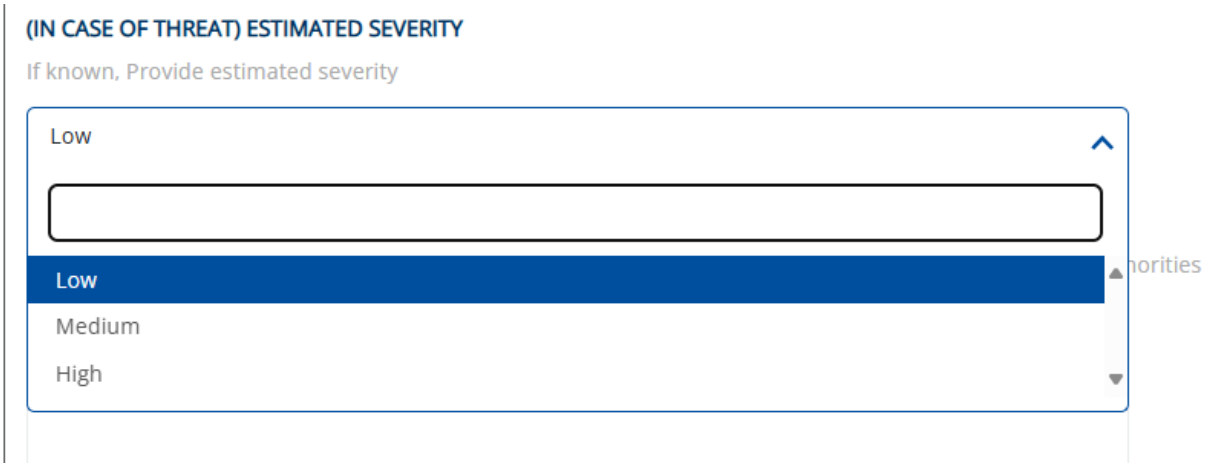
B.2.3.6. Scale of impact

Only one option is possible



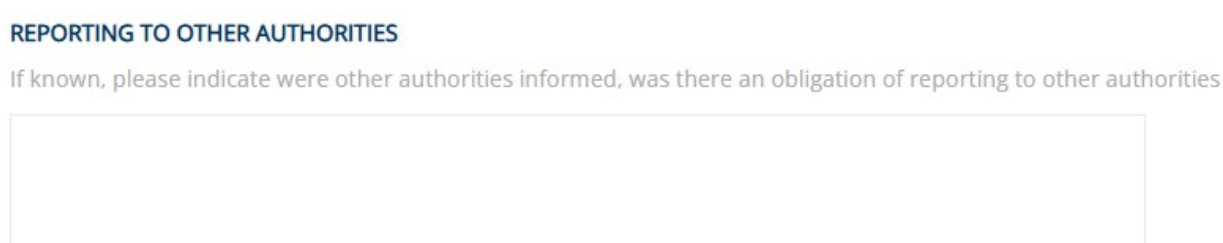
B.2.3.7. Estimated severity (in case of threat)

Only one option is possible



B.2.3.8. Reporting to other authorities

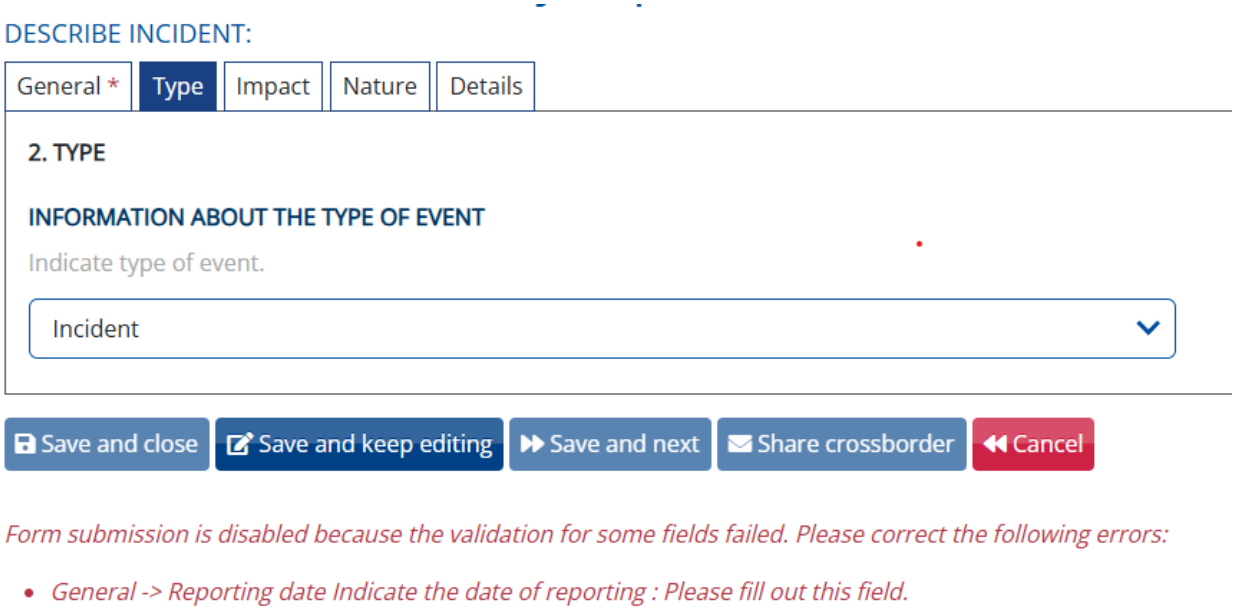
Text field



B.2.3.9. National level support

Text field

B.3. Steps for TYPE INCIDENT



No other details can be added in this tab

B.3.1. Impact TAB

Follow the same procedure for significant incident, as indicated in B.2.1.3

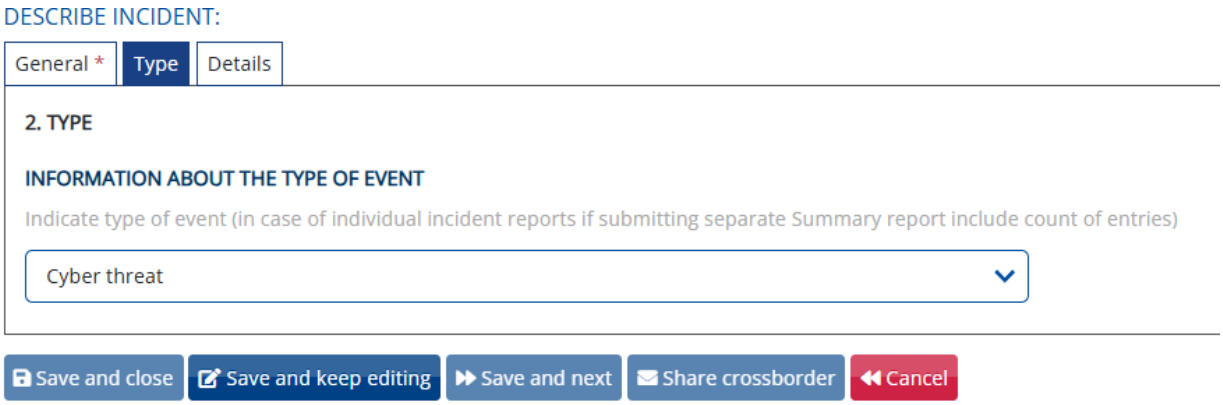
B.3.2. Nature TAB

Follow the same procedure for significant incident, as indicated in B.2.2

B.3.3. Details TAB

Follow the same procedure for significant incident, as indicated in B.2.3

B.4. Steps for TYPE CYBER THREAT

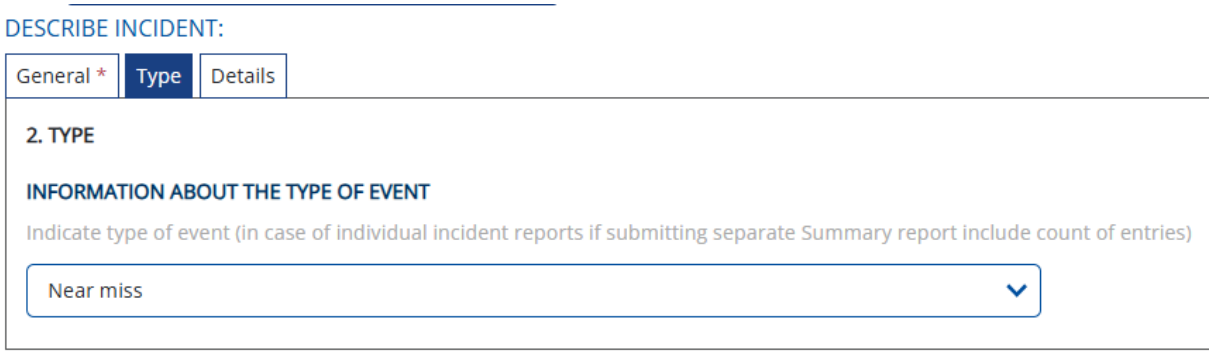


No other details can be added in this tab

B.4.1. Details TAB

Follow the same procedure for significant incident, as indicated in B.2.3

B.5. Steps for TYPE NEAR MISS



No other details can be added in this tab

B.5.1. Details TAB

Follow the same procedure for significant incident, as indicated in B.2.3

C. Bulk Import reporting procedure

C.1.1. File instructions

Download a file with auto generated sample data to familiarize yourself with the file.

In the bulk import page the templates can be seen as well as samples.

Two types of files are available for import: MS Excel (XLS) and JavaScript Object Notation (JSON).

The sample template has been provided with multiple sheets, one per each type of incident.

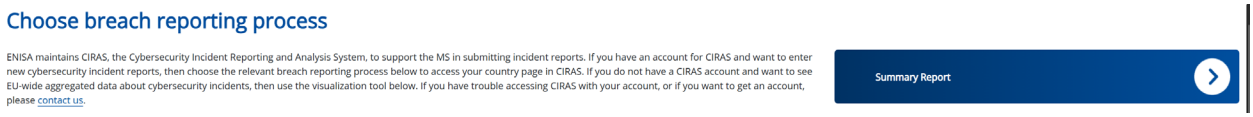
Please input one incident report per row, using the formats described.

Some sheets (incident types) may not include all fields.

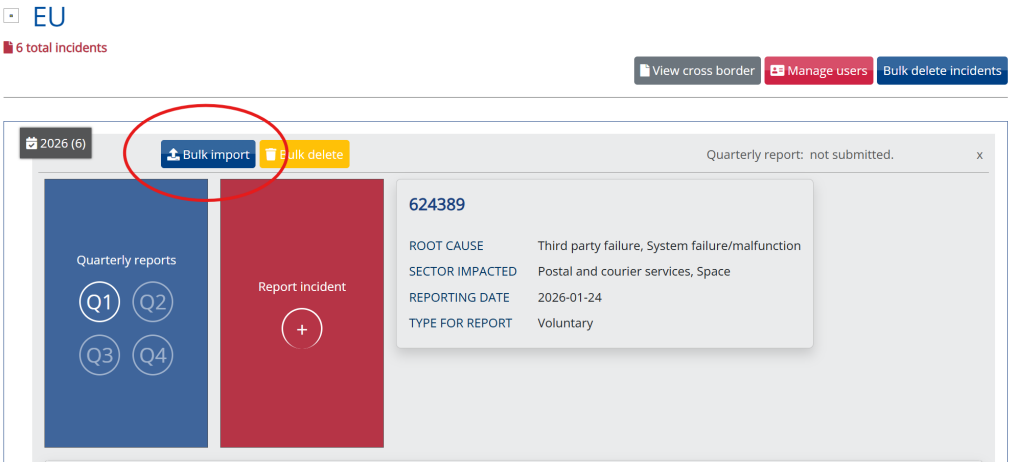
Please, ensure that the reporting date is included in the file. This is the only mandatory field in the file.

If you don't have this filed the import will fail.

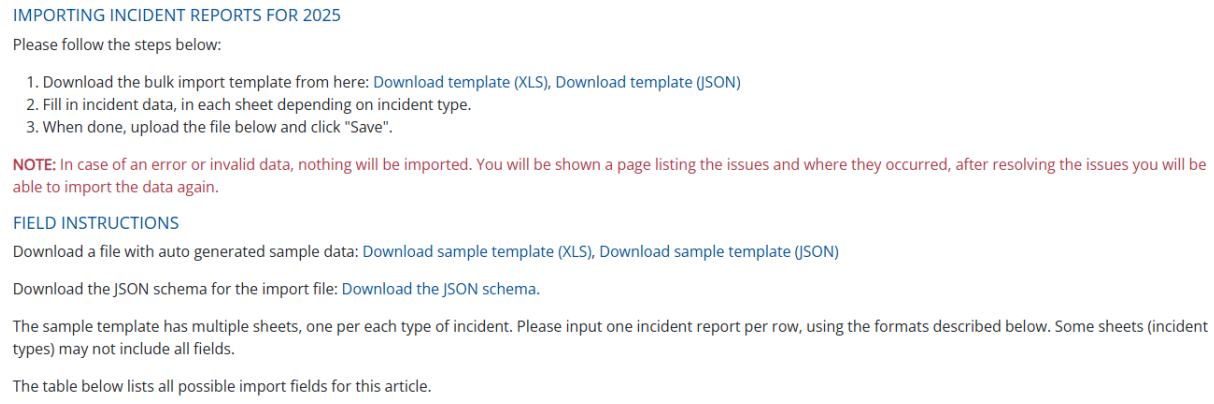
To get to the import page, login with your EU login account and go to summary report



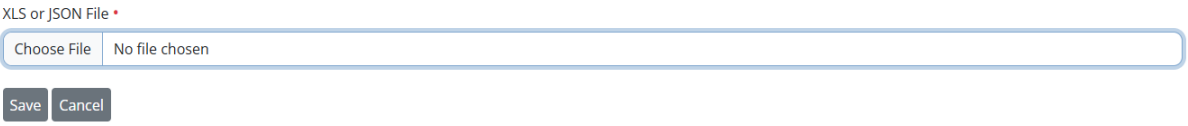
Select your country and choose bulk import.



This is how the page should look like

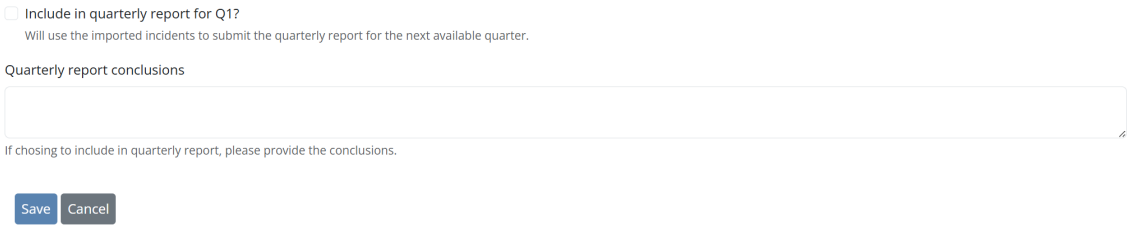


C.1.2. Select file to import



C.1.3. Direct publication of quarterly report

In case you want a direct publication of the imported incidents to the next available quarter is possible if you check the “include in quarterly report for Q”



C.1.4. Press Save

Incident import process will start.

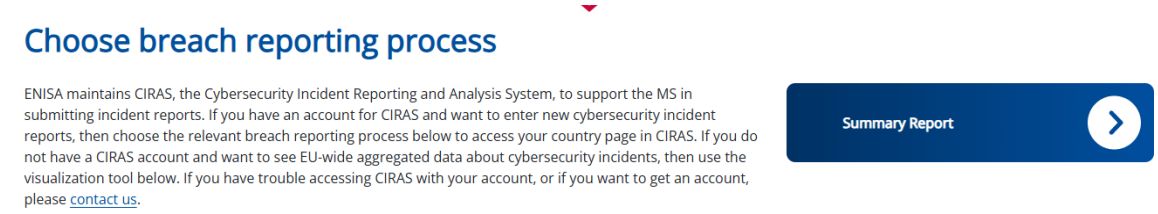
In case of an error or invalid data, nothing will be imported. You will be shown a page listing the issues and where they occurred, after resolving the issues you will be able to import the data again.

After successful validation of all data in the file the incidents will be imported.

D. How to make quarterly report

D.1.1. Go to summary report

You can find this link on the main page of CIRAS 2 below the reporting links. **Select summary report**.

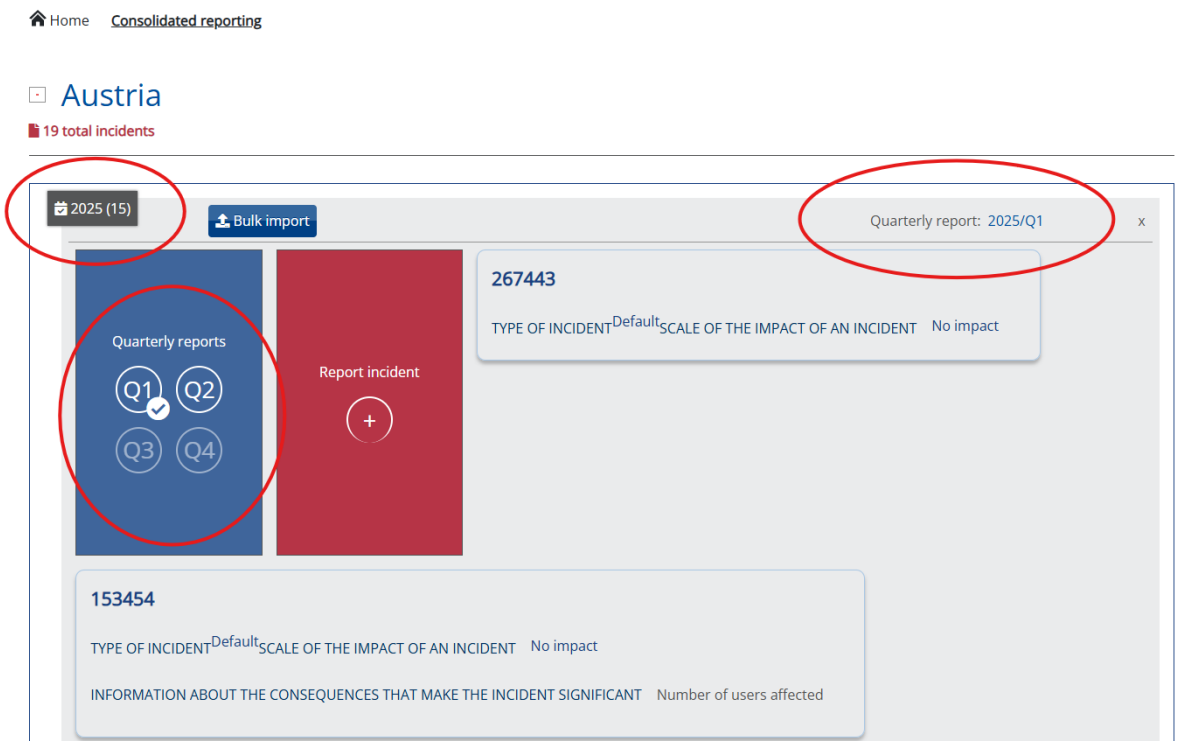


D.1.2. Select your country

You will be presented with this page (Austria selected)

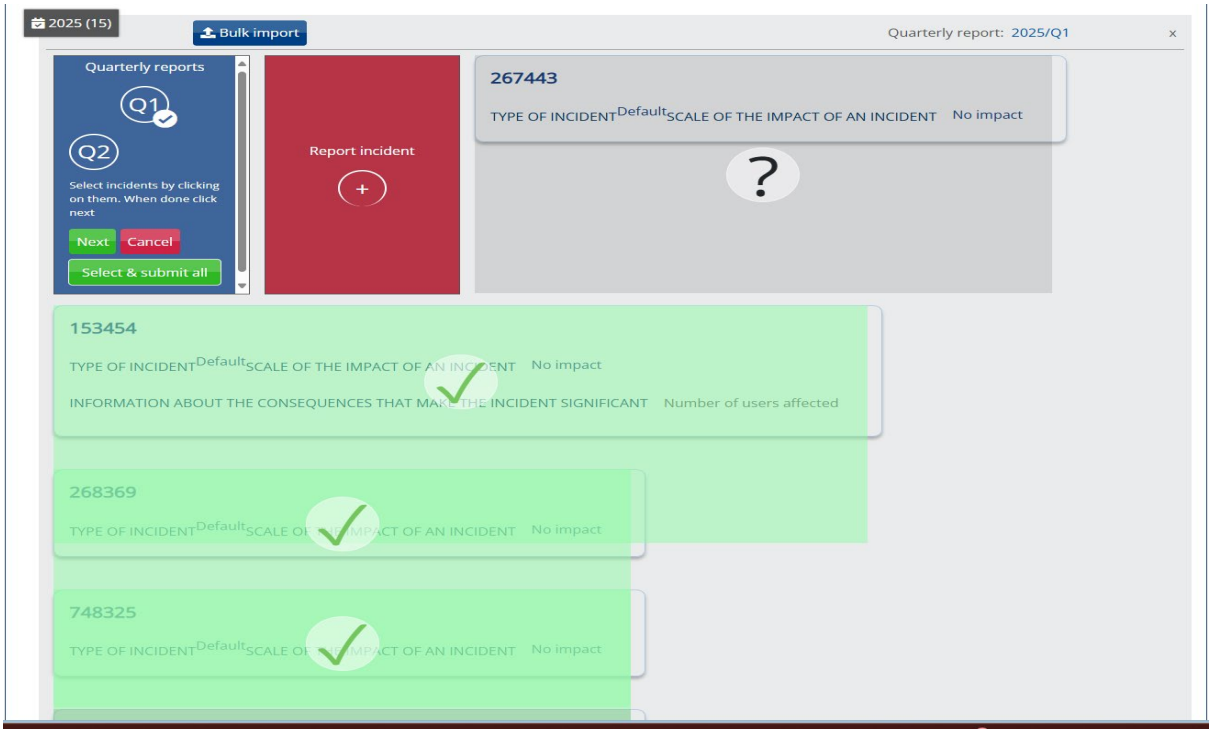
D.1.3. Select the button representing the quarter

Select Q1, Q2, Q3 or Q4 you want to report for the respective year. As indicated here, there is already quarterly report for Q1 2025



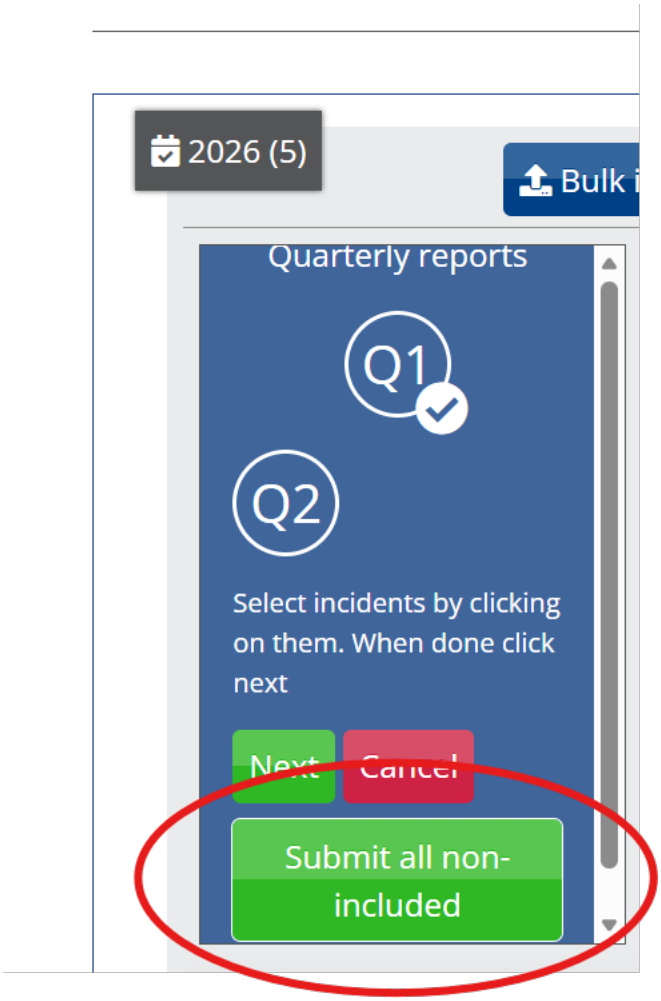
D.1.4. Select the incidents to be included in the quarterly report

Here three (3) have been selected and one not selected. There is possibility to select all incidents with the button Select & submit all. Click on an incident to include it and click again to be unselected.



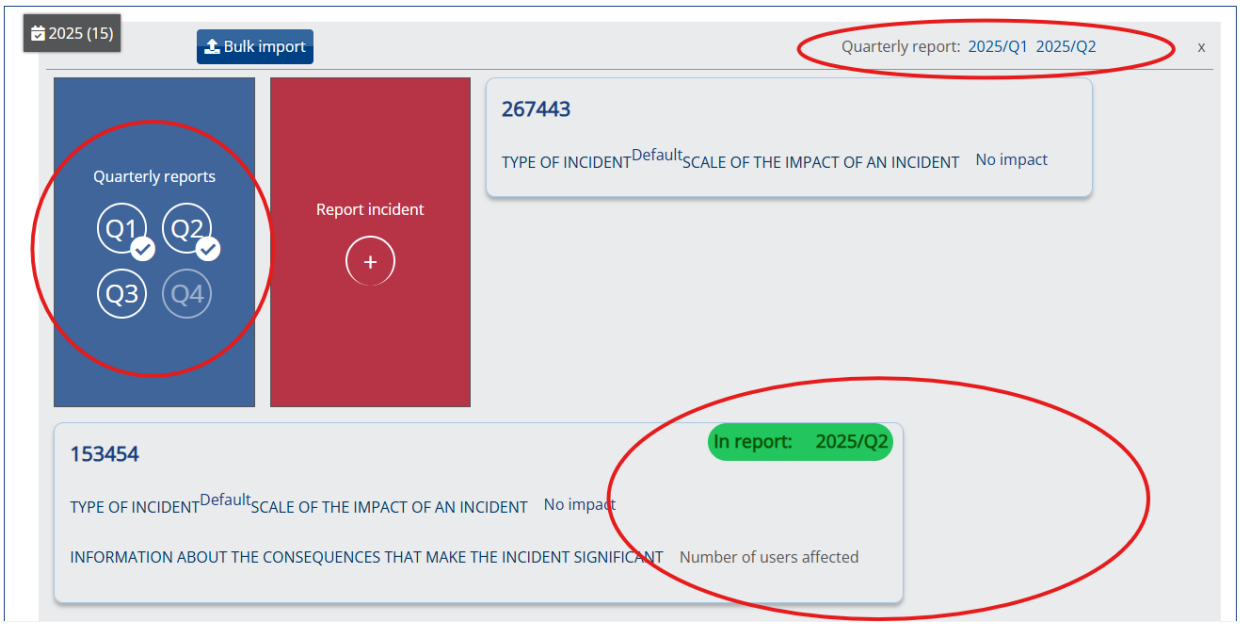
Click next or select & submit all, depending on your choice.

We have the option to submit all non-included in previous reports as indicated below



D.1.5. Provide details about the quarterly report

The page displays the number of selected incidents to be included in the quarterly report and asks for some details to be added.



D.1.6. Submit the quarterly report

Once the submit button is pressed the quarterly report is generated. On the upper right corner, it should show the quarterly reports that are already generated. In the list of incidents below it shows which incident to which quarterly report belongs.

D.1.7. Quarterly report management

In case a quarterly report needs to be deleted – select the quarterly report from the upper right corner

D.1.7.1. Delete a quarterly report

Use the button delete to delete a quarterly report. The page shows which incidents are included in the specific quarterly report. The deletion of quarterly report does not delete the incidents that are associated with this report. The incidents can be deleted once you select the specific incident. Incidents included in quarterly report can't be deleted. First the quarterly report needs to be deleted and then an incident can be deleted.

D.1.7.2. Download a quarterly report

Use the buttons to download the quarterly report – either in PDF or XML

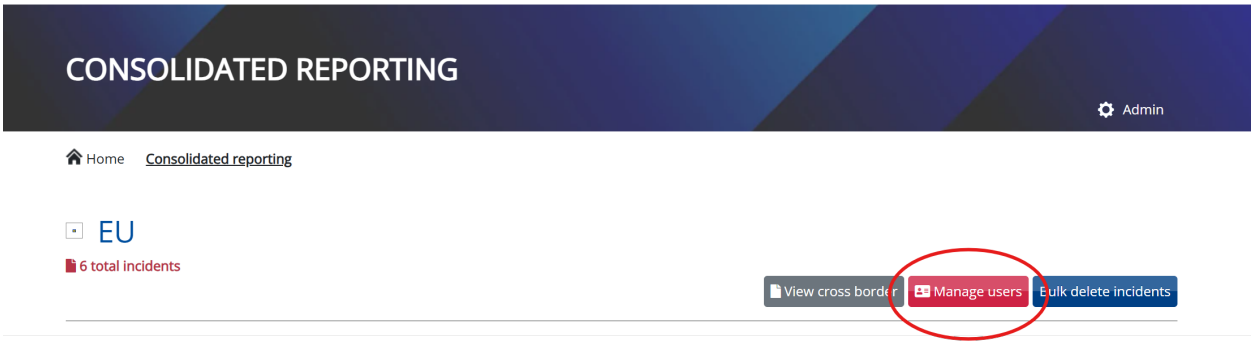
E. User Management

User Management allows one or many designated user(s) to manage users for a specific country.

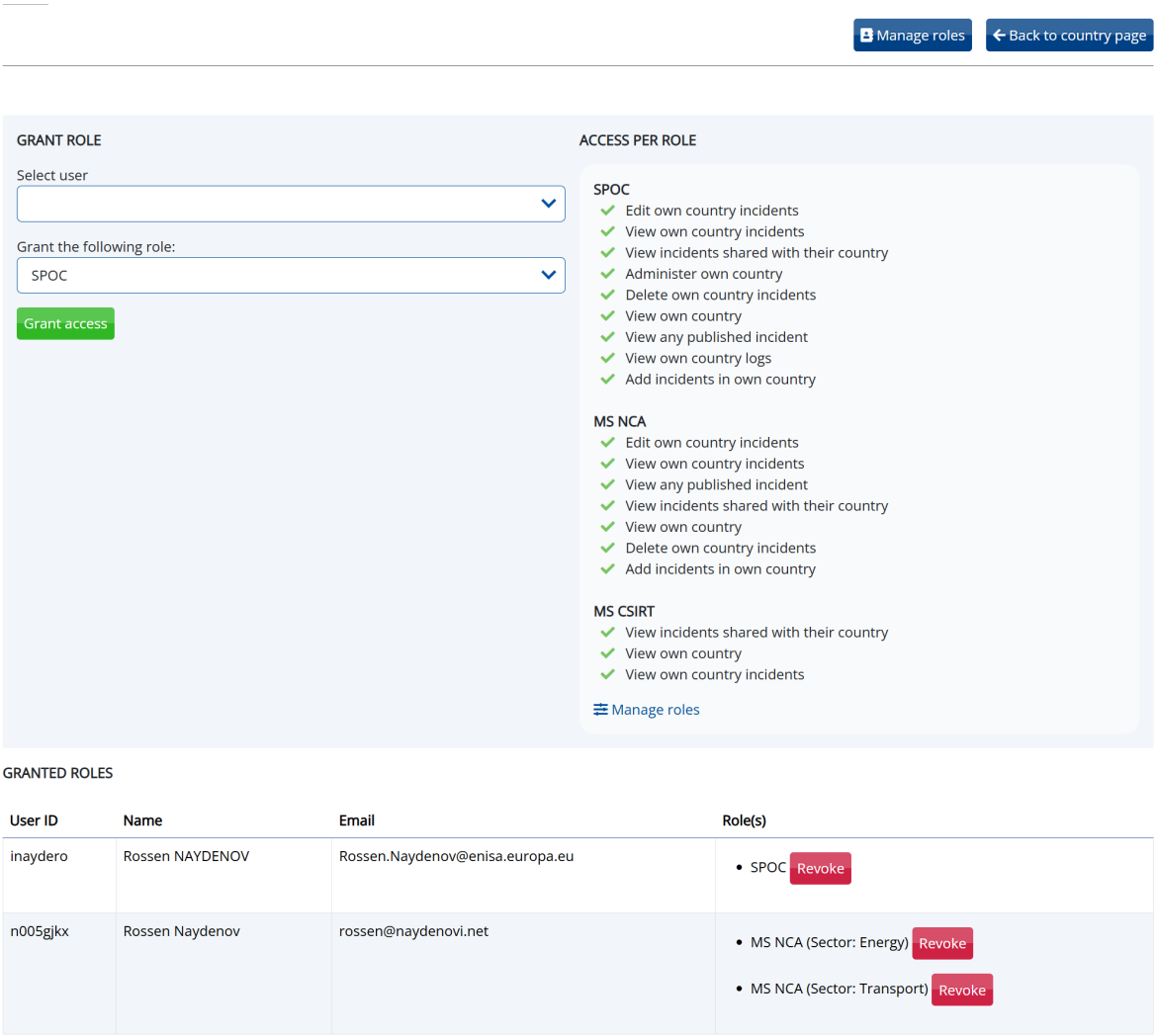
To designate a person or many a request must be sent to incidentreporting@enisa.europa.eu, after verification these persons will be assigned admin rights for this country.

To use the manage users panel, first one needs to login with their EU login and have the right assigned to them. Then go to summary report link

After that select your country and use the button Manage Users



After that you are presented with user management panel



The role of the SPOC is the role that manages users. This user can also edit or revoke the rights for the Member State National Competent Authority (MS NCA) and the Member State CSIRT (MS CSIRT).

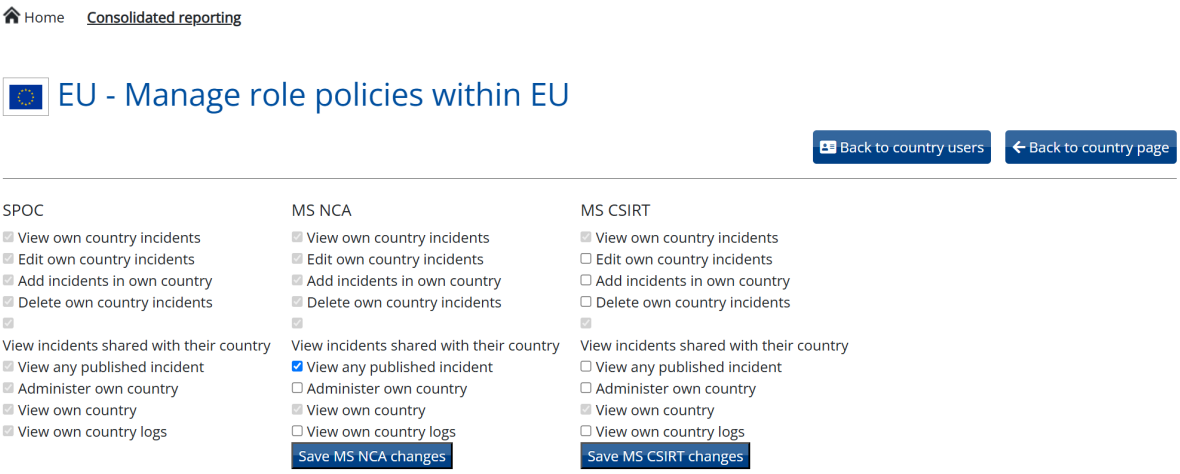
The SPOC also can revoke and grant rights to specific users under the MS NCA and the MS CSIRT.

The Member State National Competent Authority (MS NCA) is a role that can be assigned to all or one or many specific sectors. If a MS NCA is assigned to a specific sector, they will be able to receive notifications for that specific sector, as well as add/edit or view incidents in this sector based on the selection of rights given.

The Member State CSIRT (MS CSIRT) may have similar rights or other to the MS NCA. The rules for notifications and access remain the same based on the sectors the MS CSIRT is allowed to access.

E.1. Manage Roles

Managing roles gives the opportunity to remove or add rights to MS CSIRTS and MS NCA, as indicated below.



There could be many MS NCA and MS CSIRT, though the roles could be only these three – SPOC, MS NCA and MS CSIRT. More roles can be done in case there is enough requests.