

INCIDENT REPORTING WITH CIRAS v2 MANUAL

Contents

- CIRAS 2 Platform 4
 - CIRAS page 4
- Accessing NIS 2 CIRAS 4
- A. Incident reporting process 5
- B. Single incident reporting procedure 5
 - B.1. General TAB 5
 - B.1.1. Select the type of report 5
 - B.1.2. Select date 6
 - B.1.3. Select affected countries 6
 - B.2. Incident type TAB 7
 - B.2.1. Steps for significant incident 8
 - B.2.1.1. Information about the consequences that make the incident significant 8
 - B.2.1.2. Information about the consequences the incident was capable of causing that make it significant 8
 - B.2.1.3. Impact TAB 9
 - B.2.1.4. Information about sectors impacted 9
 - B.2.1.5. Information about the estimated number of users affected 9
 - B.2.1.6. Information about the duration of the unavailability of the service 10
 - B.2.1.7. Information about the reputational impact resulting from the incidents 10
 - B.2.1.8. Information if the incident is recurrent 10
 - B.2.1.9. Could the affected entity provide the essential service while the disruption was ongoing? ... 11
 - B.2.1.10. Other relevant information 11
 - B.2.2. Nature of the incident TAB 11
 - B.2.2.1. Indication of the root cause category 12
 - B.2.2.2. In case of system failure/malfunction 12
 - B.2.2.3. If root cause is external event 13
 - B.2.2.4. Other relevant information 13
 - B.2.3. Details TAB 13
 - B.2.3.1. Activation of Business continuity response measures 14
 - B.2.3.2. Follow up actions 14
 - B.2.3.3. Recovery measures 15
 - B.2.3.4. Description of the vulnerability 15
 - B.2.3.5. Information about affected technical assets/infrastructure components 15
 - B.2.3.6. Scale of impact 16
 - B.2.3.7. Estimated severity (in case of threat) 16

B.2.3.8.	Reporting to other authorities	16
B.2.3.9.	National level support	17
B.3.	Steps for TYPE INCIDENT	18
B.3.1.	Impact TAB.....	18
B.3.2.	Nature TAB	18
B.3.3.	Details TAB.....	18
B.4.	Steps for TYPE CYBER THREAT	19
B.4.1.	Details TAB.....	19
B.5.	Steps for TYPE NEAR MISS	19
B.5.1.	Details TAB.....	19
C.	Bulk Import reporting procedure.....	20
C.1.1.	File instructions	20
C.1.2.	Select file to import	21
C.1.3.	Direct publication of quarterly report	21
C.1.4.	Press Save	21
D.	How to make quarterly report.....	22
D.1.1.	Go to summary report.....	22
D.1.2.	Select your country.....	22
D.1.3.	Select the button representing the quarter	23
D.1.4.	Select the incidents to be included in the quarterly report	23
D.1.5.	Provide details about the quarterly report	24
D.1.6.	Submit the quarterly report	25
D.1.7.	Quarterly report management.....	26
D.1.7.1.	Delete a quarterly report.....	26
D.1.7.2.	Download a quarterly report.....	26
E.	User Management	27
E.1.	Manage Roles.....	28

CIRAS 2 Platform

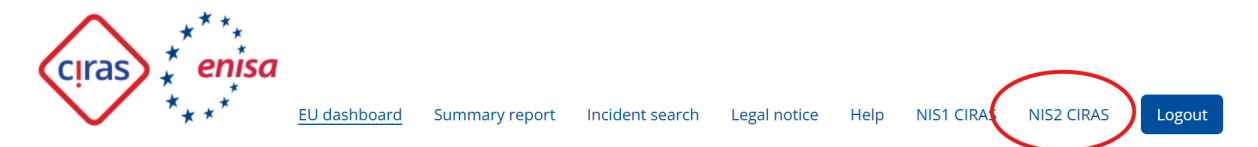
CIRAS 2 is evolution of CIRAS and follows the templates and the requirements set in NIS 2.

CIRAS page

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

Accessing NIS 2 CIRAS

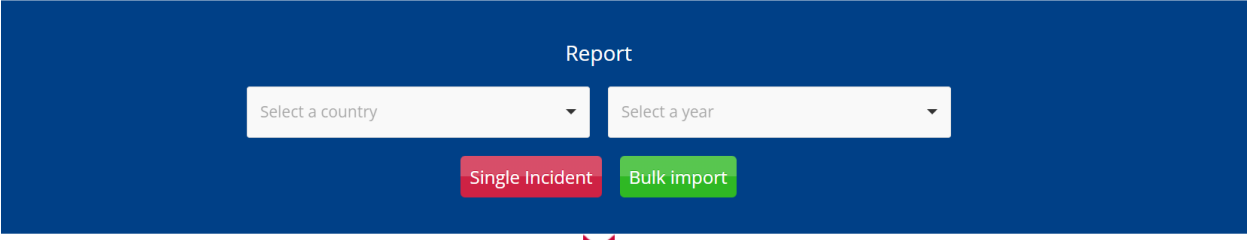
Go to CIRAS web page and click NIS 2 CIRAS, as indicated below.



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.

New incident: Summary Report/Atlantica

CHOSEN SECTOR(S) / ARTICLE

Energy []

Oil []

DESCRIBE INCIDENT:

General * | Type | Impact | Nature | Details

1. GENERAL

TYPE OF THE REPORT
Indicate the type of report (in case of individual incident reports if submitting separate Summary report include count of entries)

Mandatory ^

Mandatory

Voluntary v

AFFECTED MS (EEA)
Indicate affected countries (EU and EEA)

v

B.1.2. Select date

DESCRIBE INCIDENT:

General * Type Impact Nature Details

1. GENERAL

TYPE OF THE REPORT

Indicate the type of report (in case of individual incident reports if submitting separate Summary report include count of entries)

Mandatory

REPORTING DATE *

Indicate the date of reporting

dd-----yyyy

March 2025

Mo	Tu	We	Th	Fr	Sa	Su
24	25	26	27	28	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Because the validation for some fields failed. Please correct the following errors:

- General -> Reporting date Indicate the date of reporting : Please fill out this field.

B.1.3. Select affected countries

Multiple countries can be selected

Indicate the type of report (in case of individual incident reports if submitting separate Summary report include count of entries)

Mandatory

REPORTING DATE *

Indicate the date of reporting

dd-----yyyy

Please fill out this field.

AFFECTED MS (EEA)

Indicate affected countries (EU and EEA)

BG x CZ x HR x

FI
FR
GR
HR
HU
IE

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.

DESCRIBE INCIDENT:

General *	Type	Impact	Nature	Details
-----------	------	--------	--------	---------

2. TYPE

INFORMATION ABOUT THE TYPE OF EVENT

Indicate type of event (in case of individual incident reports if submitting separate Summary report include count of entries)

Significant incident ▲

Significant incident ▲

Incident

Cyber threat

Near miss ▼

STATE THE CONSEQUENCES OF THE INCIDENT

State the consequences the incident was capable of causing that make the incident significant (criteria that triggered the incident report)

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

INFORMATION ABOUT THE TYPE OF EVENT
Indicate type of event (in case of individual incident reports if submitting separate Summary report include count of entries)

Significant incident

INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT
State the consequences that make the incident significant (criteria that triggered the incident report)

Material damage x Non-material damage x
Exfiltration of trade secrets or other sensitive information x

Geographical spread
Direct financial loss
Non-material damage
Material damage
Reputational damage
Exfiltration of trade secrets or other sensitive information

Form submission is disabled because the validation for some fields failed. Please correct the following errors.

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

Multiple options can be selected

INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT
State the consequences that make the incident significant (criteria that triggered the incident report)

Material damage x Non-material damage x
Exfiltration of trade secrets or other sensitive information x

INFORMATION ABOUT THE CONSEQUENCES THE INCIDENT WAS CAPABLE OF CAUSING THAT MAKE IT SIGNIFICANT
State the consequences the incident was capable of causing that make the incident significant (criteria that triggered the

Geographical spread x Non-material damage x
Incident is capable of gaining a successful, suspectedly malicious and unauthorized access to network and information systems x
None x Other x

Incident is capable of causing the death of natural legal person
Incident is capable of causing considerable damage to natural person's health
Incident is capable of gaining a successful, suspectedly malicious and unauthorized access to network and information systems
None
Other

B.2.1.3. Impact TAB

DESCRIBE INCIDENT:

General * **Impact** Nature Details

3. IMPACT

B.2.1.4. Information about sectors impacted

Multiple choices can be made

INFORMATION ABOUT SECTORS IMPACTED

Indicate information about sectors impacted.

Banking x Health x

Energy

Transport

Banking

Financial market infrastructures

Health

Drinking water

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

Numbers only

INFORMATION ABOUT THE ESTIMATED NUMBER OF USERS AFFECTED

Indicate estimated number of users affected, also noting if they are natural or legal persons. Keep empty, if not known. Set to 0 if no users are affected.

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

Numbers only

INFORMATION ABOUT THE DURATION OF UNAVAILABILITY OF SERVICE

Duration of the unavailability of service measured from the moment the unavailability (including partial) starts until the moment when the service is resumed at the level before the incident. Keep empty, if not known. Set to 0 if availability is not impacted.

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

Text only

INFORMATION ABOUT THE REPUTATIONAL IMPACT RESULTING FROM THE INCIDENTS

If available Information about the reputational impact resulting from the incident (for example - complains, media, potential loss of clients) Keep empty, if not known. Set to 0 if no known reputational damage.

B.2.1.8. Information if the incident is recurrent

Only one option can be selected

INFORMATION IF INCIDENT IS RECURRENT

Indicate if such incident has been reported before. If submitting separate Summary report include count of entries.

 Yes

 Yes
 No
 Unknown

OTHER RELEVANT INFORMATION

(Optional) Provide other relevant information

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

Only one option can be selected

COULD THE AFFECTED ENTITY PROVIDE THE ESSENTIAL SERVICE WHILE THE DISRUPTION WAS ONGOING?

Describe impact of the incident

Yes, all functions were available

Yes, all functions were available

Yes, but some functions were not available

Yes, but several functions were not available

No

The incident did not cause disruption of the services

B.2.1.10. Other relevant information

Text only

OTHER RELEVANT INFORMATION

(Optional) Provide other relevant information

B.2.2. Nature of the incident TAB

DESCRIBE INCIDENT:

General *	Type	Impact	Nature	Details
-----------	------	--------	---------------	---------

4. NATURE

B.2.2.1. Indication of the root cause category

Multiple options can be selected

DESCRIBE INCIDENT:

General * | Type | Impact | **Nature** | Details

4. NATURE

INDICATION OF THE ROOT CAUSE CATEGORY

High-level classification of root cause of the incident

External event ✕ Other ✕ System failure/malfunction ✕

- System failure/malfunction
- Human error
- External event
- Third party failure
- Unknown
- Other
- Natural disasters

B.2.2.2. In case of system failure/malfunction

Multiple selections are possible

IF ROOT CAUSE - SYSTEM FAILURE/MALFUNCTION

Detailed classification of root causes of the incident

Hardware obsolescence/ageing ✕ Software performance ✕

- Software compatibility/configuration
- Software performance
- Network configuration
- Loss of other used infrastructure, e.g. cooling or power distribution
- Physical damage
- Other

B.2.2.3. If root cause is external event

Only one option is possible

IF ROOT CAUSE - EXTERNAL EVENT

Detailed classification of root causes of the incident

Natural disasters ^

Natural disasters

Force majeure

Other v

B.2.2.4. Other relevant information

Text field

OTHER RELEVANT INFORMATION ON ROOT CAUSE

Provide other relevant information that was not addressed in the previous questions

B.2.3. Details TAB

DESCRIBE INCIDENT:

General *	Type	Impact	Nature	Details
-----------	------	--------	--------	----------------

5. DETAILS

B.2.3.1. Activation of Business continuity response measures

Only one option is possible

5. DETAILS

ACTIVATION OF BUSINESS CONTINUITY RESPONSE MEASURES

Indication of whether there has been a formal activation of business continuity response measures

The screenshot shows a dropdown menu with a search bar at the top. The menu is open, displaying four options: 'Yes', 'No', 'Unknown', and 'Details (if available)'. The 'Yes' option is highlighted in blue. A vertical scrollbar is visible on the right side of the menu. The text 'ruptic' is partially visible on the right edge of the image.

B.2.3.2. Follow up actions

Only one option is possible

FOLLOW UP ACTIONS

Is there any follow up actions that have been taken (or planned to be taken) to prevent similar incidents/disruptions

The screenshot shows a dropdown menu with a search bar at the top. The menu is open, displaying four options: 'Yes', 'No', 'Unknown', and 'Details (if available)'. The 'Yes' option is highlighted in blue. A vertical scrollbar is visible on the right side of the menu. The text 'If known, describe vulnerability(ies) including CVSS number' is partially visible at the bottom of the image.

B.2.3.3. Recovery measures

Only one option is possible

RECOVERY MEASURES

Is there any recovery measures that have been taken (or planned to be taken) to recover

Yes

Yes

No

Unknown

Details (if available)

B.2.3.4. Description of the vulnerability

Text only

DESCRIPTION OF THE VULNERABILITY

If known, describe vulnerability(ies) including CVSS number

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

Multiple selections are possible

INFORMATION ABOUT AFFECTED TECHNICAL ASSETS/ INFRASTRUCTURE COMPONENTS

If known, Information on whether technical assets or infrastructure components have been affected

Backup power supplies ✕ Mailbox ✕ Submarine cables ✕

Industrial systems

Mailbox

Mobile base stations and controllers

Servers/Domain controllers

Submarine cables

Switches/routers

Summary report)

B.2.3.6. Scale of impact

Only one option is possible

SCALE OF THE IMPACT OF AN INCIDENT

If known, indicate scale of impact of significant incident (assessment should be done by entity submitting summary report)

No impact ▲

No impact

Minor impact

Large impact

Very large impact

None

Other

authorities

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

Only one option is possible

(IN CASE OF THREAT) ESTIMATED SEVERITY

If known, Provide estimated severity

Low ▲

Low

Medium

High

authorities

B.2.3.8. Reporting to other authorities

Text field

REPORTING TO OTHER AUTHORITIES

If known, please indicate were other authorities informed, was there an obligation of reporting to other authorities

B.2.3.9. National level support

Text field

NATIONAL LEVEL SUPPORT (COMPETENT AUTHORITY OR CSIRT)

If known, please indicate was support requested at national level

B.3. Steps for TYPE INCIDENT

DESCRIBE INCIDENT:






General *	Type	Impact	Nature	Details
-----------	-------------	--------	--------	---------

2. TYPE

INFORMATION ABOUT THE TYPE OF EVENT

Indicate type of event.

Incident ▼

 Save and close  Save and keep editing  Save and next  Share crossborder  Cancel

Form submission is disabled because the validation for some fields failed. Please correct the following errors:

- *General -> Reporting date Indicate the date of reporting : Please fill out this field.*

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

DESCRIBE INCIDENT:





General *	Type	Details
-----------	------	---------

2. TYPE

INFORMATION ABOUT THE TYPE OF EVENT

Indicate type of event (in case of individual incident reports if submitting separate Summary report include count of entries)

Cyber threat ▼

 Save and close  Save and keep editing  Save and next  Share crossborder  Cancel

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

DESCRIBE INCIDENT:

General *	Type	Details
-----------	------	---------

2. TYPE

INFORMATION ABOUT THE TYPE OF EVENT

Indicate type of event (in case of individual incident reports if submitting separate Summary report include count of entries)

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.

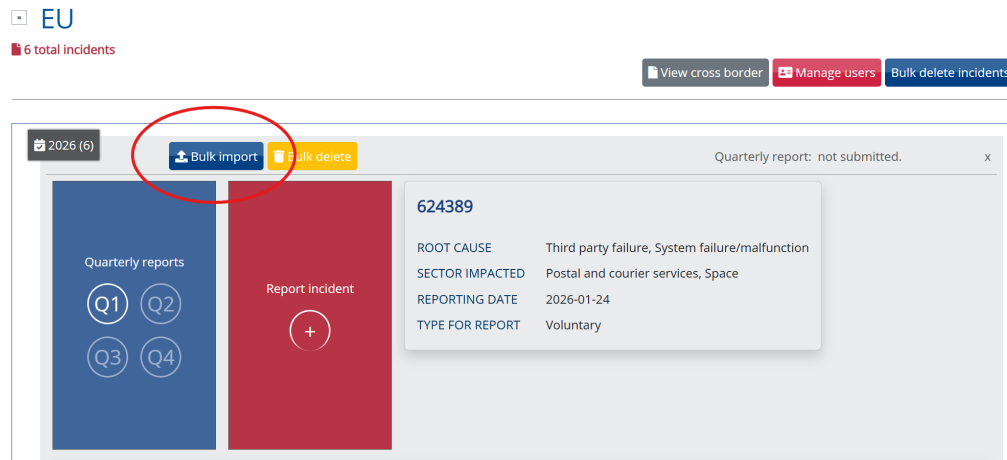
To get to the import page, login with your EU login account and go to summary report

Choose breach reporting process

ENISA maintains CIRAS, the Cybersecurity Incident Reporting and Analysis System, to support the MS in submitting incident reports. If you have an account for CIRAS and want to enter new cybersecurity incident reports, then choose the relevant breach reporting process below to access your country page in CIRAS. If you do not have a CIRAS account and want to see EU-wide aggregated data about cybersecurity incidents, then use the visualization tool below. If you have trouble accessing CIRAS with your account, or if you want to get an account, please [contact us](#).



Select your country and choose bulk import.



This is how the page should look like

IMPORTING INCIDENT REPORTS FOR 2025

Please follow the steps below:

1. Download the bulk import template from here: [Download template \(XLS\)](#), [Download template \(JSON\)](#)
2. Fill in incident data, in each sheet depending on incident type.
3. When done, upload the file below and click "Save".

NOTE: 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.

FIELD INSTRUCTIONS

Download a file with auto generated sample data: [Download sample template \(XLS\)](#), [Download sample template \(JSON\)](#)

Download the JSON schema for the import file: [Download the JSON schema](#).

The sample template has multiple sheets, one per each type of incident. Please input one incident report per row, using the formats described below. Some sheets (incident types) may not include all fields.

The table below lists all possible import fields for this article.

C.1.2. Select file to import

XLS or JSON File •

Choose File No file chosen

Save Cancel

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”

- Include in quarterly report for Q1?
Will use the imported incidents to submit the quarterly report for the next available quarter.

Quarterly report conclusions

If choosing to include in quarterly report, please provide the conclusions.

Save Cancel

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.**

Choose breach reporting process

ENISA maintains CIRAS, the Cybersecurity Incident Reporting and Analysis System, to support the MS in submitting incident reports. If you have an account for CIRAS and want to enter new cybersecurity incident reports, then choose the relevant breach reporting process below to access your country page in CIRAS. If you do not have a CIRAS account and want to see EU-wide aggregated data about cybersecurity incidents, then use the visualization tool below. If you have trouble accessing CIRAS with your account, or if you want to get an account, please [contact us](#).



D.1.2. Select your country

Summary Report



You will be presented with this page (Austria selected)

[Home](#) [Consolidated reporting](#)

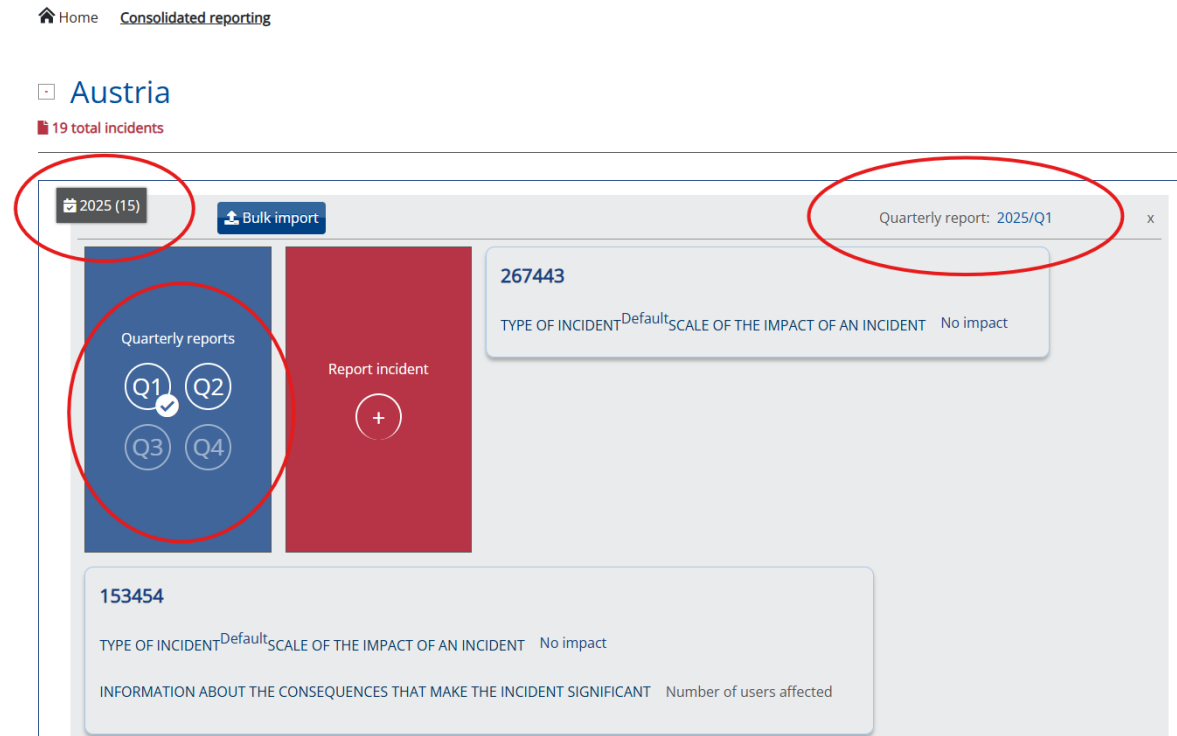
[Austria](#)

19 total incidents

A screenshot of the CIRAS interface for Austria. At the top, there is a navigation bar with "Home" and "Consolidated reporting". Below that, the country "Austria" is selected, showing "19 total incidents". The main content area is titled "2025 (15)" and "Quarterly report: 2025/Q1". It features a "Bulk import" button and a "Report incident" button. A large red box contains the number "267443" and the text "TYPE OF INCIDENT Default SCALE OF THE IMPACT OF AN INCIDENT No impact". Below this, another large red box contains the number "153454" and the text "TYPE OF INCIDENT Default SCALE OF THE IMPACT OF AN INCIDENT No impact" and "INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT Number of users affected". On the left, there are four circular icons for quarterly reports: Q1 (checked), Q2, Q3, and Q4.

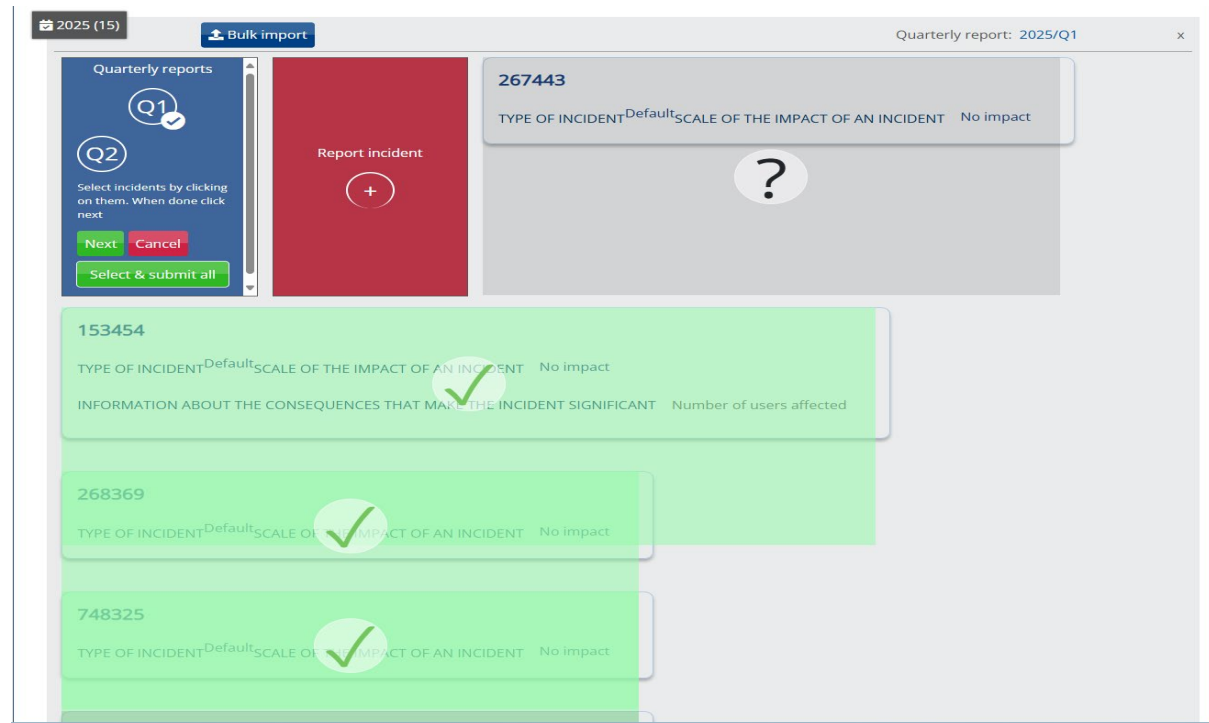
D.1.3. Select the button representing the quarter

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



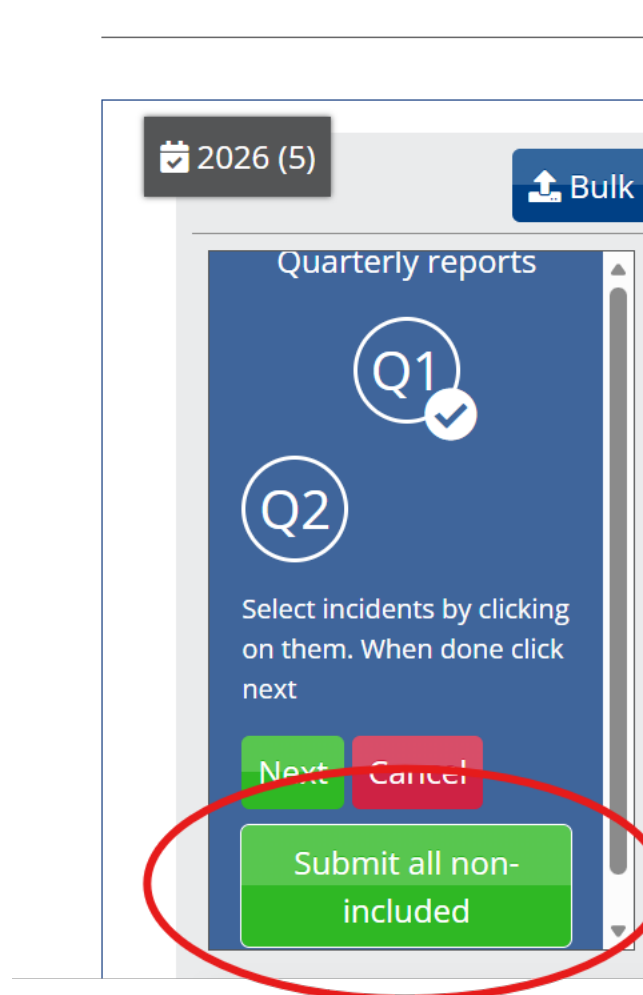
D.1.4. Select the incidents to be included in the quarterly report

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.

Q2 2025 Summary Report Austria

The total number of incidents are **3**. Please provide some additional information and click **Submit**.

CONCLUSIONS

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.

The screenshot displays the incident reporting interface. At the top left, there is a calendar icon and the text "2025 (15)". Next to it is a "Bulk import" button. On the right side of the top bar, a dropdown menu is open, showing "Quarterly report: 2025/Q1 2025/Q2" with a close button (x). Below this, there are two main panels: a blue "Quarterly reports" panel with buttons for Q1, Q2, Q3, and Q4 (Q1 and Q2 have checkmarks), and a red "Report incident" panel with a plus sign. The main content area shows a list of incidents. The first incident has ID "267443" and details: "TYPE OF INCIDENT^{Default} SCALE OF THE IMPACT OF AN INCIDENT No impact". The second incident has ID "153454" and details: "TYPE OF INCIDENT^{Default} SCALE OF THE IMPACT OF AN INCIDENT No impact" and "INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT Number of users affected". A green badge next to the second incident reads "In report: 2025/Q2". Red circles highlight the "Quarterly reports" panel, the dropdown menu, and the "In report: 2025/Q2" badge.

D.1.7. Quarterly report management

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

2025 (15) Bulk import Quarterly report: 2025/Q1 2025/Q2 x

Quarterly reports

Q1 Q2 Q3 Q4

Report incident +

267443

TYPE OF INCIDENT^{Default}SCALE OF THE IMPACT OF AN INCIDENT No impact

153454 In report: 2025/Q2

TYPE OF INCIDENT^{Default}SCALE OF THE IMPACT OF AN INCIDENT No impact

INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT Number of users affected

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.

Q2 2025 Summary Report Austria

Total number of incidents included: 1

Download XML Download PDF Country page Delete quarterly report

153454 In report: 2025/Q2

TYPE OF INCIDENT^{Default}SCALE OF THE IMPACT OF AN INCIDENT No impact

INFORMATION ABOUT THE CONSEQUENCES THAT MAKE THE INCIDENT SIGNIFICANT Number of users affected

D.1.7.2. Download a quarterly report

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

E. User Management

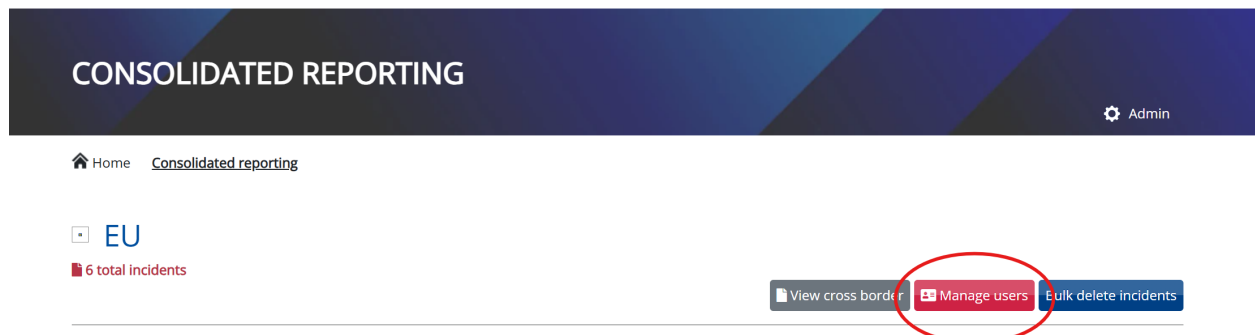
User Management allows one or many designated user(s) to manage users for a specific country.

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

GRANT ROLE

Select user

Grant the following role:

[Grant access](#)

ACCESS PER ROLE

SPOC

- ✓ Edit own country incidents
- ✓ View own country incidents
- ✓ View incidents shared with their country
- ✓ Administer own country
- ✓ Delete own country incidents
- ✓ View own country
- ✓ View any published incident
- ✓ View own country logs
- ✓ Add incidents in own country

MS NCA

- ✓ Edit own country incidents
- ✓ View own country incidents
- ✓ View any published incident
- ✓ View incidents shared with their country
- ✓ View own country
- ✓ Delete own country incidents
- ✓ Add incidents in own country

MS CSIRT

- ✓ View incidents shared with their country
- ✓ View own country
- ✓ View own country incidents

[Manage roles](#)

GRANTED ROLES

User ID	Name	Email	Role(s)
inaydero	Rossen NAYDENOV	Rossen.Naydenov@enisa.europa.eu	<ul style="list-style-type: none"> • SPOC Revoke
n005gjkx	Rossen Naydenov	rossen@naydenovi.net	<ul style="list-style-type: none"> • MS NCA (Sector: Energy) Revoke • MS NCA (Sector: Transport) Revoke

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.



EU - Manage role policies within EU

[Back to country users](#)

[Back to country page](#)

SPOC

- View own country incidents
- Edit own country incidents
- Add incidents in own country
- Delete own country incidents

View incidents shared with their country

- View any published incident
- Administer own country
- View own country
- View own country logs

MS NCA

- View own country incidents
- Edit own country incidents
- Add incidents in own country
- Delete own country incidents

View incidents shared with their country

- View any published incident
- Administer own country
- View own country
- View own country logs

[Save MS NCA changes](#)

MS CSIRT

- View own country incidents
- Edit own country incidents
- Add incidents in own country
- Delete own country incidents

View incidents shared with their country

- View any published incident
- Administer own country
- View own country
- View own country logs

[Save MS CSIRT changes](#)

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.