Guide for the Article13a Incident Reporting

Table of Contents

1 Introduction

This document is twofold a manual for using CIRAS v2.0, the incident reporting tool developed for the Article 13a incident reporting, and also a procedure document which provides the information about the overall annual reporting procedure.

1.1 Summary of the technical architecture

The incident reporting tool is called CIRAS, which stands for Cyber Incident Reporting and Analysis System. The functionality of CIRAS is based on requirements collected via a survey across all NRAs and subsequent change requests, discussed and agreed with NRAs. CIRAS was developed to replace the system used for the annual reporting in 2012, which was based on PDF forms and email.

The CIRAS software is basically a collection of Python classes, developed as an extension of a specific Plone instance at https://resilience.enisa.europa.eu. Plone is an online content-management system, which is open-source and based on Python (a so-called 3rd generation programming language).

The first version of CIRAS was developed at the end of 2012 by an external software development company. Later a second company carried out functional tests and performance tests and a third company carried out a security scan of CIRAS and the entire Plone instance. Most NRAs were involved in a pilot with this software. The software was released in production at the end of 2012, and runs in a datacentre of GTS, one of the largest hosting providers of Central Europe.

Through the years CIRAS has evolved to a more complete tool, adding many functionalities. Among them are the data visualisation, provider-to-provider incident sharing, batch import/export of incident reports, updated graphic user interface.

In 2016 a new updated version of CIRAS, CIRAS 2.0, was introduced combining all these functionalities under a more enhanced user experience.

1.2 User authorization for CIRAS

Users need an account for the portal at http://resilience.enisa.europa.eu. If you do not already have such an account please send us an email, explaining for each user who needs access, the names of the user, their affiliation and their email address.

If you already have an account for the portal at http://resilience.enisa.europa.eu this account needs to be authorized for using the reporting tool for your country. In that case send an email to article13@enisa.europa.eu providing us with the user names of the people in your organization who should have access to the incident reporting tool. We will authorize these user names and send you a confirmation.

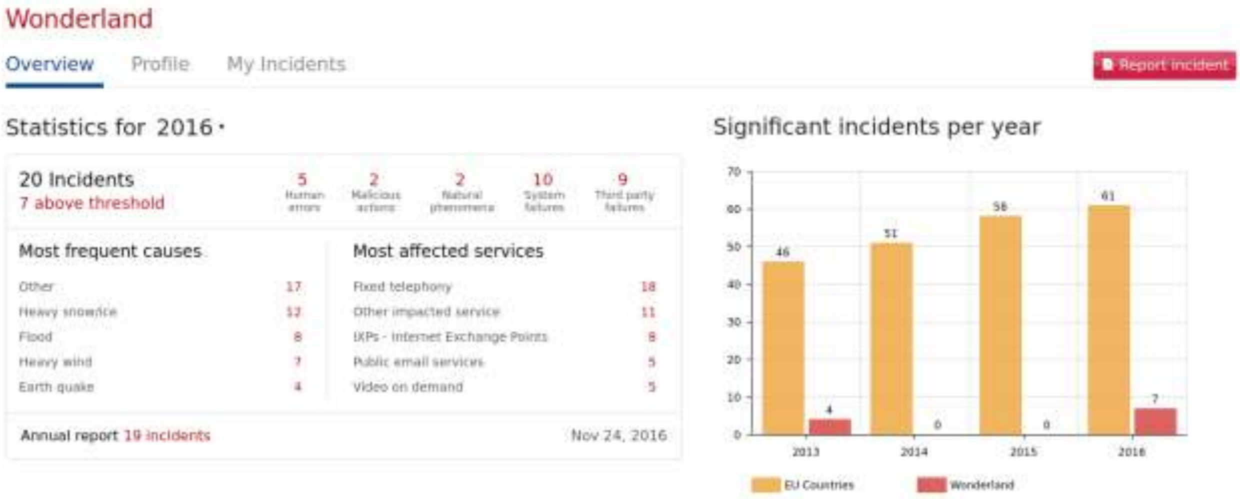
You can also add or remove authorizations later, by sending an email to article13@enisa.europa.eu.

In the next chapter you will find a guide for using CIRAS 2.0.

2 Country

Browse to https://resilience.enisa.europa.eu/article-13/reporting-tool or visit https://resilience.enisa.europa.eu and login through the box on bottom right of the landing page and go to the menu item: Article13a → Reporting tool.

You now see the country page (see Figure 1). This is the main page for NRAs. From here users can a) have an **overview** of country statistics for each year, b) view and edit **country profile** information and c) view and edit **incident** reports.



Statistics for 2016 ▾

20 Incidents
7 above threshold

5	2	2	10	9
Human errors	Malicious actions	Natural phenomena	System failures	Third party failures

Most frequent causes		Most affected services	
Other	17	Fixed telephony	18
Heavy snow/ice	12	Other impacted service	11
Flood	8	IXPs - Internet Exchange Points	8
Heavy wind	7	Public email services	5
Earth quake	4	Video on demand	5

Annual report 19 incidents — Nov 24, 2016

Significant incidents per year

Figure 1- Overview

2.1 Overview

The Overview page is divided in two main areas. On the left side, where **statistics** for a defined year appear and on the right side, where the **significant incidents per year** appear.

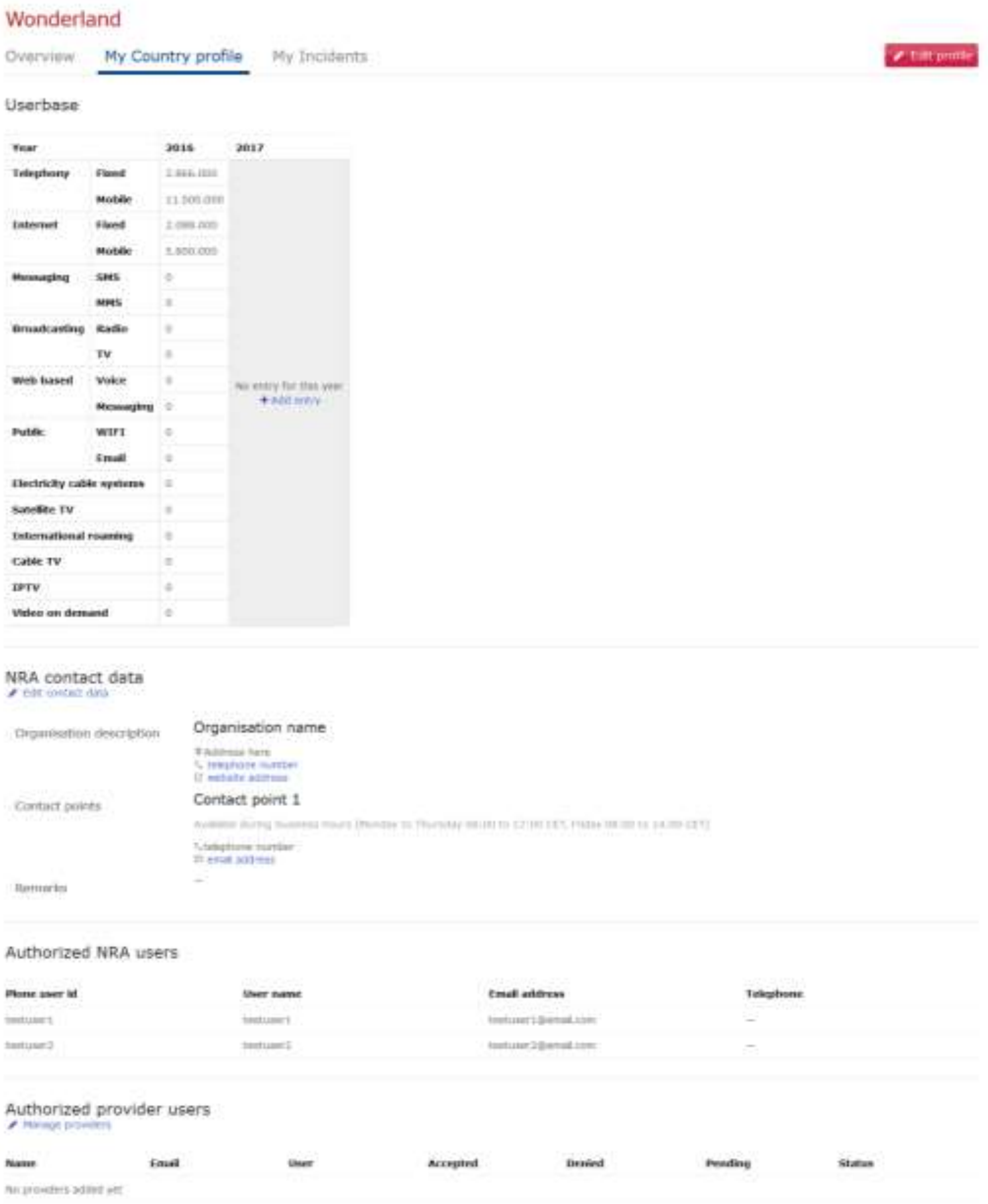
On the left side, displays a set of statistics for each year where annual incident reports have been submitted (must include at least one incident report). The user is able to select through the dropdown menu the year for display. By default, the current year is selected. Once the user selects the year, statistics on the left side are updated and the table updates and shows the following info:

- Number of incidents in total and number of incident above EU thresholds.
- Number of incidents per root cause.
- Top five most frequent subsequent causes and top five most affected services.
- Number of incidents in annual report and date of submission.

On the right side, a bar chart shows the total number of EU incidents above EU thresholds versus the total number of national incidents above EU thresholds for the last four years.

Finally, on the bottom side of the overview page, a log shows the last actions performed on the country page in general. The user can load more logs by clicking the blue button “Load more”.

2.2 My Country Profile



Wonderland

Userbase

Year		2016	2017
Telephony	Fixed	2.866.000	No entry for this year + Add entry
	Mobile	11.500.000	
Internet	Fixed	2.088.000	
	Mobile	5.800.000	
Messaging	SMS	0	
	MMS	0	
Broadcasting	Radio	0	
	TV	0	
Web based	Voice	0	
	Messaging	0	
Public	WIFI	0	
	Email	0	
Electricity cable systems		0	
Satellite TV		0	
International roaming		0	
Cable TV		0	
IPTV		0	
Video on demand		0	

NRA contact data

Organisation description	Organisation name Address here telephone number website address
Contact points	Contact point 1 Available during business hours (Monday to Thursday 08:00 to 17:00 CET, Friday 08:00 to 14:00 CET) telephone number email address
Remarks	–

Authorized NRA users

Phone user id	User name	Email address	Telephone
testuser1	testuser1	testuser1@email.com	–
testuser2	testuser2	testuser2@email.com	–

Authorized provider users

Name	Email	User	Accepted	Denied	Pending	Status
No providers added yet						

Figure 2 My Country profile

This page contains/allows Information about a country profile. More specifically, this page shows the following information about the country:

- *User base definitions* - used for determining the significant EU incidents as well as graph generation in the Data Visualization section of the Incident search section. User bases must be provided per year.
- *NRA contact data* - contact information about NRA and contact points to be used by ENISA and other NRAs.

- *Authorized NRA users* - a list of all NRA users that have been granted access for a particular country.
- *Authorized provider users* - a list of all assigned providers and the status of their incidents in the P2P workflow.

2.2.1 Edit profile

Edit Profile area can be accessed by clicking on the "*Edit profile*" button on the "My Country profile" page, or by clicking the "*Edit contact data*" link in the "*NRA contact data*" section of the same page.

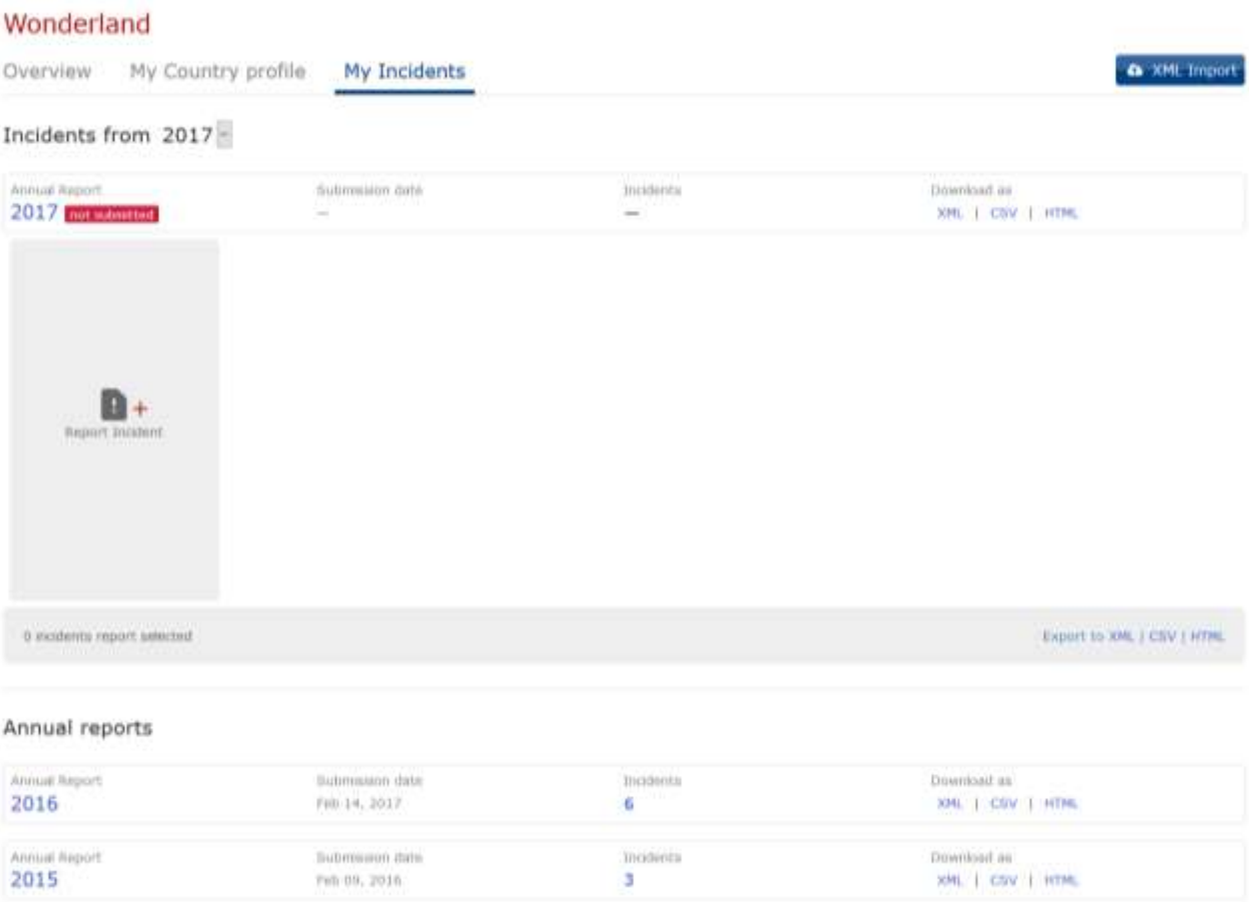
On this page the following can be edited:

- User base definitions per year
- Description of the organization (NRA)
- Contact data
- Additional remarks

Apart from the user base, all other info entered here will be displayed on the "*NRA contact list*" page.

Modifying the user base will affect calculations regarding significant incidents as well as the graphs generated in the *Data Visualization* section of the incident search. It is the responsibility of the NRAs to keep this data up to date.

2.3 My Incidents



Wonderland

Incidents from 2017

Annual Report	Submission date	Incidents	Download as
2017 not submitted	—	—	XML | CSV | HTML

0 incidents report selected

Annual reports

Annual Report	Submission date	Incidents	Download as
2016	Feb 14, 2017	6	XML | CSV | HTML
2015	Feb 09, 2016	3	XML | CSV | HTML

Figure 3 My Incidents

The last tab of the Country page is “My Incidents” section which displays, per each year, incidents and annual reports submitted. The user can perform the following actions through that page:

- Report a new incident.
- View / edit / delete an existing incident report.
- Submit or retract an annual report (only available for the current and last year).
- Export incident reports and annual reports in the following formats: XML, CSV and/or HTML.
- XML Import of incidents from an external system that can comply with the format used by CIRAS.

On the top of that page a status of the latest annual report is displayed. A ribbon displays the year of the latest annual report, its status, the number of incidents included and the date of submission.

My Incidents page shows a button that allows a user to Add an Incident Report for the current year. Moreover, in case the user has already submitted incident reports they appear in that section. The user is able to select the year and the area is updated with the corresponding data/incident reports. In case there are incident reports for the last year to be submitted in an annual report a blue button “Submit annual report” will appear. In case no incident reports for the last year and an annual report has to be submitted for that year a button “Submit empty report” will appear.

Under the section of Incident Reports, the user can see all the past annual reports; each one summarized in a ribbon. Clicking the incident count in an annual report will navigate to the incident search page with the correct filters selected to display those particular incident reports. Clicking the incident ID will navigate to that particular incident.

More details about incident reporting procedure are described on the following sections.

2.3.1 Report a new incident

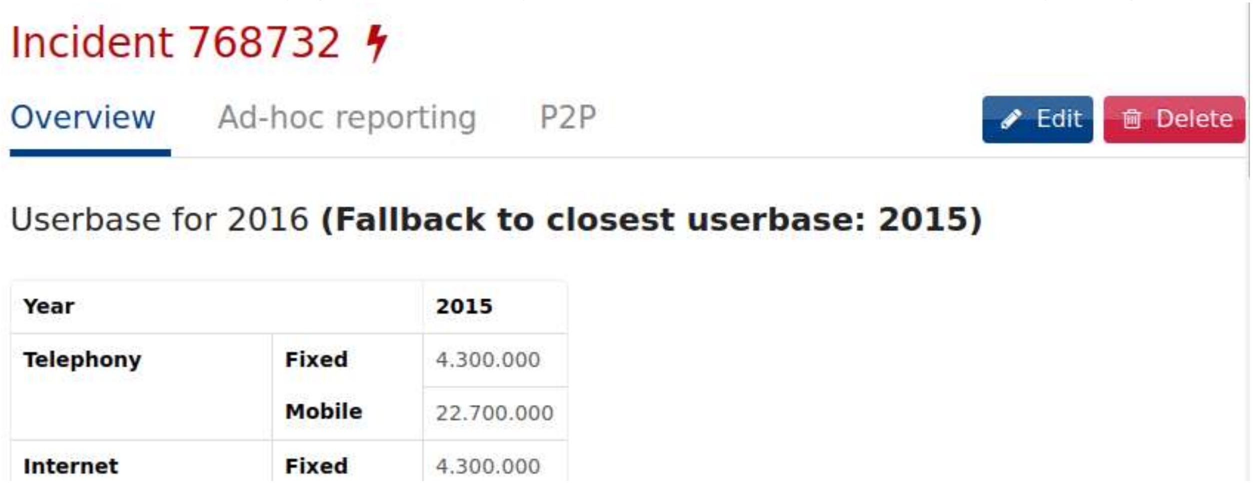
See Chapter 3.

2.3.2 View incident reports

An incident report can be accessed through multiple ways: logs, search results, country incidents page, providers page, links submitted in email reports. Incident Report page displays the details of a particular incident report and has the look of Figure 4 below. Incident Report is always followed by a unique ID and an icon of a thunder flag is visible in case this is an incident report that exceeds the informal EU thresholds. View mode of an Incident Report is available to all NRA users, while the incident report owner has also edit and delete rights. Incident Report consist of three main action categories, **Overview** of the Incident Report, **Ad-hoc Reporting** and **P2P** (Provider to Provider) sharing. More details on each one of them is described on the following sections.

2.3.2.1 Overview

The incident overview page shows the **userbase** for the incident’s year (this is the same userbase used for calculations). From this page, an incident report can be edited, deleted or included in a pending annual report.



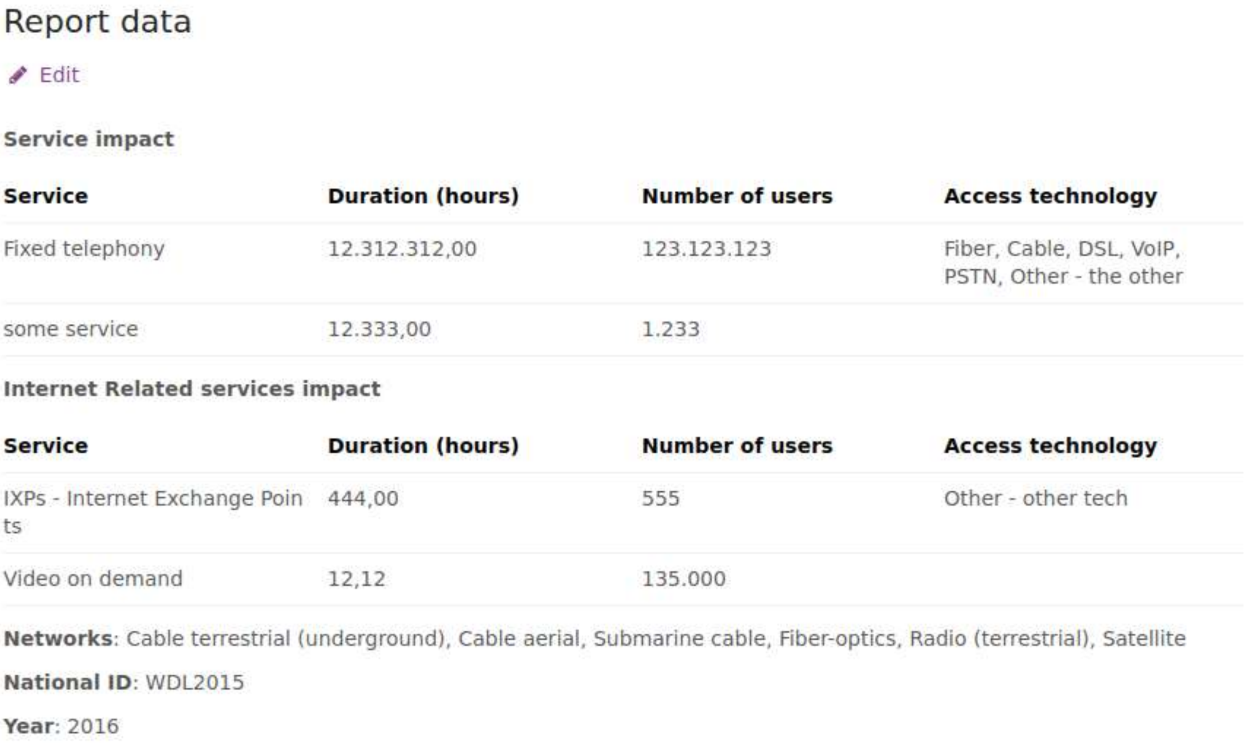
Userbase for 2016 **(Fallback to closest userbase: 2015)**

Year		**2015**
Telephony	**Fixed**	4.300.000
	Mobile	22.700.000
Internet	**Fixed**	4.300.000

Figure 4 Incident report page

Note: If there is no user base definition for the incident’s year, the closest available user base will be used, when this happens the title of the section will also include the fallback user base used.

The **report data** section displays the information contained in the incident report as well as an edit link.



Report data

Service impact

Service	Duration (hours)	Number of users	Access technology
Fixed telephony	12.312.312,00	123.123.123	Fiber, Cable, DSL, VoIP, PSTN, Other - the other
some service	12.333,00	1.233	

Internet Related services impact

Service	Duration (hours)	Number of users	Access technology
IXPs - Internet Exchange Poin ts	444,00	555	Other - other tech
Video on demand	12,12	135.000	

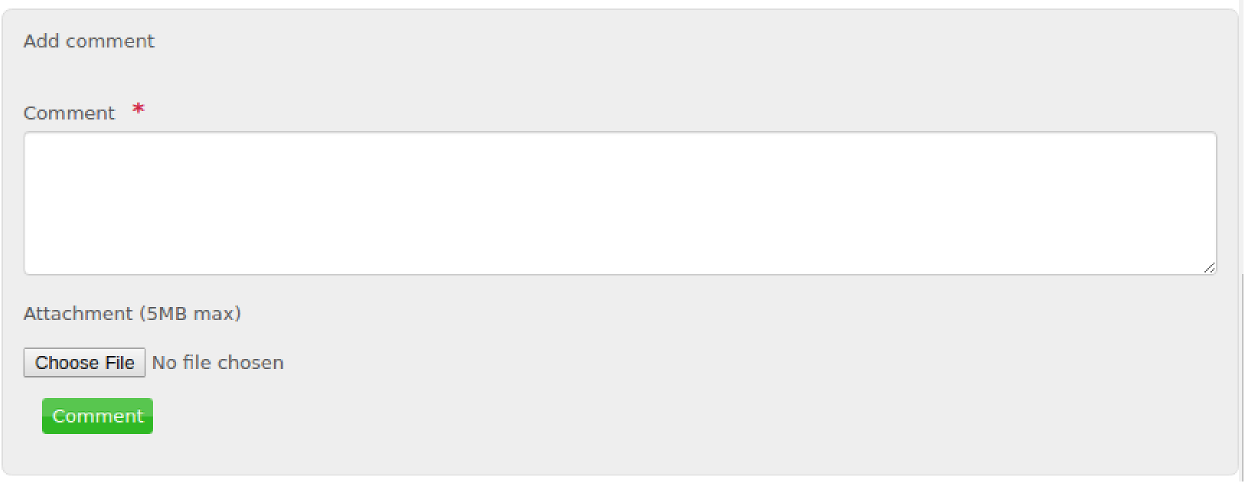
Networks: Cable terrestrial (underground), Cable aerial, Submarine cable, Fiber-optics, Radio (terrestrial), Satellite

National ID: WDL2015

Year: 2016

Figure 5 Report Data

This page also allows for NRAs to post **comments** regarding the current incident report.



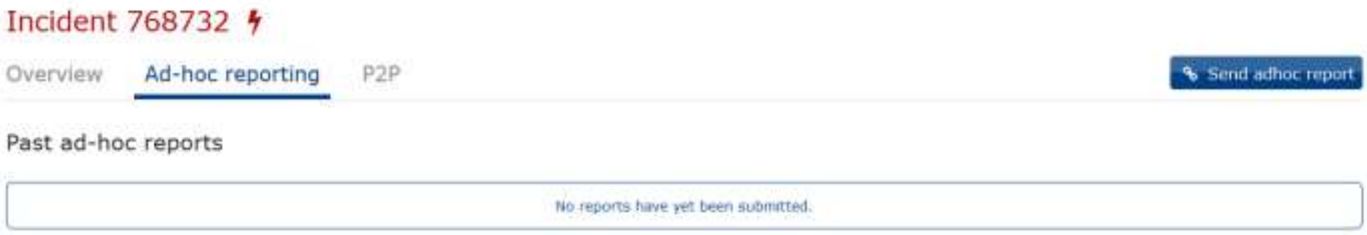
Add comment

Comment *

Attachment (5MB max)

Figure 6 Add Comment area

2.3.2.2 Ad-hoc reporting



Past ad-hoc reports

No reports have yet been submitted.

Figure 7 Ad-hoc reporting

Ad-hoc reporting gives to NRAs the opportunity to share among NRAs of other countries incident reports.

This mechanism allows the NRAs to notify other NRAs from other countries about incidents that had a cross-border impact.

This is what happens when an ad-hoc report is submitted:

- A new "*Ad-hoc*" report is created, containing a snapshot of the incident.
- The selected countries receive an email notification with the attached report exported in various formats (XML, CSV and HTML). The country the incident report belongs to will be disclosed in this way.
- The incident report becomes "shared" with all countries; meaning it will appear in incident report searches for all NRAs and be accessible via direct link. The country the incident belongs is not disclosed.

Once at least an ad-hoc report is submitted, a table listing previous ad-hoc report submissions will be displayed. A "*Revoke access*" button will revoke access to the current incident report for all NRAs (unless it is included in a submitted annual report) and **delete** all ad-hoc reports associated with it.

Submitting a new ad-hoc report will create another snapshot and re-send emails as well as allow view access to other NRAs.

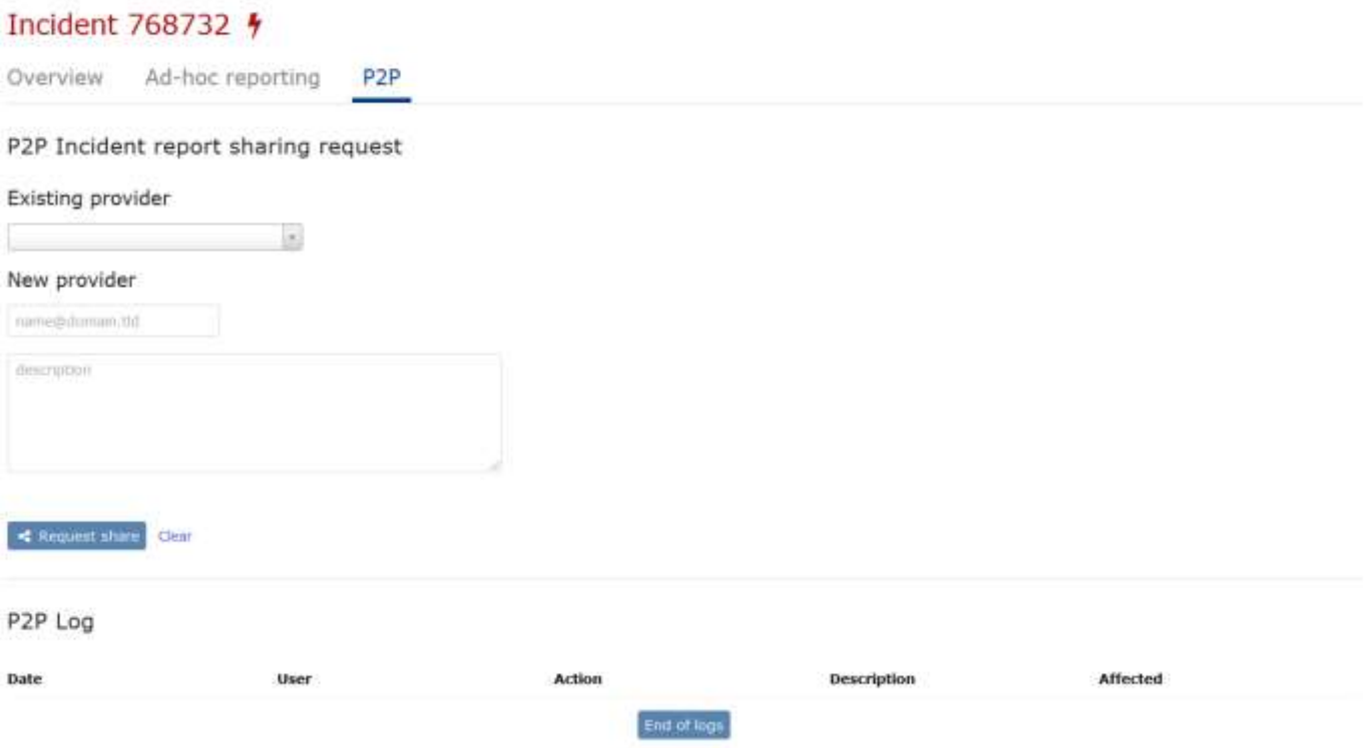
2.3.2.3 P2P – Cross EU Provider to Provider Sharing

The Provider 2 Provider (P2P) functionality is an extension of the incident reporting tool CIRAS, which enables Cross-EU Provider to provider sharing of incident reports. In short, it allows NRAs to request the provider, who is the incident owner, to share an incident report with the providers of other countries. Sharing of incident reports remain anonymous until the two providers mutually agree to contact each other.

The flow of the P2P functionality is described below:

- **P2P sharing request from NRA**

NRA browses incident reports in CIRAS and discovers an interesting incident that would like to share with other providers subscribed in CIRAS. NRA will open that incident report an d will navigate to the P2P tab in order to request from the provider -the incident owner- to share the incident report with other providers. This provider can be an existing provider (already enrolled in the system) or a new provider, but in any case it is a provider from the same country as the NRA who has reported this particular incident. The provided is either already created through the "*Providers*" page or is created at the time NRA adds a new Provider by email address. In the latter case, where a new provider is added, an account will be created automatically by the system. Figure 8 depicts the P2P sharing request form that NRA submits to initiate the request. It has to be noted that it is under the responsibility of the NRA to input and/or select the corresponding email of the provider and needs to perform this action with the necessary care so to not send the incident sharing request to the wrong provider.


Incident 768732

P2P Incident report sharing request

Existing provider

New provider

name@domain.tld

description

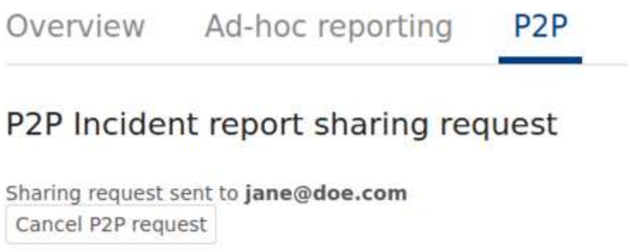
P2P Log

Date	User	Action	Description	Affected

Figure 8 P2P Incident Report Sharing

Afterwards, provider will receive a notification email informing about the pending sharing request. The newly added provider will receive two emails, an email to get enrolled in the resilience portal where follows the link to set a password and activate its account and an email to approve or reject the sharing request. Alternatively, the provider can access its own dashboard and either approve or reject the P2P sharing request. Moreover, the provider can check its current approved and denied incident reports and navigate to the shared incident reports of other providers. NRA can view a summary of approved and rejected requests in the "*Providers*" section. Additionaly, an email notification will arrive at NRA's mailbox once the provide approves or rejects the incident report sharing request.

Once a sharing request has been issued to a Provider, NRA can cancel the request at any time by clicking on the "*Cancel P2P request*" button (see figure 9). The provider will be notified about the cancellation.

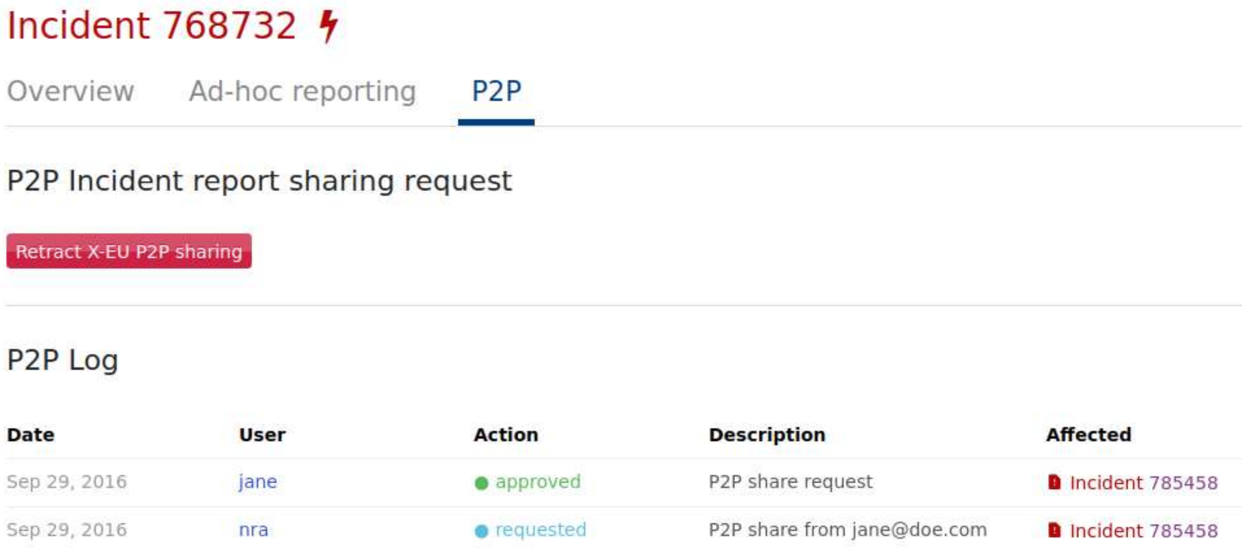


P2P Incident report sharing request

Sharing request sent to **jane@doe.com**

Figure 9 P2P Cancel request

In case an incident report has already been approved by the provider an NRA can retract it from P2P sharing by clicking the "Retract X-EU P2P sharing" button. This will not count towards the accepted/denied count for the provider, see figure 10.



Incident 768732

P2P Incident report sharing request

P2P Log

Date	User	Action	Description	Affected
Sep 29, 2016	jane	● approved	P2P share request	Incident 785458
Sep 29, 2016	nra	● requested	P2P share from jane@doe.com	Incident 785458

Figure 10 P2P Retract Sharing

Foreign NRA P2P sharing request is also available in CIRAS to enable NRAs from other countries to initiate an incident report sharing request. Therefore, when an NRA is browsing an incident report which is submitted by another country and wants to share it with other providers can generate an incident sharing request which will be sent to the appropriate NRA who submitted that incident report. Then the other NRA will follow the steps as described before to initiate the sharing request towards the provider/incident owner. Foreign NRA P2P sharing request is available to each foreign NRA once per day.

Contact Provider is part of the P2P functionality and facilitates information sharing among providers from either the same or different countries. The flow of that functionality is described below in steps:

Provider **A** can begin a contact request by typing in a message and clicking on "Contact provider". This will start the following workflow:

- A new contact request content type will be created to handle the exchanges between Provider **A** and Provider **B**.
- An email will be sent to Provider **B** informing them of the contact request and the message.
- Provider **B** can approve or reject the contact request.
- If Provider **B** approves the contact request Provider **A** will be asked for their final confirmation.
  - If the request is approved and confirmed the email address of Provider **A**/**B** will be sent to Provider **B**/**A**. The providers will continue their conversation via email.
  - If the request is denied or canceled no contact information is shared.
- Incoming and outgoing contact requests also appear for providers on their Provider page.

2.3.2.4 Edit

NRAs cannot edit incident reports that are part of a submitted annual report. Administrators can edit any incident report at any time.

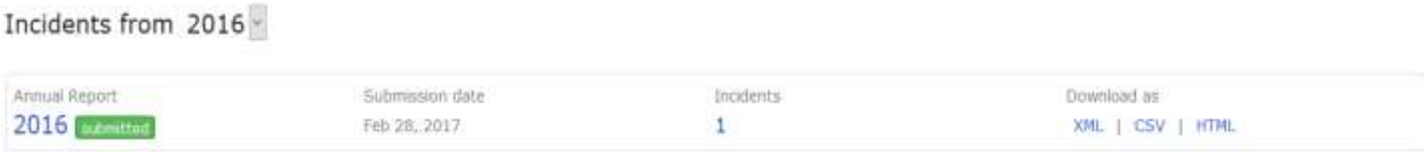
The incident edit page can be accessed from the Overview page by clicking the "*Edit*" button on top right of an Incident Report (see Figure 4) or the "*Edit*" link in the "*Report data*" section (see Figure 5).

2.3.3 Submit an annual report

Annual reports exist in a pending state until submitted. There are two types of annual reports:

- annual reports that contain incidents;
- empty annual reports.

A pending annual report can be identified by having an empty "*Submission date*" value.



Incidents from 2016

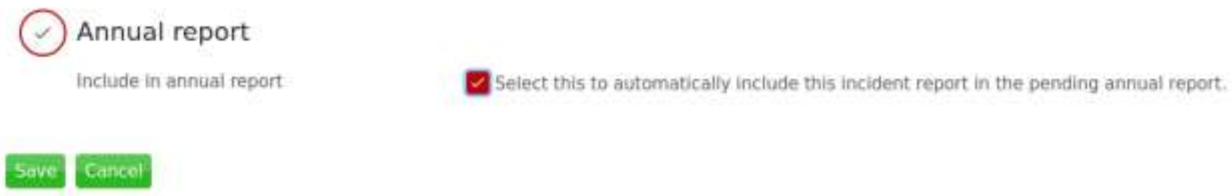
Annual Report	Submission date	Incidents	Download as
2016 submitted	Feb 28, 2017	1	XML | CSV | HTML

Figure 11 Pending Annual Report

Annual reports that contain incidents can be created with one of the following ways:

- Through the add form, when reporting a new incident by selecting the "*Include in annual report*" checkbox (see Figure 12).

- Through the edit form by selecting or deselecting the “Include in annual report” checkbox (see Figure 12).



Annual report

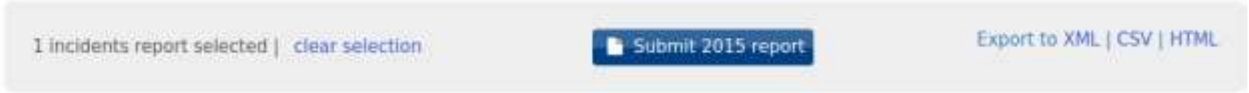
Include in annual report ☑ Select this to automatically include this incident report in the pending annual report.

Save Cancel

Figure 12 A priori inclusion in Annual Report

- Through the Incident “*Overview*” page by clicking on “*Include in annual report*” or “*Exclude from annual report*” button.

- By selecting them and clicking the “*Submit [YEAR] report*” button in the footer of the incidents display (see Figure 13).



1 incidents report selected | clear selection

Submit 2015 report

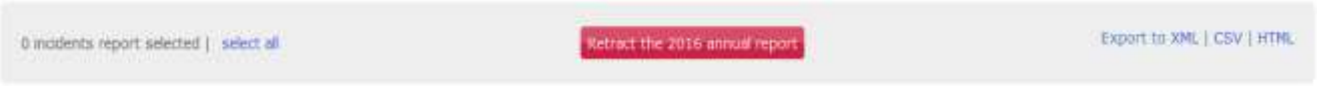
Export to XML | CSV | HTML

Figure 13 Submit Annual Report

Selecting incidents when there are already incidents assigned to a pending annual report the selected incidents will also be included in the annual report submission.

Empty annual reports can be submitted by the same blue button that appears when submitting Annual reports with incidents. In the case of empty annual reports, the blue button displays the text ‘Submit empty report”.

Retracting an annual report is necessary when NRA needs to edit an incident report that is included in an Annual Report which has been submitted already. Retracting will keep track of incident reports were included a-priori and therefore the resubmission of the Annual Report is easier for the user. This functionality is available on the area of Annual Report through the red button that replaces the blue button which appears when submitting an Annual Report.



0 incidents report selected | select all

Retract the 2016 annual report

Export to XML | CSV | HTML

Figure 14 Retract annual report

2.3.4 Export incident reports / annual reports

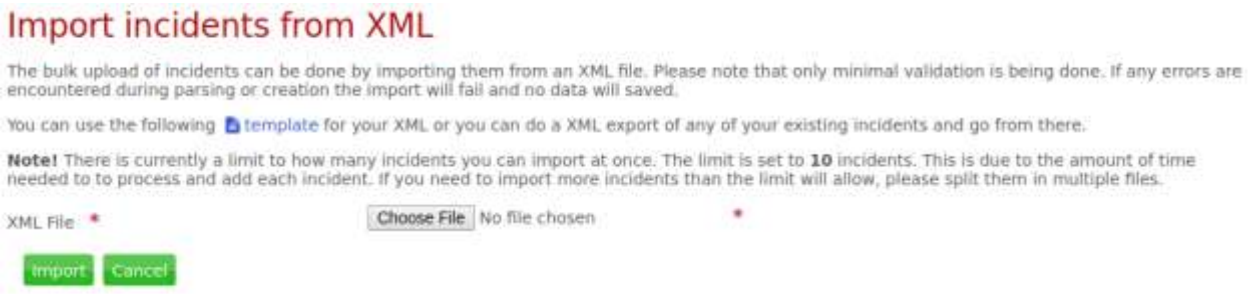
CIRAS allows the exporting of data in a structured way. Exporting mechanisms are available for both incident reports as well as for annual reports and is available through the “My Incidents” page.

Figure 13 shows on the right side the exporting of the selected incident reports to either xml, csv, or html format. The same functionality is also applicable to annual reports through the annual reports section on the same page.

2.3.5 Import incident reports through XML

This section allows the bulk upload of incident reports through XML file. There is an imposed limit to the maximum number of incident reports that can be imported at one time; and therefore the importing mechanism supports importing of 10 incidents at a time.

Clicking on the “XML Import” button on the “My Incidents” page will open a new upload form.



Import incidents from XML

The bulk upload of incidents can be done by importing them from an XML file. Please note that only minimal validation is being done. If any errors are encountered during parsing or creation the import will fail and no data will saved.

You can use the following template for your XML or you can do a XML export of any of your existing incidents and go from there.

Note! There is currently a limit to how many incidents you can import at once. The limit is set to **10** incidents. This is due to the amount of time needed to to process and add each incident. If you need to import more incidents than the limit will allow, please split them in multiple files.

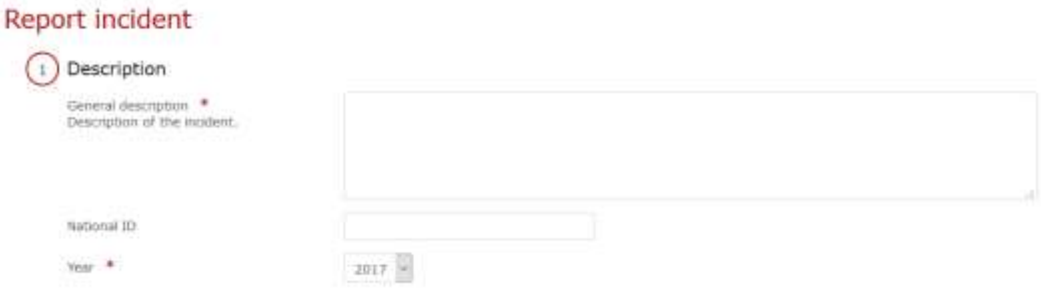
XML File * Choose File No file chosen *

Figure 15 Import Incidents from XML

The same format as for the incident XML export is used. An empty template is provided to aid the user in creating a correct XML document.

3 Report Incident

The second global menu item of CIRAS is the “Report Incident” where the user is able to fill in a form in order to report an incident. There are certain steps to follow when filling in that form. First, user needs to provide a general description and specify the year of the incident event. Optionally, the user can fill in the corresponding national id of that incident report to link the incident report on NRAs database to the incident report on CIRAS.



Report incident

1 Description

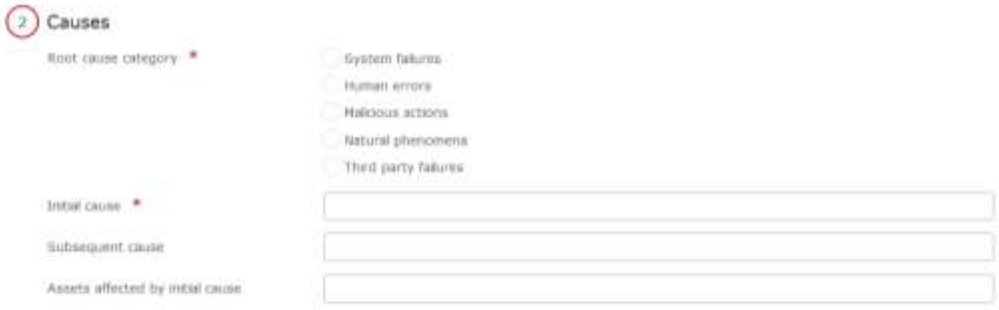
General description *
Description of the incident.

National ID

Year * 2017

Figure 16 Report Incident

Secondly, user specifies the root cause of the incident and the and the initial cause. Optionally, subsequent cause as well as assets affected can be filled in the reporting form.



2 Causes

Root cause category *
○ System failures
○ Human errors
○ Malicious actions
○ Natural phenomena
○ Third party failures

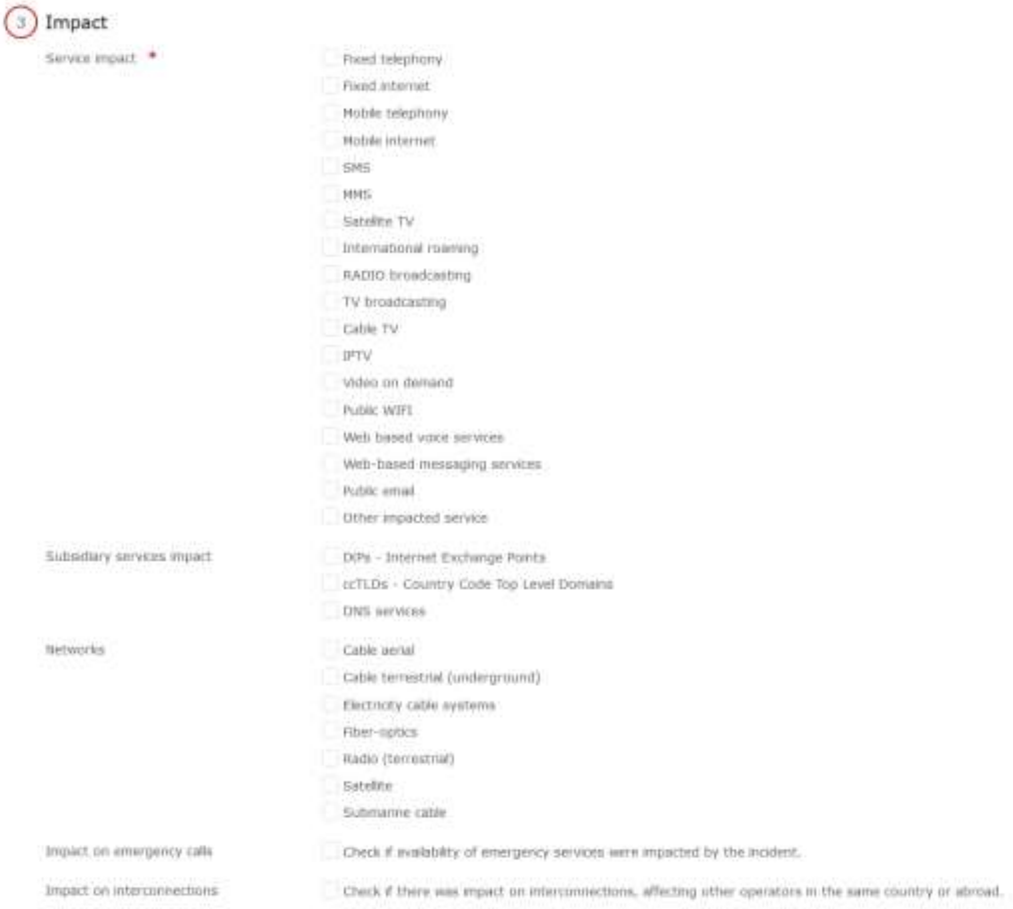
Initial cause *

Subsequent cause

Assets affected by initial cause

Figure 17 Incident Causes

Next step is to indicate the impact of the incident in terms of services and networks.



3 Impact

Service impact *
□ Fixed telephony
□ Fixed internet
□ Mobile telephony
□ Mobile internet
□ SMS
□ MMS
□ Satellite TV
□ International roaming
□ RADIO broadcasting
□ TV broadcasting
□ Cable TV
□ IPTV
□ Video on demand
□ Public WIFI
□ Web based voice services
□ Web-based messaging services
□ Public email
□ Other impacted service

Subsidiary services impact
□ IXPs - Internet Exchange Points
□ ccTLDs - Country Code Top Level Domains
□ DNS services

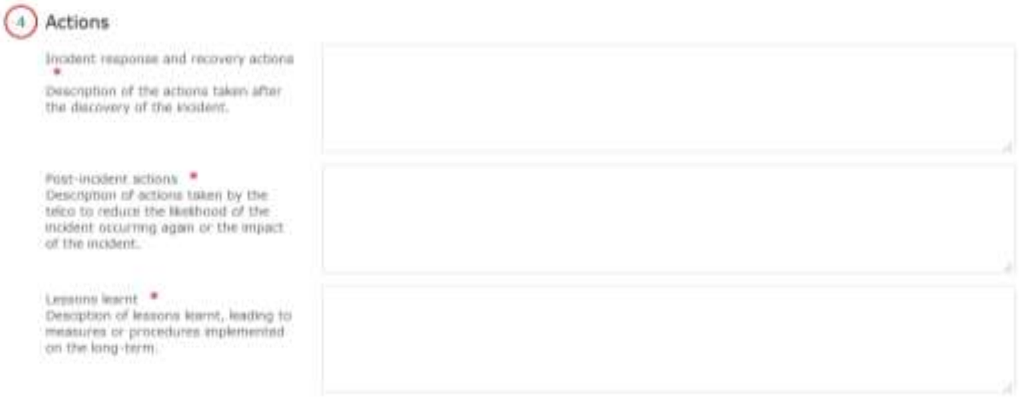
Networks
□ Cable aerial
□ Cable terrestrial (underground)
□ Electricity cable systems
□ Fiber-optics
□ Radio (terrestrial)
□ Satellite
□ Submarine cable

Impact on emergency calls
□ Check if availability of emergency services were impacted by the incident.

Impact on interconnections
□ Check if there was impact on interconnections, affecting other operators in the same country or abroad.

Figure 18 Impact on services etc.

Actions taken for the incident response, post-incident and lessons learnt are the last set of information expected from the user. These fields are filled in with free text answers.



4 Actions

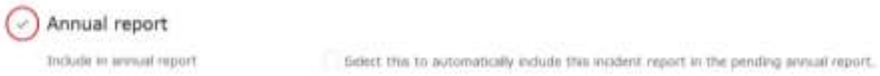
Incident response and recovery actions *
Description of the actions taken after the discovery of the incident.

Post-incident actions *
Description of actions taken by the telco to reduce the likelihood of the incident occurring again or the impact of the incident.

Lessons learnt *
Description of lessons learnt, leading to measures or procedures implemented on the long-term.

Figure 19 Actions taken

As last step, before submitting the incident report, user can specify whether this incident report will be included in the annual report of the aforementioned year.



✓ Annual report

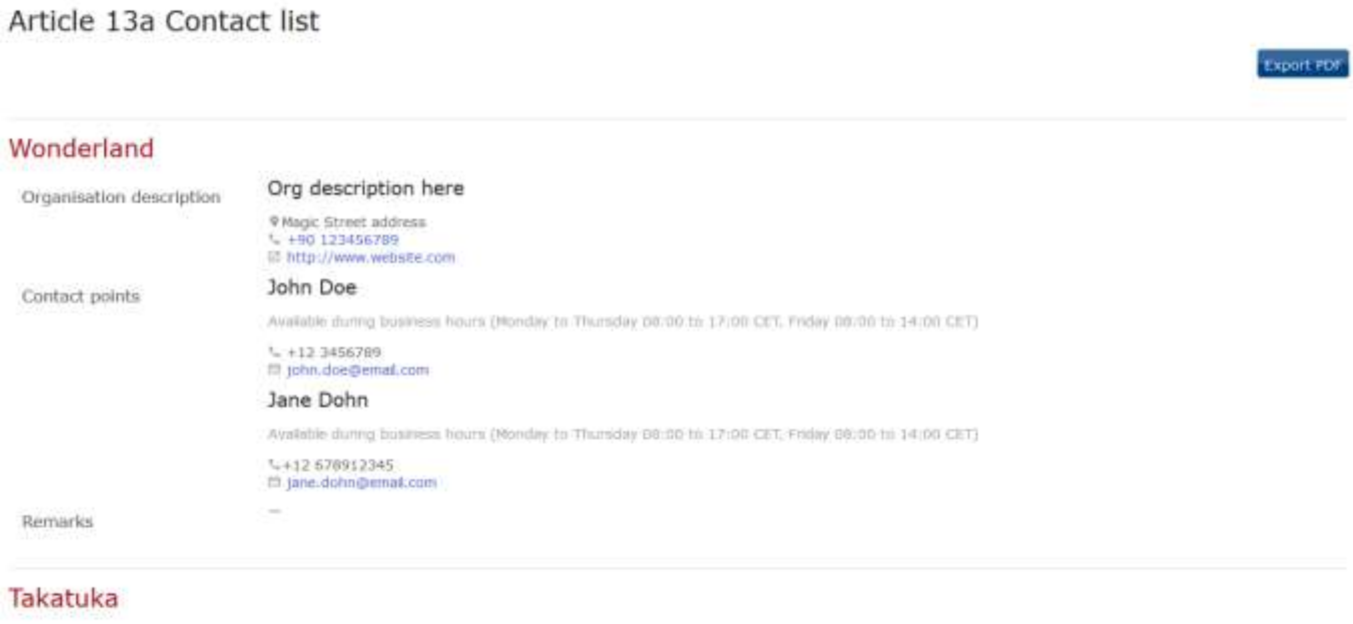
Include in annual report □ Select this to automatically include this incident report in the pending annual report.

Figure 20 Include in Annual Report

After all the above steps user can submit the incident report clicking on the submit button. Cancel button will exit the process and will navigate back to the country page.

4 NRA contact list

The global menu of NRA contact list allows the NRAs to easily access all the necessary information in order to contact with the NRAs from other EU countries. The list of the EU countries shows in alphabetical order in the webpage, while user is also able to download a pdf with all the information through the "Export PDF" button on the top right of the webpage.



Article 13a Contact list

Wonderland

Organisation description

Org description here

Magic Street address
+90 123456789
http://www.website.com

Contact points

John Doe

Available during business hours (Monday to Thursday 08:00 to 17:00 CET, Friday 08:00 to 14:00 CET)

+12 3456789
john.doe@email.com

Jane Dohn

Available during business hours (Monday to Thursday 08:00 to 17:00 CET, Friday 08:00 to 14:00 CET)

+12 678912345
jane.dohn@email.com

Remarks

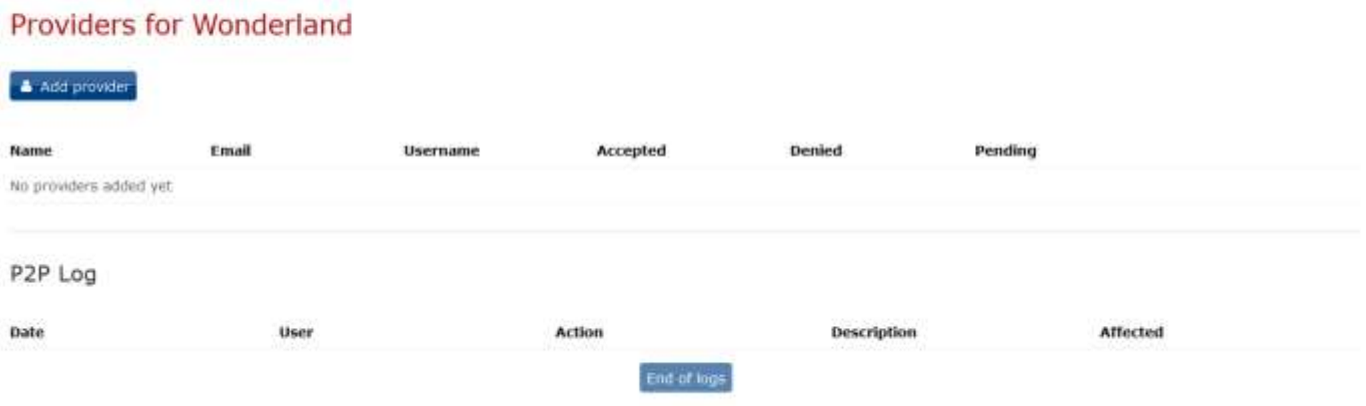
—

Takatuka

Figure 21 NRA Contact List

5 Providers

Providers page is focusing on the extra feature of CIRAS, P2P Sharing, that was analysed in the previous sections. From the global menu item of Providers an NRA can easily access a webpage where can add new provider accounts and see logs of the p2p sharing actions.



Providers for Wonderland

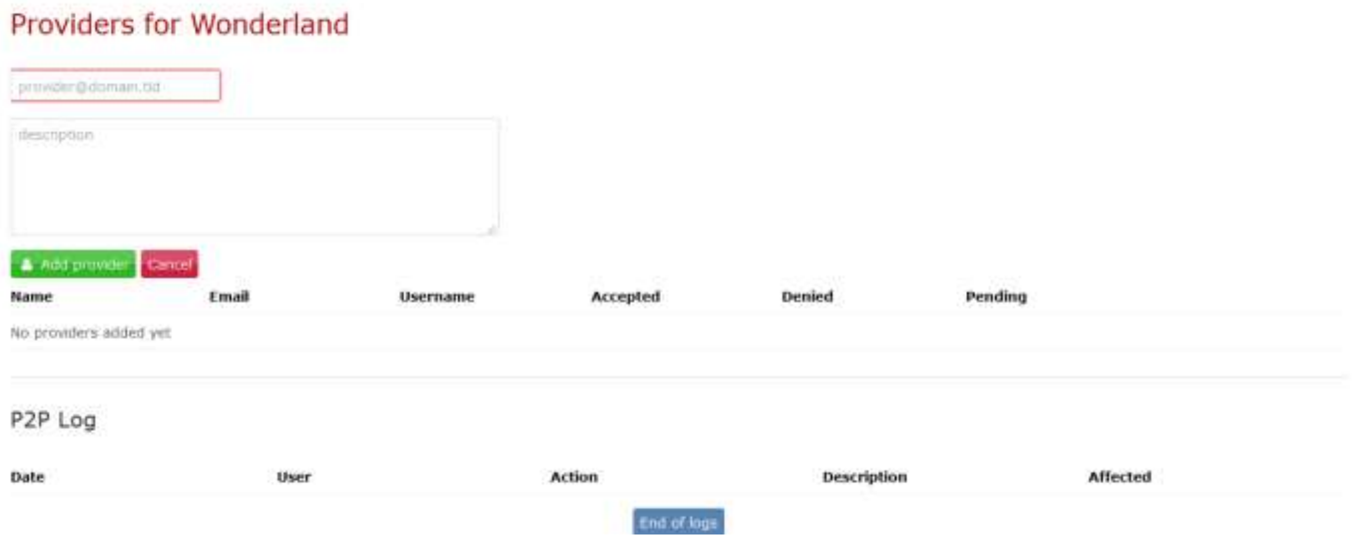
Name	Email	Username	Accepted	Denied	Pending
No providers added yet					

P2P Log

Date	User	Action	Description	Affected

Figure 22 Providers page

NRA needs to give an email address and a short description for that contact. No more information is collected so to preserve data minimization. The figure below shows the page when adding a new contact point for a telco provider from country Wonderland.



Providers for Wonderland

Name	Email	Username	Accepted	Denied	Pending
No providers added yet					

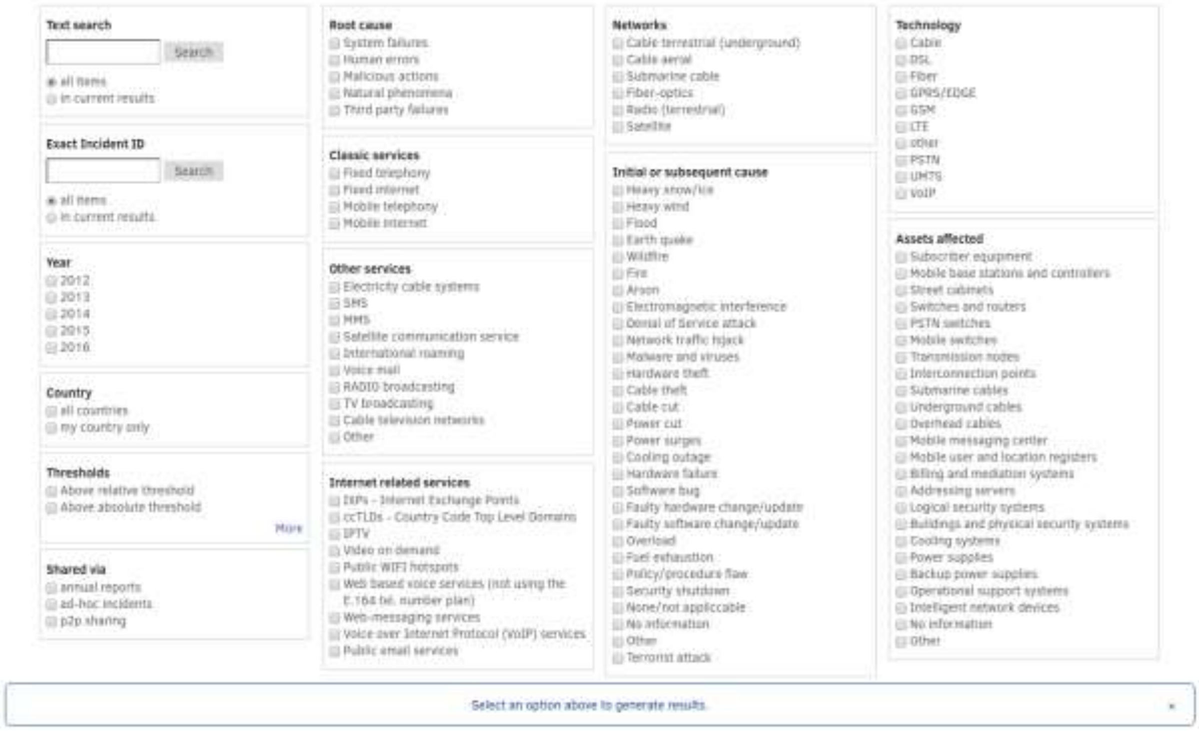
P2P Log

Date	User	Action	Description	Affected

Figure 23 Add Provider

6 Search incident reports

The search page can be accessed through the global navigation from any page by clicking on “*Search incidents*”. This page presents various filters:



Text search
Search
● all items
○ in current results

Exact Incident ID
Search
● all items
○ in current results

Year
☐ 2012
☐ 2013
☐ 2014
☐ 2015
☐ 2016

Country
☐ all countries
☐ my country only

Thresholds
☐ Above relative threshold
☐ Above absolute threshold
More

Shared via
☐ annual reports
☐ ad-hoc incidents
☐ p2p sharing

Root cause
☐ System failures
☐ Human errors
☐ Malicious actions
☐ Natural phenomena
☐ Third party failures

Classic services
☐ Fixed telephony
☐ Fixed internet
☐ Mobile telephony
☐ Mobile internet

Other services
☐ Electricity cable systems
☐ SMS
☐ MMS
☐ Satellite communication service
☐ International roaming
☐ Voice mail
☐ RADIO broadcasting
☐ TV broadcasting
☐ Cable television networks
☐ Other

Internet related services
☐ IXPs - Internet Exchange Points
☐ ccTLDs - Country Code Top Level Domains
☐ IPTV
☐ Video on demand
☐ Public WIFI hotspots
☐ Web based voice services (not using the E.164 tel. number plan)
☐ Web-messaging services
☐ Voice over Internet Protocol (VoIP) services
☐ Public email services

Networks
☐ Cable terrestrial (underground)
☐ Cable aerial
☐ Submarine cable
☐ Fiber-optics
☐ Radio (terrestrial)
☐ Satellite

Initial or subsequent cause
☐ Heavy snow/ice
☐ Heavy wind
☐ Flood
☐ Earth quake
☐ Wildfire
☐ Fire
☐ Arson
☐ Electromagoetic interference
☐ Denial of Service attack
☐ Network traffic hijack
☐ Malware and viruses
☐ Hardware theft
☐ Cable theft
☐ Cable cut
☐ Power cut
☐ Power surges
☐ Cooling outage
☐ Hardware failure
☐ Software bug
☐ Faulty hardware change/update
☐ Faulty software change/update
☐ Overload
☐ Fuel exhaustion
☐ Policy/procedure flaw
☐ Security shutdown
☐ None/not appliccable
☐ No information
☐ Other
☐ Terrorist attack

Technology
☐ Cable
☐ DSL
☐ Fiber
☐ GPRS/EDGE
☐ GSM
☐ LTE
☐ other
☐ PSTN
☐ UMTS
☐ VoIP

Assets affected
☐ Subscriber equipment
☐ Mobile base stations and controllers
☐ Street cabinets
☐ Switches and routers
☐ PSTN switches
☐ Mobile switches
☐ Transmission nodes
☐ Interconnection points
☐ Submarine cables
☐ Underground cables
☐ Overhead cables
☐ Mobile messaging center
☐ Mobile user and location registers
☐ Billing and mediation systems
☐ Addressing servers
☐ Logical security systems
☐ Buildings and physical security systems
☐ Cooling systems
☐ Power supplies
☐ Backup power supplies
☐ Operational support systems
☐ Intelligent network devices
☐ No information
☐ Other

Select an option above to generate results. ×

By default there will be no results displayed until some filters are selected . Queries may take a longer time to display, depending on selected filters.

Results are displayed beneath the filters offering two display and an export option:

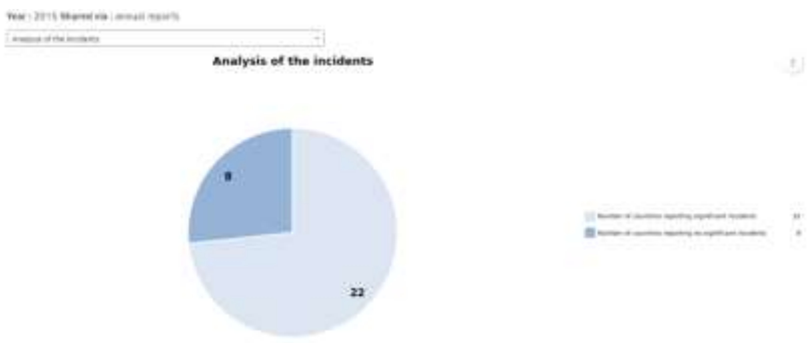
- Incident cards listing - similar to the country Incidents tab.
- XLS Export, available on the *Results* tab - will provide the user with a downloadable tabular representation of the incident reports.
- Data visualization - this will display predefined charts and datasets based on the current result set.

6.1 Data visualisation

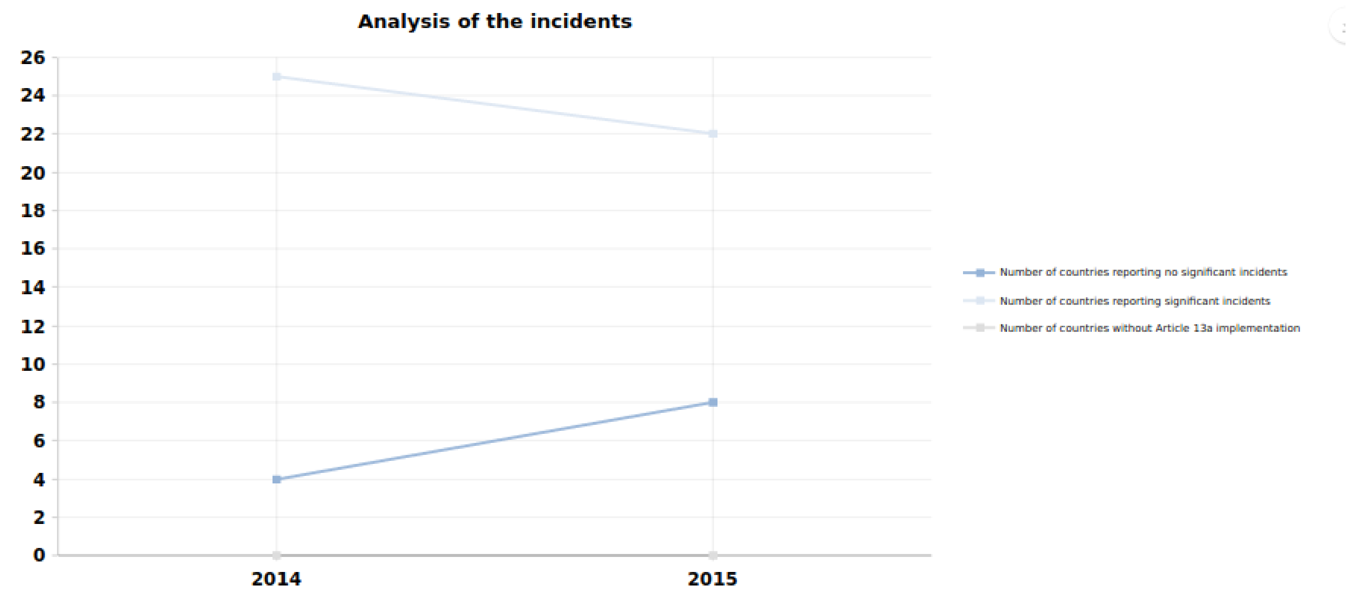
Displays predefined charts and datasets based on the current result set.

Depending on the amount of information available in the results, some charts may be unavailable or display no information.

Selecting “*Annual reports*” and one year (e.g. “*2015*”) in the filters will generate the charts corresponding to that year’s annual report. Please note that queries involving the “*annual report*” filter will take longer to complete.


Year : 2015 Shared via : annual reports
Analysis of the incidents
Analysis of the incidents
8
22
Number of countries reporting significant incidents 22
Number of countries reporting no significant incidents 8

Selecting “Annual reports” and two or more years (e.g. “2015” and “2014”) will display charts using trend lines.



Selecting both “*all countries*” and “*my country only*” will display two sets of charts, one using the data for the current user’s assigned country and one for all countries (including the current user’s).

Charts as well as the dataset used can be exported in various formats by using the download icon on the top right of the chart.

7 Technical Procedure of Article 13a Annual Incidents Reporting

Annual summary reporting is mandated by paragraph 3 of Article 13a of the Framework Directive of the EU’s Regulatory Framework for Electronic communications. This document describes the procedure for annual summary reporting. Annual summary reporting is described in more detail in the latest version of the Technical guideline on Incident reporting which was produced by the Article 13a Expert Group.

7.1 Reporting interval

Annual summary reporting should include incident reports for incidents which were *resolved* between January 1st and December 31st the previous year).

7.2 Reporting thresholds

Reporting thresholds are based on the thresholds described in the latest version of the Technical guideline on Incident reporting, Chapter 6.

7.3 Reporting modality

7.3.1 Deadline

NRAs should send annual summary reports over the previous year to the European Commission and ENISA before the end of February.

7.3.2 ENISA online reporting tool

NRAs should use the ENISA online reporting tool for submitting the report. Access to the online reporting tool can be obtained by contacting ENISA (article13@enisa.europa.eu).

When using the tool, the obligation to report also to the European Commission is fulfilled. It is not needed to report separately to the European Commission, as the online reporting tool instantly sends the full report also to the European Commission’s mailbox for incident reports.

7.3.3 Alternative reporting option

As an alternative option, instead of using the online reporting tool, NRAs may send reports using email. In this case, NRAs should use the reporting thresholds and the reporting fields described in the latest version of the Technical guideline on Incident reporting, Chapter 6 and 7, and send the email to both mailboxes:

- cnect-nis-article13a@ec.europa.eu and
- article13@enisa.europa.eu