Commission de Surveillance du Secteur Financier

CSSF 24/847 Major ICT-related incident notification, DORA Major ICT-related incident and significant cyber threats reporting - User Guide

CSSF 24/847 Major ICT-related incident notification, DORA Major ICT-related incident and significant cyber threats reporting - User Guide

TABLE OF CONTENTS

1. Introduction

Circular CSSF 24/847 and the application of DORA require entities subject to the supervision of the CSSF to notify the CSSF of major ICT-related incidents, while also allowing for the notification of significant cyber threats. These notifications are required to be submitted through the respective eDesk procedures, called :

- "**CSSF 24/847 Major ICT-related incident notification**" procedure,
- **"DORA Major ICT-related incident and significant cyber threat notification"** procedure,

or via an API (S3 protocol), both established by the CSSF.

The eDesk portal allows Supervised Entities for **CSSF 24/847 incident reports** and **DORA - Major Incident Reports** to:

a) fill in and submit major ICT-related incident notifications with attachments in three phases: Initial notification ("Initial information"); Intermediate report ("Incident cause, classification and impact"); and Final report ("Root cause, follow up and additional information").
b) exchange comments with the CSSF regarding each notified major ICT-related incident.
c) submit updates of notifications when applicable.

The eDesk portal allows Supervised Entities for **DORA - Significant Cyber Threat Reports** to :

a) fill in and submit major ICT-related incident notifications with attachments.
b) exchange comments with the CSSF regarding each notified major ICT-related incident.
c) submit updates of notifications when applicable.

The S3 protocol allows Supervised Entities to perform a) and c) above.

Definitions, criteria, notification deadlines and other details regarding the reporting obligations are available in Circular CSSF 24/847.

The purpose of this document is to guide the user(s) for:

1. the completion and submission of the *above-mentioned procedures* accessible on the eDesk portal;
2. the completion and submission of the *above-mentioned procedures* via the S3 protocol.

Should Supervised Entities experience difficulties in creating an account or in case of technical difficulties to submit a notification, please contact the CSSF via email at: edesk@cssf.lu

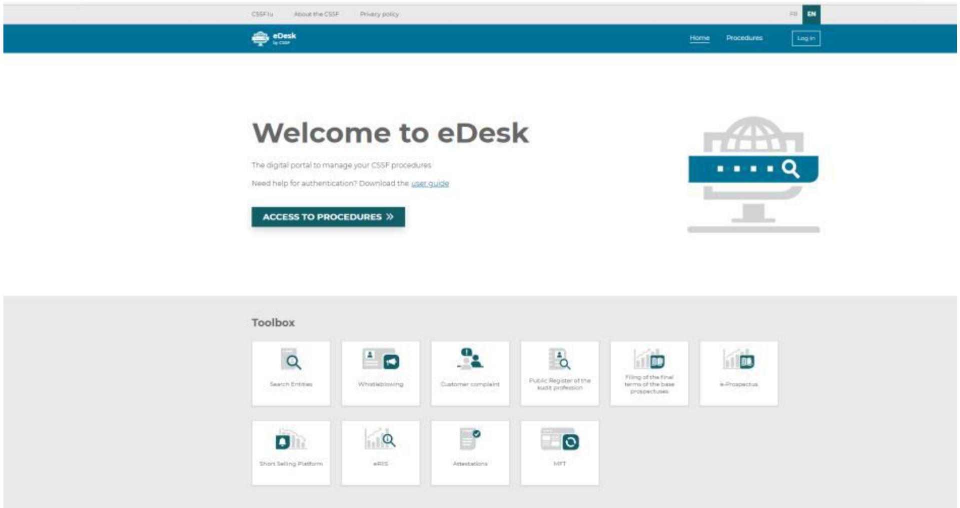
Should Supervised Entities have any questions in relation to the timeline or the content of the notifications to be submitted, please contact the CSSF via email at: ictrisksupervision@cssf.lu

2. Connection to the eDesk portal

2.1. Authentication and connection to the eDesk portal

Important: The **prerequisites** enabling the connection to eDesk and the initiation of a notification (activation of an entity link, …) are detailed in the eDesk Authentication User Guide in the eDesk portal home page (https://edesk.apps.cssf.lu/edesk-dashboard/dashboard/getstarted). Please refer to the eDesk Authentication User Guide.

2.2. Access to the 2 notification procedures

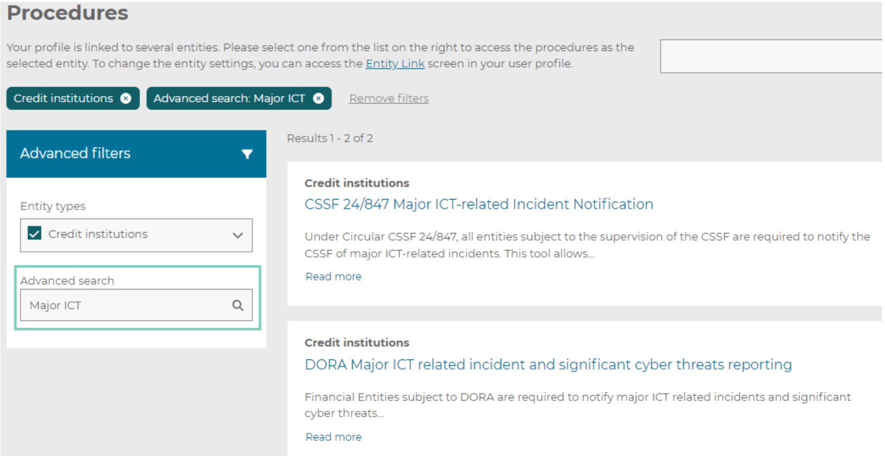


Welcome to eDesk

The digital portal to manage your CSSF procedures

Need help for authentication? Download the user guide

From the eDesk homepage, to find the 2 notification procedures, click on the **"Access to procedures"** button and then type **"Major ICT"** in the **"Advanced search"** bar. The user can select the corresponding procedure by clicking the corresponding link.



Procedures

Your profile is linked to several entities. Please select one from the list on the right to access the procedures as the selected entity. To change the entity settings, you can access the Entity Link screen in your user profile.

Results 1 - 2 of 2

Entity types

☑ Credit institutions

Advanced search

Major ICT

Credit institutions

CSSF 24/847 Major ICT-related Incident Notification

Under Circular CSSF 24/847, all entities subject to the supervision of the CSSF are required to notify the CSSF of major ICT-related incidents. This tool allows...

Read more

Credit institutions

DORA Major ICT related incident and significant cyber threats reporting

Financial Entities subject to DORA are required to notify major ICT related incidents and significant cyber threats...

Read more

Important: The "IT Incident Notifier" role is required to access and manage the filing of Major ICT-related Incident Notifications. The roles existing in eDesk and allowing access to this eDesk module are detailed in the eDesk Authentication User Guide in the eDesk portal home page (https://edesk.apps.cssf.lu/edesk-dashboard/dashboard/getstarted). Please request the role from the advanced user of your entity.

For information, the eDesk homepage screen is split as follows:

- The Header is the upper part of the screen where the user can find:
  - The **navigation menu** that shows several useful links. "CSSF.lu" takes the user back to the CSSF website. "About the CSSF" and "Privacy policy" take the user to the dedicated CSSF website sections respectively about CSSF itself and its privacy policy.
  - The **language option** (FR or EN) is available on each screen, and it is possible to switch between languages throughout the authentication procedure.
  - The "**Log in**" button takes the user to the screen to be used to connect to the eDesk portal.
  - The "**Procedures**" button takes the user to the "Log in" page if the user is not connected yet or the procedures list.

•The **Toolbox** gathers several e-services (modules) that do not require an authentication.

• The **News** section presents the latest information related to eDesk.

• The **Footer** at the bottom of the screen is non-interactive.

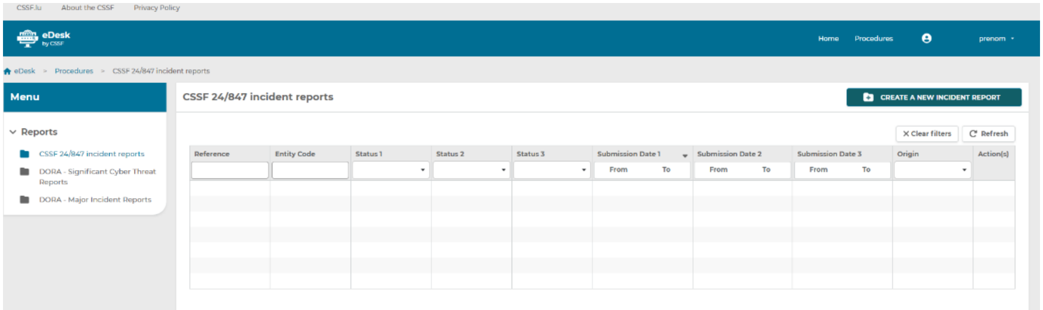
2.3. CSSF 24/847 incident reports form

The following actions are possible:

- Creation of a new notification
- Modification of a submitted notification
- Reclassification of an incident
- Addition of document(s) to the notification form
- Exchange of comment(s) with the CSSF

2.3.1. Dashboard of CSSF 24/847 incident reports notifications

When connecting to the modules, the main part of the page is a dashboard providing a general view of all the notifications created by the Supervised Entity, with usual filtering and sorting functionalities.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
CSSF 24/847 incident reports
CREATE A NEW INCIDENT REPORT
Clear filters
Refresh

Reference	Entity Code	Status 1	Status 2	Status 3	Submission Date 1	Submission Date 2	Submission Date 3	Origin	Action(s)
					From To	From To	From To		

The dashboard for **CSSF 24/847 incident reports** contains the following columns:

- **Reference:** Reference of CSSF 24/847 incident reports notification, automatically assigned once a notification is submitted,
- **Entity code**: CSSF code of the Supervised Entity,

- **Status 1**: Status of the 1st section of the form "Initial information". The value of each status can be either "Draft", "Submitted" or "Closed",
- **Status 2**: Status of the 2nd section of the form "Incident cause, classification and impact",
- **Status 3**: Status of the 3rd section of the form "Root cause, follow up and additional information",
- **Submission Date 1**: Date of submission of the 1st section of the form,
- **Submission Date 2**: Date of submission of the 2nd section of the form,
- **Submission Date 3**: Date of submission of the 3rd section of the form,
- **Origin**: The submission channel through which the incident was submitted to the CSSF. The value will be either "eDesk" or "S3",
- **Action(s):** The Supervised Entity can "open" the notification form by clicking on the "folder" icon. The entity can also double-click on a given line to consult a form.

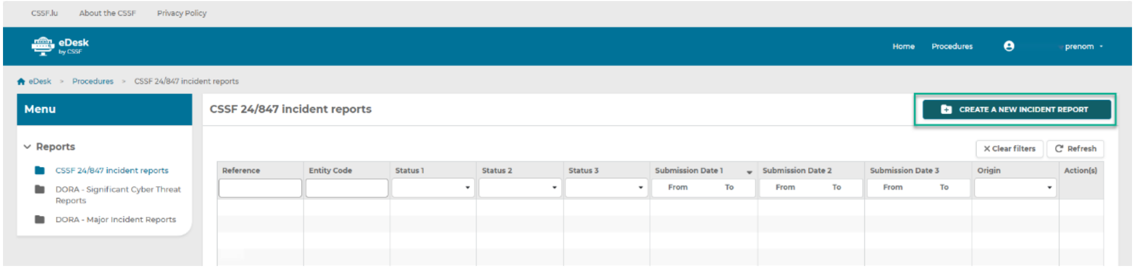
Above the dashboard, a top banner contains several links and useful information:

- a link to the **global eDesk** dashboard (by clicking on the eDesk logo or "**Home**"),
- a link to the procedures accessible by the connected Supervised Entity user (by clicking on "**Procedures**"),
- the **name** of the user connected and corresponding Supervised Entity name *(not visible in the above illustration)*, with a small arrow on the right which can be used to access:
  - the "User profile" by clicking "Manage profile",
  - the "Entity management" (available only for the advanced users), and
  - the Logout functionality.

Below the top banner is a button labelled "**CREATE A NEW INCIDENT REPORT**", which allows the Supervised Entity to create a new incident notification. Further details are provided in the next section.

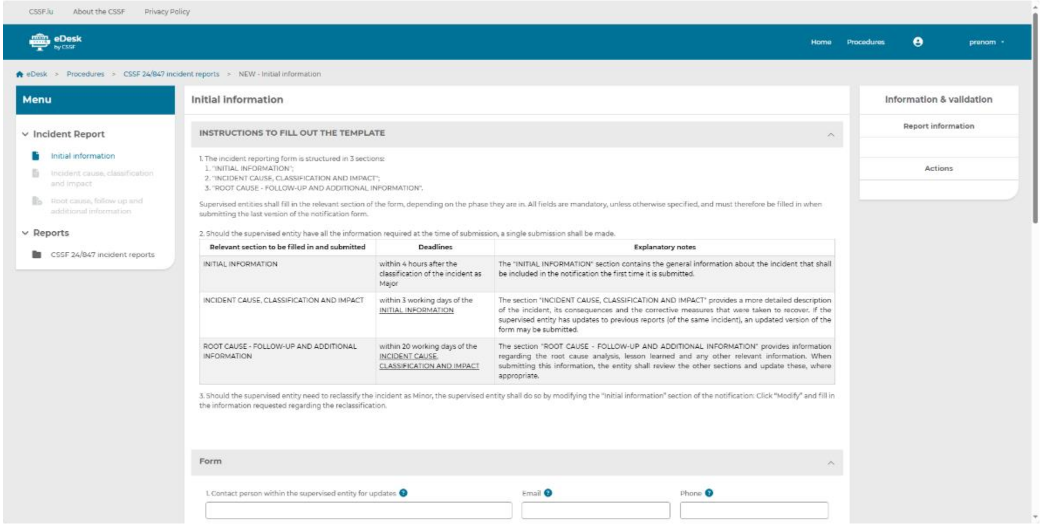
2.3.2. Creation of a new notification

To create a new major ICT-related incident notification, the user shall click on the "**CREATE A NEW INCIDENT REPORT**" button on the dashboard page.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
CSSF 24/847 incident reports
CREATE A NEW INCIDENT REPORT
Clear filters
Refresh

Reference	Entity Code	Status 1	Status 2	Status 3	Submission Date 1	Submission Date 2	Submission Date 3	Origin	Action(s)
					From To	From To	From To		

Once the button is clicked, a new incident notification page opens.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports > NEW - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Initial information
Information & validation
Report information
Actions

INSTRUCTIONS TO FILL OUT THE TEMPLATE

1. The incident reporting form is structured in 3 sections:
   1. "INITIAL INFORMATION";
   2. "INCIDENT CAUSE, CLASSIFICATION AND IMPACT";
   3. "ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION".

Supervised entities shall fill in the relevant section of the form, depending on the phase they are in. All fields are mandatory, unless otherwise specified, and must therefore be filled in when submitting the last version of the notification form.

2. Should the supervised entity have all the information required at the time of submission, a single submission shall be made.

Relevant section to be filled in and submitted	Deadlines	Explanatory notes
INITIAL INFORMATION	within 4 hours after the classification of the incident as Major	The "INITIAL INFORMATION" section contains the general information about the incident that shall be included in the notification the first time it is submitted.
INCIDENT CAUSE, CLASSIFICATION AND IMPACT	within 3 working days of the INITIAL INFORMATION	The section "INCIDENT CAUSE, CLASSIFICATION AND IMPACT" provides a more detailed description of the incident, its consequences and the corrective measures that were taken to recover. If the supervised entity has updates to previous reports (of the same incident), an updated version of the form may be submitted.
ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION	within 20 working days of the INCIDENT CAUSE, CLASSIFICATION AND IMPACT	The section "ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION" provides information regarding the root cause analysis, lesson learned and any other relevant information. When submitting this information, the entity shall review the other sections and update these, where appropriate.

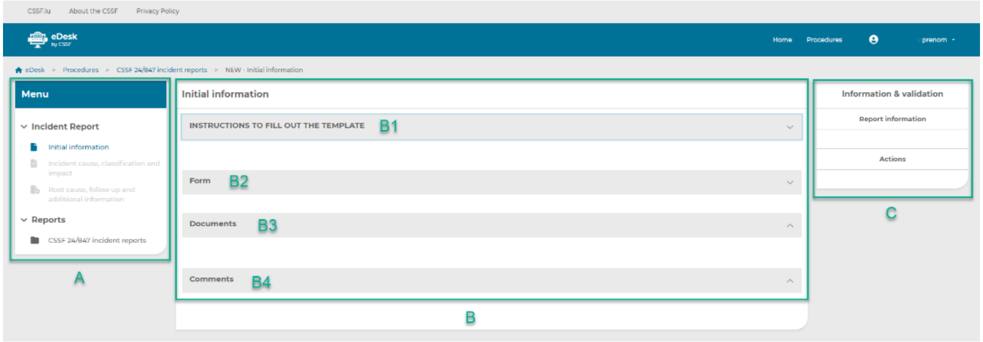
3. Should the supervised entity need to reclassify the incident as Minor, the supervised entity shall do so by modifying the "Initial information" section of the notification: Click "Modify" and fill in the information requested regarding the reclassification.

Form

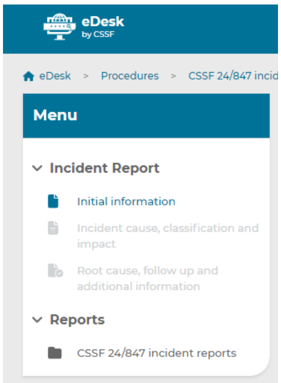
1. Contact person within the supervised entity for updates
Email
Phone

To ease the navigation within the form, sub-sections can be reduced by clicking on the greyed out sub-section's title.

2.3.2.1. Description of the notification form structure


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports > NEW - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
A
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE
B1
Form
B2
Documents
B3
Comments
B4
B
Information & validation
Report information
Actions
C

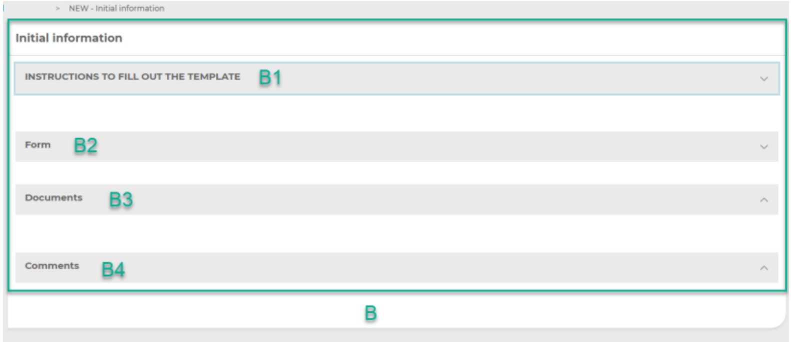
2.3.2.1.1. Navigation Menu (A)


eDesk by CSSF
eDesk > Procedures > CSSF 24/847 incid
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports

The left part of the screen is dedicated to:

- the navigation within the 3 sections of the CSSF 24/847 incident reports notification form, that is:
  - "Initial information",
  - "Incident cause, classification and impact",
  - "Root cause, follow up and additional information"
- "CSSF 24/847 incident reports: this allows the Supervised Entity to return to the main dashboard and access the ongoing or completed notifications.

2.3.2.1.2. The information to be filled in by the Supervised Entity (B)



> NEW - Initial information
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE
B1
Form
B2
Documents
B3
Comments
B4
B

The main part of the notification page devoted to form information, identified in the figure above as "B", is the part of the screen where the metadata relating to the incident notification is displayed. This part is made up of the following sub-sections:

- **B1**: "**INSTRUCTIONS TO FILL OUT THE TEMPLATE**"
- **B2**: "**Form**",
- **B3**: "**Documents**", and
- **B4**: "**Comments**"

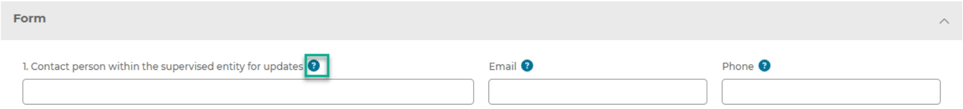
1. INSTRUCTIONS TO FILL OUT THE TEMPLATE (B1)

"**INSTRUCTIONS TO FILL OUT THE TEMPLATE**" is **only** available in the first section, "Initial information", of the incident notification form. It provides, amongst others, general information regarding the structure of the notification, the reporting deadlines to be met by the supervised entities and the possibilities for reclassification of the incident.

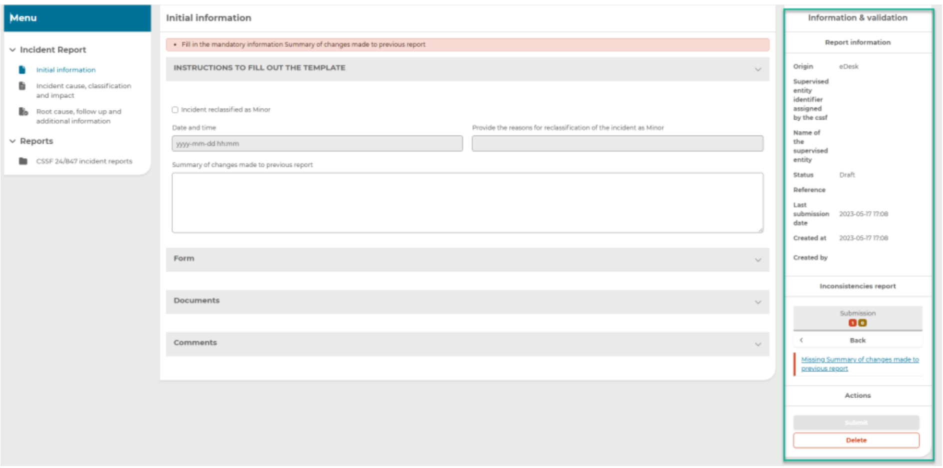
2. Form (B2)

The "**Form**" part contains the questions related to the incident, to be answered by the Supervised Entity. This part exists in the 3 sections of the notification form.

Explanatory notes are available by hovering over the "question mark" symbol to provide further explanations regarding the information to be provided by the Supervised Entity.



2.3.2.1.3. Information and validation (C)



- Fill in the mandatory information Summary of changes made to previous report

□ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor:

Summary of changes made to previous report:

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Reference	
Last submission date	2023-05-17 17:08
Created at	2023-05-17 17:08
Created by	

Missing Summary of changes made to previous report

The “**Information & validation**” section of the screen covers the following:

- “**Report information**”: Provides general information of the Supervised Entity such as the Supervised Entity’s name, and code, the status of the notification, the creation date and the user who created the notification.

- “**Inconsistencies report**”: Displays the potential missing information and inconsistencies to be resolved by the Supervised Entity before submitting the notification to the CSSF.

- “**Actions**”: These are action buttons that represent actions that can be taken by the user at any given point in time. Actions could be for example Submit, Delete or Modify. When actions are “greyed”, the action button cannot be clicked. This may be because the report is incomplete, or the incident has already been closed on the CSSF side.

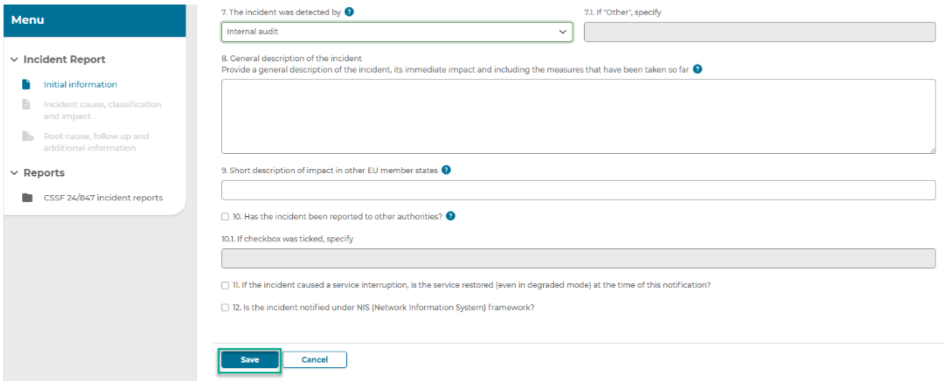
2.3.2.2. Filling in the first draft of a notification

Once a new incident notification form is created, the user can fill in the information requested. The user can complete and submit the relevant sections of the notification form.

Each section of a notification form can be accessed by clicking on the corresponding name of the section in the navigation Menu.

- **Initial information**: This section gathers the general information about the incident.
- **Incident cause, classification and impact**: This second section provides a more detailed description of the incident, its consequences and the corrective measures that were taken to recover.
- **Root cause, follow up and additional information**: This third section provides information regarding the root cause analysis, lesson learned and any other relevant information. When submitting this information, the Supervised Entity shall review the other sections and update these, where appropriate.

The user shall always save the information filled-in by clicking on the "**Save**" button at the bottom of the section prior to submitting any section of an incident notification.


Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports

7. The incident was detected by: Internal audit

7.1. If "Other", specify

8. General description of the incident
Provide a general description of the incident, its immediate impact and including the measures that have been taken so far

9. Short description of impact in other EU member states

□ 10. Has the incident been reported to other authorities?

10.1. If checkbox was ticked, specify

□ 11. If the incident caused a service interruption, is the service restored (even in degraded mode) at the time of this notification?

□ 12. Is the incident notified under NIS (Network Information System) framework?

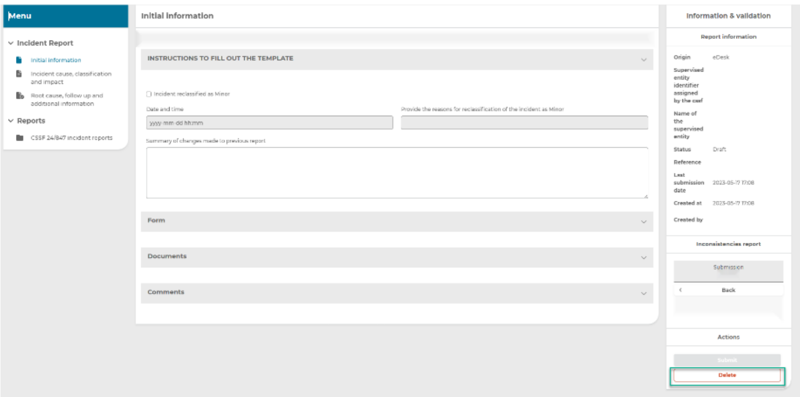
Any saved section will have the status "Draft" and will **not yet be visible by the CSSF**.

The draft data already saved can be deleted any time before the information is submitted to the CSSF via the dedicated "Delete" action button.

2.3.2.3. Deletion of a draft notification

A notification at status "Draft" can be deleted by the Supervised Entity by clicking on the "**Delete**" action button in the "Information & validation" section.

Any deleted notification cannot be restored and shall be started over.


Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE

□ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor

Summary of changes made to previous report

Form
Documents
Comments
Information & validation
Report information

Origin: eDesk

Supervised entity identifier assigned by the cssf:

Name of the supervised entity:

Status: Draft

Reference:

Last submission date: 2023-05-17 17:08

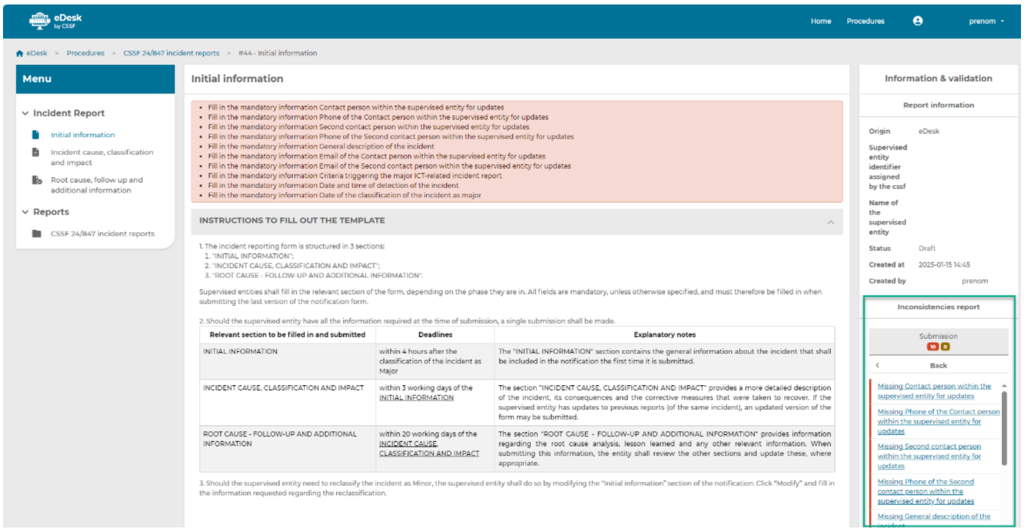
Created at: 2023-05-17 17:08

Created by:

2.3.2.4. Submission of a draft notification

A notification can be submitted by clicking the “**Submit**” action button in the “Information & validation” section.

The system automatically prevents the user from submitting any incomplete notification form to the CSSF. In such case, the system will display a list of the missing data at the top of the form, as well as in the “Inconsistencies report” in the right section.


eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports > #44 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports

Initial information

- Fill in the mandatory information Contact person within the supervised entity for updates
- Fill in the mandatory information Phone of the Contact person within the supervised entity for updates
- Fill in the mandatory information Second contact person within the supervised entity for updates
- Fill in the mandatory information Phone of the Second contact person within the supervised entity for updates
- Fill in the mandatory information General description of the incident
- Fill in the mandatory information Email of the Contact person within the supervised entity for updates
- Fill in the mandatory information Email of the Second contact person within the supervised entity for updates
- Fill in the mandatory information Criteria triggering the major ICT-related incident report
- Fill in the mandatory information Date and time of detection of the incident
- Fill in the mandatory information Date of the classification of the incident as major

INSTRUCTIONS TO FILL OUT THE TEMPLATE

1. The incident reporting form is structured in 3 sections:
   1. "INITIAL INFORMATION";
   2. "INCIDENT CAUSE, CLASSIFICATION AND IMPACT";
   3. "ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION".

Supervised entities shall fill in the relevant section of the form, depending on the phase they are in. All fields are mandatory, unless otherwise specified, and must therefore be filled in when submitting the last version of the notification form.

2. Should the supervised entity have all the information required at the time of submission, a single submission shall be made.

Relevant section to be filled in and submitted	Deadlines	Explanatory notes
INITIAL INFORMATION	within 4 hours after the classification of the incident as Major	The "INITIAL INFORMATION" section contains the general information about the incident that shall be included in the notification the first time it is submitted.
INCIDENT CAUSE, CLASSIFICATION AND IMPACT	within 3 working days of the INITIAL INFORMATION	The section "INCIDENT CAUSE, CLASSIFICATION AND IMPACT" provides a more detailed description of the incident, its consequences and the corrective measures that were taken to recover. If the supervised entity has updates to previous reports (of the same incident), an updated version of the form may be submitted.
ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION	within 20 working days of the INCIDENT CAUSE, CLASSIFICATION AND IMPACT	The section "ROOT CAUSE - FOLLOW-UP AND ADDITIONAL INFORMATION" provides information regarding the root cause analysis, lesson learned and any other relevant information. When submitting this information, the entity shall review the other sections and update these, where appropriate.

3. Should the supervised entity need to reclassify the incident as Minor, the supervised entity shall do so by modifying the "Initial information" section of the notification: Click "Modify" and fill in the information requested regarding the reclassification.

Information & validation

Report information

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Created at	2025-01-15 14:45
Created by	prenom

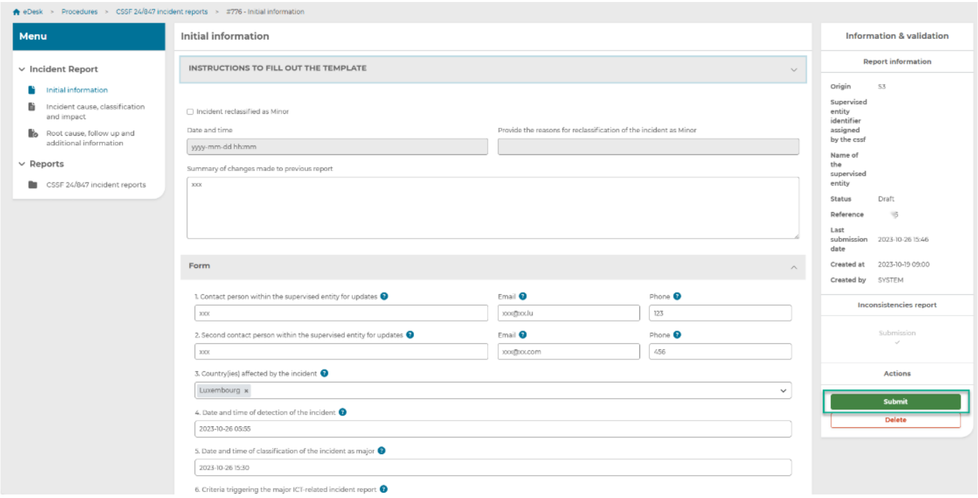
Inconsistencies report

Submission 10 0

Back

- Missing Contact person within the supervised entity for updates
- Missing Phone of the Contact person within the supervised entity for updates
- Missing Second contact person within the supervised entity for updates
- Missing Phone of the Second contact person within the supervised entity for updates
- Missing General description of the incident

Once the form is filled-in with the mandatory information and the changes are saved, the “**Submit**” button will be enabled.


eDesk > Procedures > CSSF 24/847 incident reports > #776 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Submit
Delete

Initial information

INSTRUCTIONS TO FILL OUT THE TEMPLATE

☐ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor:

Summary of changes made to previous report: xxx

Form

1. Contact person within the supervised entity for updates: xxx — Email: xxx@xx.lu — Phone: 123
2. Second contact person within the supervised entity for updates: xxx — Email: xxx@xx.com — Phone: 456
3. Country(ies) affected by the incident: Luxembourg ×
4. Date and time of detection of the incident: 2023-10-26 05:55
5. Date and time of classification of the incident as major: 2023-10-26 15:30
6. Criteria triggering the major ICT-related incident report

Information & validation

Report information

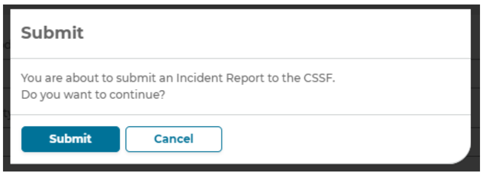
Origin	53
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Reference	[redacted]
Last submission date	2023-10-26 15:46
Created at	2023-10-19 09:00
Created by	SYSTEM

Inconsistencies report

Submission ✓

Actions

When clicking on the “Submit” button, a confirmation window will pop up for the user to confirm the requested action. The user will have to confirm this action for the notification to be submitted to the CSSF.

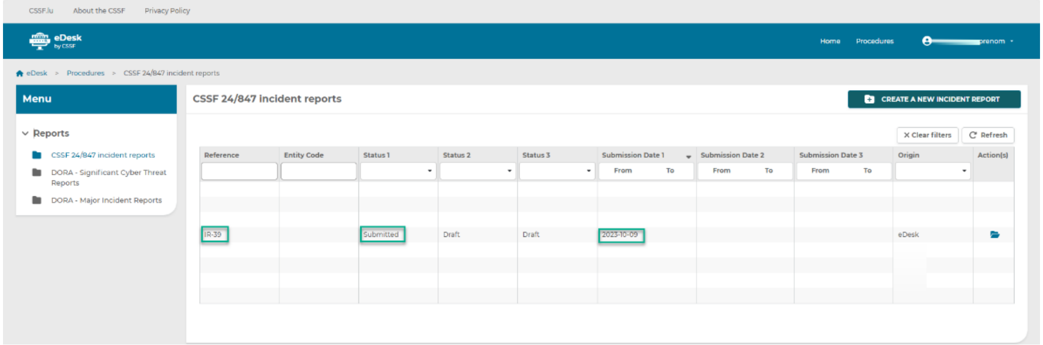


Submit

You are about to submit an Incident Report to the CSSF.
Do you want to continue?

Once confirmed, the status of this submitted section of the notification will change to "Submitted" and its respective submission date will be automatically displayed in the "Report information" section, as well as in the dashboard.

A dedicated reference will also be automatically assigned to this submitted notification. Unlike the status, the filing reference is unique for the 3 sections of an incident notification.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
[redacted] prenom
eDesk > Procedures > CSSF 24/847 incident reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
CSSF 24/847 incident reports
CREATE A NEW INCIDENT REPORT
Clear filters
Refresh

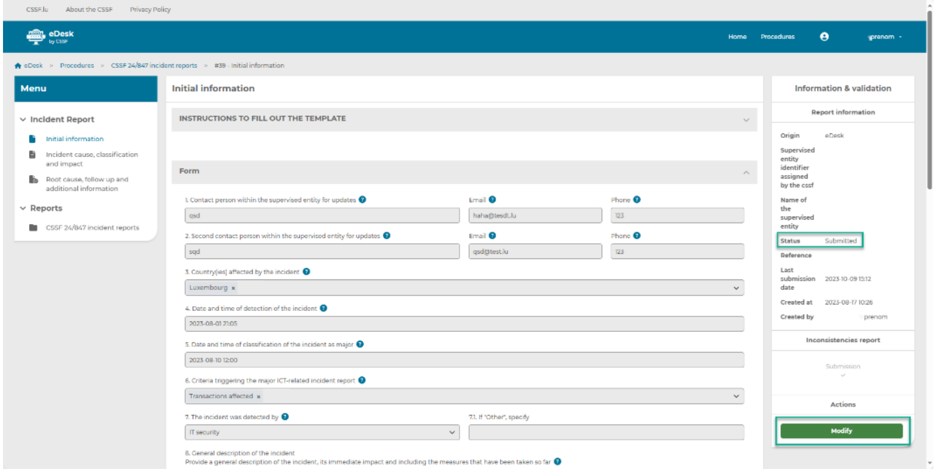
Reference	Entity Code	Status 1	Status 2	Status 3	Submission Date 1	Submission Date 2	Submission Date 3	Origin	Action(s)
					From To	From To	From To		
IR-39		Submitted	Draft	Draft	2023-10-09			eDesk	

Important: The section "Initial information" of a notification shall be submitted first, followed by the section "Incident cause, classification and impact", and lastly the section "Root cause, follow up and additional information".

2.3.3. Modification of a submitted notification

If the Supervised Entity has updates to an incident report already submitted, an updated version of the form may be submitted.

In this case, the user shall click on the action "Modify", that is only available at status "Submitted".


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports > #39 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE
Form
Information & validation
Report information
Inconsistencies report
Submission
Actions
Modify

1. Contact person within the supervised entity for updates: qsd — Email: haha@tesdt.lu — Phone: 123

2. Second contact person within the supervised entity for updates: sqd — Email: qsd@test.lu — Phone: 123

3. Country(ies) affected by the incident: Luxembourg

4. Date and time of detection of the incident: 2023-08-01 21:05

5. Date and time of classification of the incident as major: 2023-08-10 12:00

6. Criteria triggering the major ICT-related incident report: Transactions affected

7. The incident was detected by: IT security

7.1. If "Other", specify:

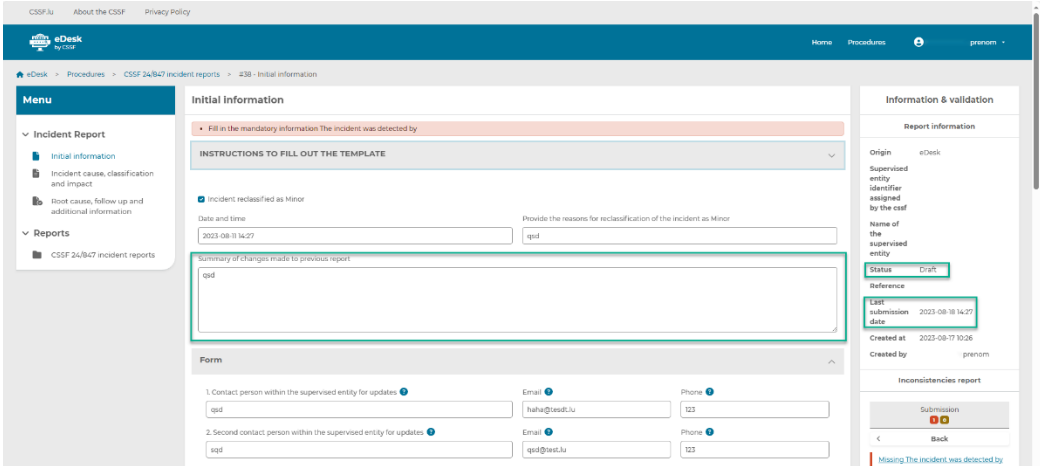
8. General description of the incident
Provide a general description of the incident, its immediate impact and including the measures that have been taken so far

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Submitted
Reference	
Last submission date	2023-10-09 15:12
Created at	2023-08-17 10:26
Created by	prenom

A new information "Last submission date" is then displayed in the "Report information" for the user to easily differentiate a new form from an update of an already submitted one.

For any modification of an already submitted form, the user must complete the section "Summary of changes made to previous report".

A modified form reverts to the status "Draft" and must be saved and submitted again via the "**Submit**" action, for the CSSF to receive the updated information.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > CSSF 24/847 incident reports > #38 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Form
Submission
1 0
Back

Initial information

- Fill in the mandatory information The incident was detected by

INSTRUCTIONS TO FILL OUT THE TEMPLATE

☑ Incident reclassified as Minor

Date and time: 2023-08-11 14:27

Provide the reasons for reclassification of the incident as Minor: qsd

Summary of changes made to previous report: qsd

1. Contact person within the supervised entity for updates: qsd — Email: haha@tesdt.lu — Phone: 123

2. Second contact person within the supervised entity for updates: sqd — Email: qsd@test.lu — Phone: 123

Information & validation

Report information

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Reference	
Last submission date	2023-08-18 14:27
Created at	2023-08-17 10:26
Created by	prenom

Inconsistencies report

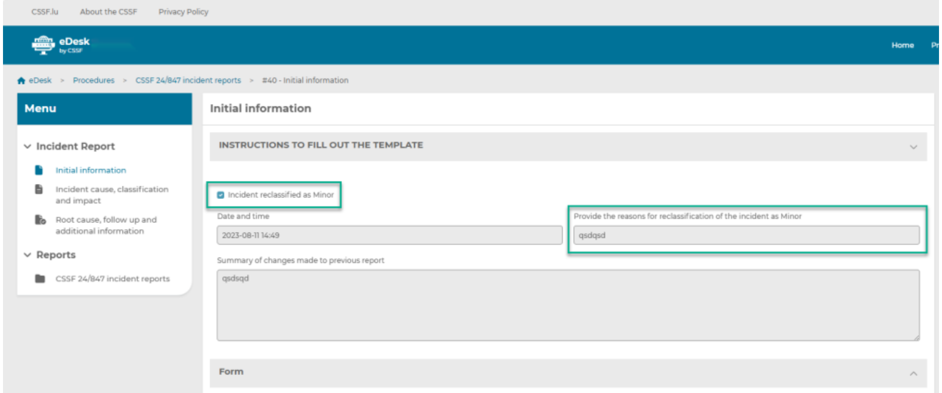
Missing The incident was detected by

Any new ongoing version of a form can be deleted via the "Delete" action, which, if confirmed via the usual popup window, brings the user back to its previous submitted version.

Important: An incident notification with the status "Closed" can no longer be modified. New document(s) or comment(s) can however still be added and submitted.

2.3.4. Reclassification of an incident

In case the incident no longer fulfils the criteria to be considered as major, the user can reclassify the incident notification in the system. The incident shall then be reclassified as minor by ticking the dedicated box at the top of the "Initial information" section of the notification form. Supervised entities must provide the date and an explanation of the reasons for this reclassification. This option is only available after the initial submission of the notification form.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
eDesk > Procedures > CSSF 24/847 incident reports > #40 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Form

Initial information

INSTRUCTIONS TO FILL OUT THE TEMPLATE

☑ Incident reclassified as Minor

Date and time: 2023-08-11 14:49

Provide the reasons for reclassification of the incident as Minor: qsdqsd

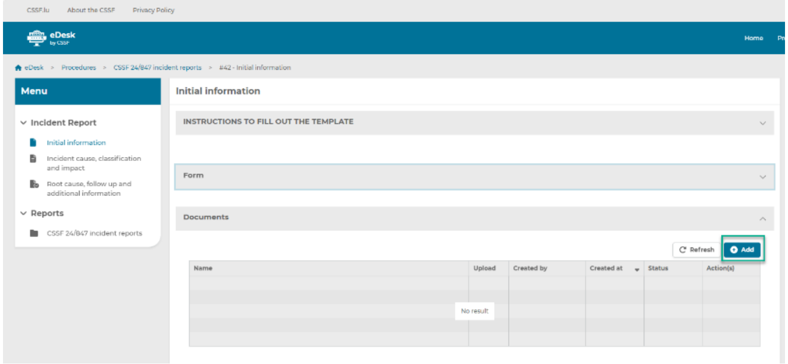
Summary of changes made to previous report: qsdsqd

2.3.5. Addition of document(s) to the notification form

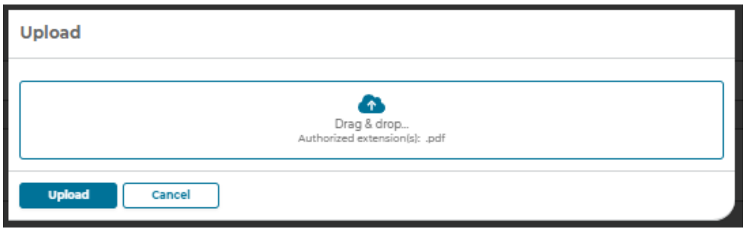
The “**Documents**” part allows the user to attach document(s) to its notification where applicable.

To add a document, follow the steps below:

1. Click on the “Add” button.

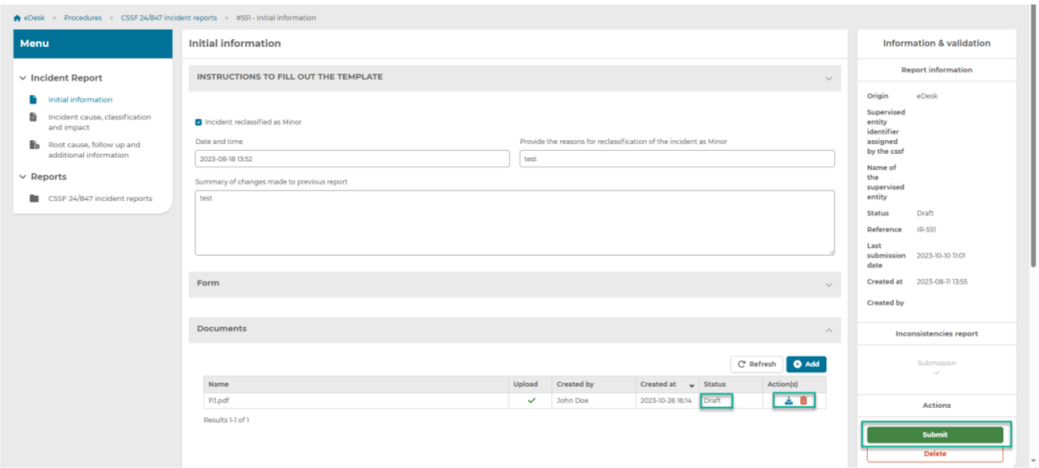

CSSF.lu
About the CSSF
Privacy Policy
eDesk
Home
eDesk > Procedures > CSSF 24/847 incident reports > #42 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE
Form
Documents
Refresh
Add
Name
Upload
Created by
Created at
Status
Action(s)
No result

2. A new window will open allowing the user to upload a new document. **Note**: only pdf extension is authorized.



The document is then uploaded and attached to the dedicated section with status “Draft” and can be downloaded or deleted by the user.

Document(s) attached to a specific section of an incident notification are submitted to the CSSF together with the corresponding section of the “Form”, via the action “**Submit**”. Document(s) added to closed files shall be submitted individually.


eDesk > Procedures > CSSF 24/847 incident reports > #551 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Initial information
INSTRUCTIONS TO FILL OUT THE TEMPLATE
Form
Documents
Refresh
Add
Results 1-1 of 1
Information & validation
Report information
Inconsistencies report
Submission
Actions
Submit
Delete

☑ Incident reclassified as Minor

Date and time: 2023-08-18 13:52

Provide the reasons for reclassification of the incident as Minor: test

Summary of changes made to previous report: test

Name	Upload	Created by	Created at	Status	Action(s)
PJ.pdf	✓	John Doe	2023-10-26 16:14	Draft	

Origin: eDesk

Supervised entity identifier assigned by the cssf:

Name of the supervised entity:

Status: Draft

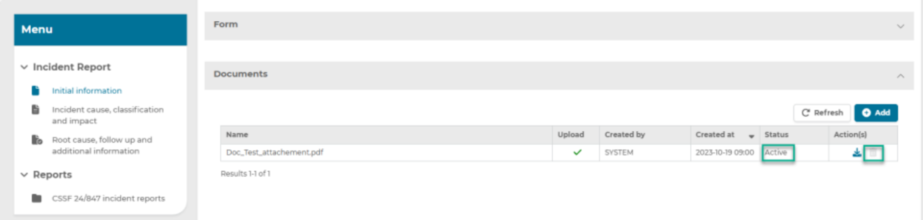
Reference: IR-551

Last submission date: 2023-10-10 11:01

Created at: 2023-08-11 13:55

Created by:

The deletion action remains available until the section is submitted to the CSSF, changing the status of the document to “Active”.


Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
Form
Documents
Refresh
Add

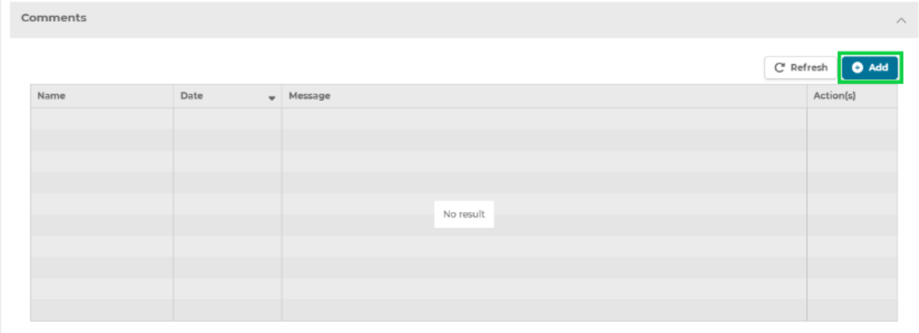
Name	Upload	Created by	Created at	Status	Action(s)
Doc_Test_attachement.pdf	✓	SYSTEM	2023-10-19 09:00	Active	

Results 1-1 of 1

2.3.6. Exchange of comment(s) with the CSSF

The “**Comments**” part allows the CSSF and supervised entities to exchange comments about the information submitted in the form.

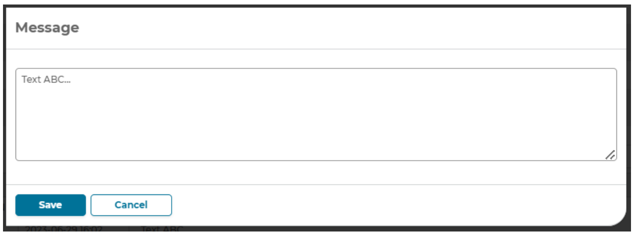
New comments can be created by clicking on “**Add**”.



Name	Date	Message	Action(s)

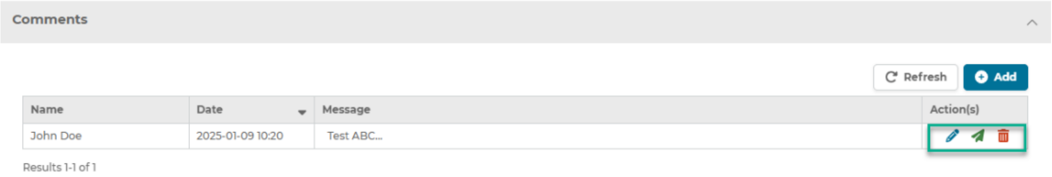
No result

A new window will be displayed, allowing the user to write a text. The user shall then click on the “**Save**” button to save the entered text.



Text ABC...

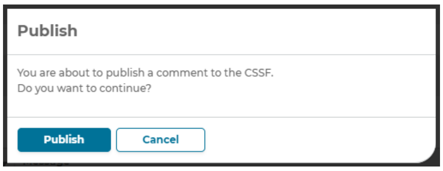
The comment will then be displayed in the dedicated “Comments” section and can be respectively “**Edited**”, “**Published to the CSSF**”, or “**Deleted**” via the action buttons.



Name	Date	Message	Action(s)
John Doe	2025-01-09 10:20	Test ABC...	

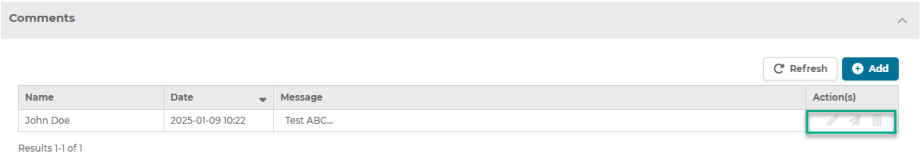
Results 1-1 of 1

Important: The "**Save**" button will only save a draft version of a comment but will **not** send the comment to the CSSF. To send a comment to the CSSF, the user shall click on the "**Publish**" icon and confirm the action in the popup window. Once the comment is published to the CSSF it can no longer be edited or deleted.



Publish

You are about to publish a comment to the CSSF.
Do you want to continue?

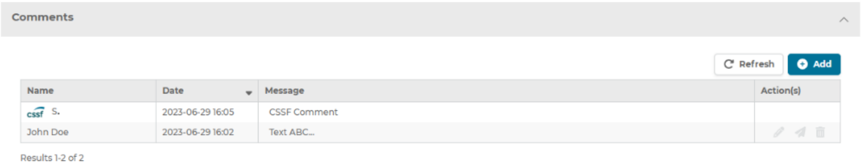


Comments

Name	Date	Message	Action(s)
John Doe	2025-01-09 10:22	Test ABC...	

Results 1-1 of 1

The comments published by the CSSF to the Supervised Entity will be visible in the same section. Those comments have the CSSF logo before the name of the CSSF agent who published it.



Comments

Name	Date	Message	Action(s)
cssf S.	2023-06-29 16:05	CSSF Comment	
John Doe	2023-06-29 16:02	Text ABC...	

Results 1-2 of 2

Comments can be added and published any time after the initial submission of the "Initial information" section.

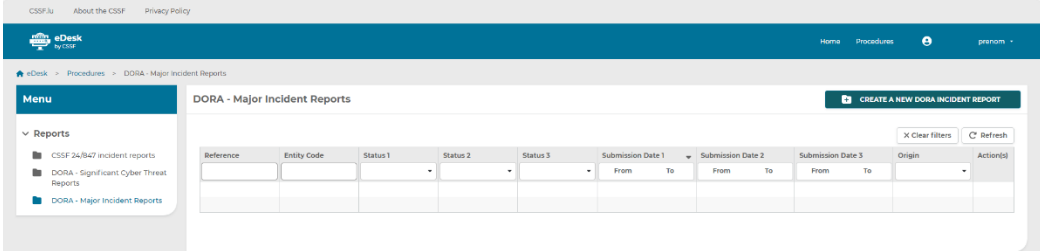
2.4. DORA - Major ICT-related incident notification form

The following actions are possible:

- Creation of a new notification
- Modification of a submitted notification
- Reclassification of an incident
- Addition of document(s) to the notification form
- Exchange of comment(s) with the CSSF

2.4.1. Dashboard of DORA - Major ICT-related incident notifications

When connecting to the modules, the main part of the page is a dashboard providing a general view of all the notifications created by the Supervised Entity, with usual filtering and sorting functionalities.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > DORA - Major Incident Reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
DORA - Major Incident Reports
CREATE A NEW DORA INCIDENT REPORT
Clear filters
Refresh

Reference	Entity Code	Status 1	Status 2	Status 3	Submission Date 1	Submission Date 2	Submission Date 3	Origin	Action(s)
					From To	From To	From To		

The dashboard for **DORA - Major Incident Reports** contains the following columns:

- **Reference:** Reference of the DORA - Major ICT-related incident notification, automatically assigned once a notification is submitted,
- **Entity code**: CSSF code of the Supervised Entity,
- **Status 1**: Status of the 1st section of the form "Initial notification". The value of each status can be either "Draft", "Submitted" or "Closed",
- **Status 2**: Status of the 2nd section of the form "Intermediate report",
- **Status 3**: Status of the 3rd section of the form "Final report",
- **Submission Date 1**: Date of submission of the 1st section of the form,
- **Submission Date 2**: Date of submission of the 2nd section of the form,
- **Submission Date 3**: Date of submission of the 3rd section of the form,
- **Origin**: The submission channel through which the incident was submitted to the CSSF. The value will be either "eDesk" or "S3",
- **Action(s):** The Supervised Entity can "open" the notification form by clicking on the "folder" icon. The entity can also double-click on a given line to consult a form.

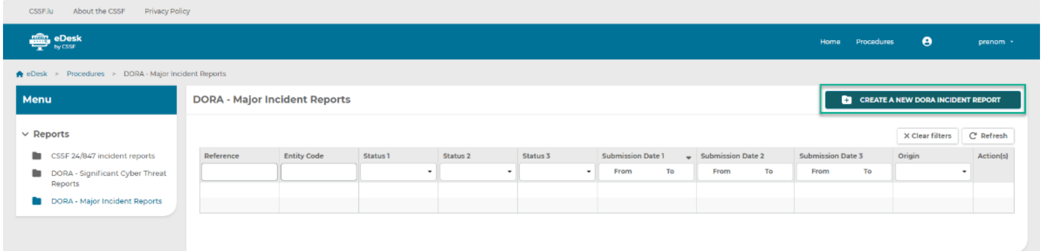
Above the dashboard, a top banner contains several links and useful information:

- a link to the **global eDesk** dashboard (by clicking on the eDesk logo or "**Home**"),
- a link to the procedures accessible by the connected Supervised Entity user (by clicking on "**Procedures**"),
- the **name** of the user connected and corresponding Supervised Entity name *(not visible in the above illustration)*, with a small arrow on the right which can be used to access:
  - the "User profile" by clicking "Manage profile",
  - the "Entity management" (available only for the advanced users), and
  - the Logout functionality.

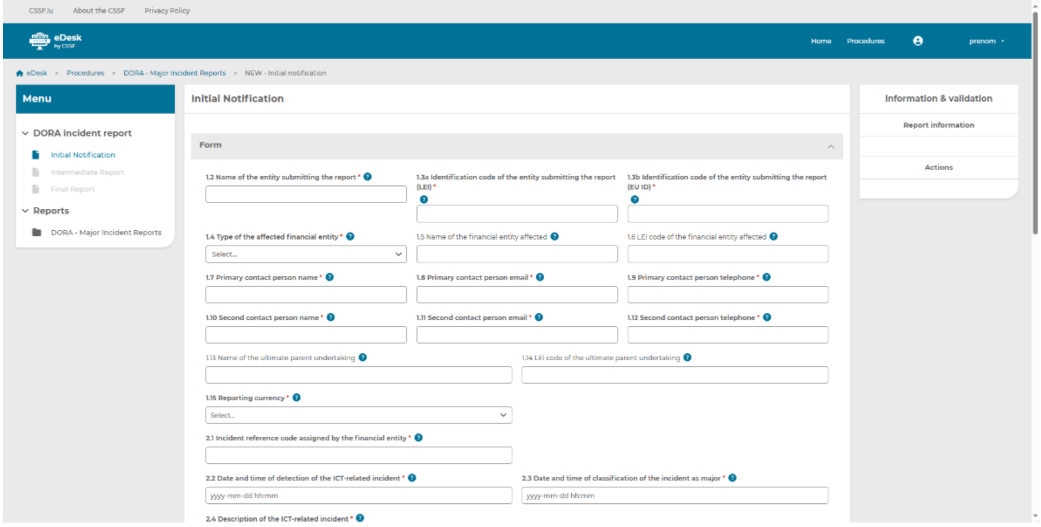
Below the top banner is a button labelled "**CREATE A NEW DORA INCIDENT REPORT**" which allows the Supervised Entity to create a new incident notification. Further details are provided in the next section.

2.4.2. Creation of a new notification

To create a new major ICT-related incident notification, the user shall click on the "**CREATE A NEW DORA INCIDENT REPORT**", button on the dashboard page, depending on the selected form.

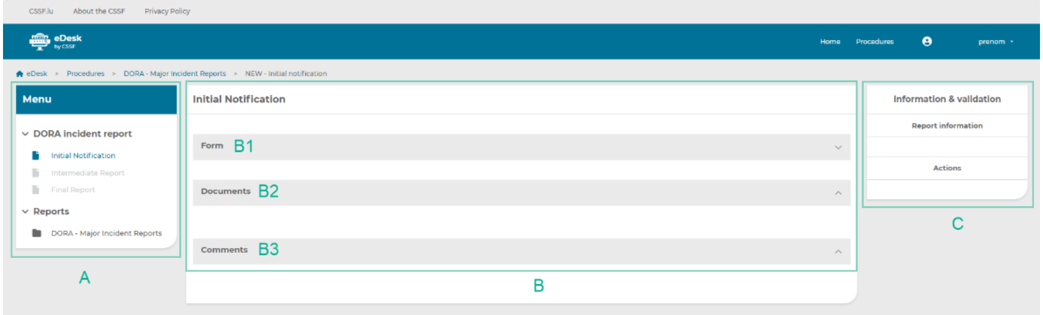


Once the button is clicked, a new incident notification page opens.

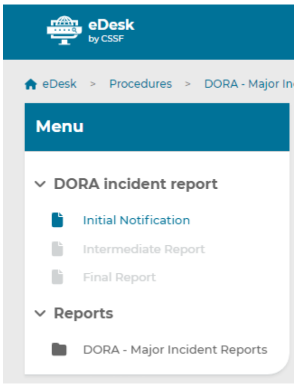

CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > DORA - Major Incident Reports > NEW - Initial notification
Menu
DORA incident report
Initial Notification
Intermediate Report
Final Report
Reports
DORA - Major Incident Reports
Initial Notification
Form
1.2 Name of the entity submitting the report *
1.3a Identification code of the entity submitting the report (LEI) *
1.3b Identification code of the entity submitting the report (EU ID) *
1.4 Type of the affected financial entity *
Select...
1.5 Name of the financial entity affected
1.6 LEI code of the financial entity affected
1.7 Primary contact person name *
1.8 Primary contact person email *
1.9 Primary contact person telephone *
1.10 Second contact person name *
1.11 Second contact person email *
1.12 Second contact person telephone *
1.13 Name of the ultimate parent undertaking
1.14 LEI code of the ultimate parent undertaking
1.15 Reporting currency *
Select...
2.1 Incident reference code assigned by the financial entity *
2.2 Date and time of detection of the ICT-related incident *
yyyy-mm-dd hh:mm
2.3 Date and time of classification of the incident as major *
yyyy-mm-dd hh:mm
2.4 Description of the ICT-related incident *
Information & validation
Report information
Actions

To ease the navigation within the form, sub-sections can be reduced by clicking on the greyed out sub-section's title.

2.4.2.1. Description of the notification form structure



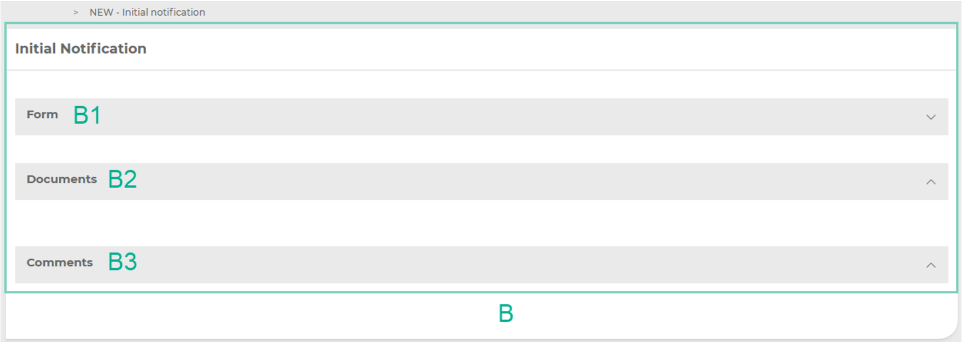
2.4.2.1.1. Navigation Menu (A)



The left part of the screen is dedicated to:

- the navigation within the 3 sections of the DORA - Major Incident Reports notification form, that is:
  - "Initial notification",
  - "Intermediate report",
  - "Final report"
- "CSSF 24/847 incident reports" or "DORA - Major Incident Reports": this allows the Supervised Entity to return to the main dashboard and access the ongoing or completed notifications.

2.4.2.1.2. The information to be filled in by the Supervised Entity (B)

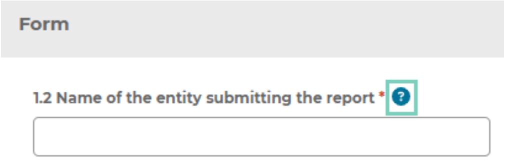


The main part of the notification page devoted to form information, identified in the figure above as "B", is the part of the screen where the metadata relating to the incident notification is displayed. This part is made up of the following sub-sections:

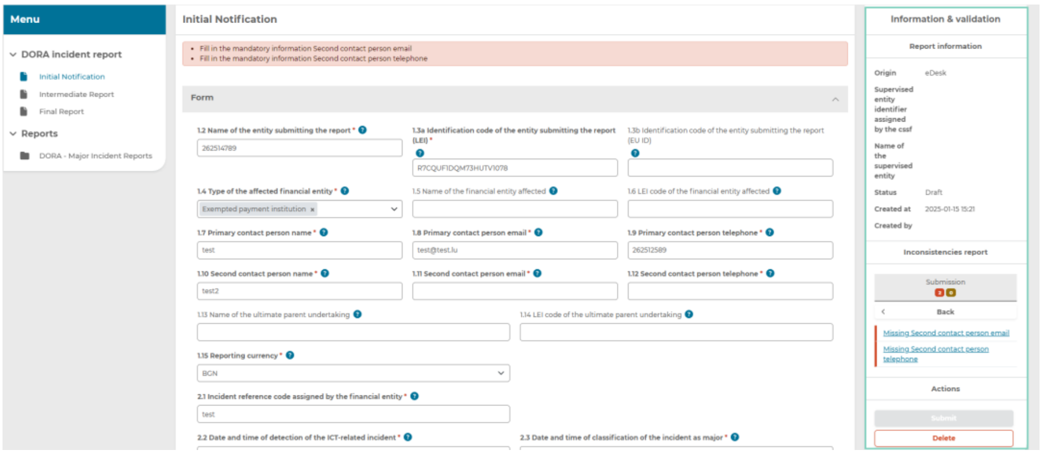
- **B1**: "**Form**",
- **B2**: "**Documents**", and
- **B3**: "**Comments**"

The "**Form**" part contains the questions related to the incident, to be answered by the Supervised Entity. This part exists in the 3 sections of the notification form.

Explanatory notes are available by hovering over the "question mark" symbol to provide further explanations regarding the information to be provided by the Supervised Entity.



2.4.2.1.3. Information and validation (C)



- Fill in the mandatory information Second contact person email
- Fill in the mandatory information Second contact person telephone

1.2 Name of the entity submitting the report *: 262514789

1.3a Identification code of the entity submitting the report (LEI) *: R7CQUFIDQM73HUTV1078

1.3b Identification code of the entity submitting the report (EU ID):

1.4 Type of the affected financial entity *: Exempted payment institution

1.5 Name of the financial entity affected:

1.6 LEI code of the financial entity affected:

1.7 Primary contact person name *: test

1.8 Primary contact person email *: test@test.lu

1.9 Primary contact person telephone *: 262512589

1.10 Second contact person name *: test2

1.11 Second contact person email *:

1.12 Second contact person telephone *:

1.13 Name of the ultimate parent undertaking:

1.14 LEI code of the ultimate parent undertaking:

1.15 Reporting currency *: BGN

2.1 Incident reference code assigned by the financial entity *: test

2.2 Date and time of detection of the ICT-related incident *

2.3 Date and time of classification of the incident as major *

Origin: eDesk

Supervised entity identifier assigned by the cssf:

Name of the supervised entity:

Status: Draft

Created at: 2025-01-15 15:21

Created by:

Missing Second contact person email

Missing Second contact person telephone

The "**Information & validation**" section of the screen covers the following:

- "**Report information**": Provides general information of the Supervised Entity such as the Supervised Entity's name, and code, the status of the notification, the creation date and the user who created the notification.

- "**Inconsistencies report**": Displays the potential missing information and inconsistencies to be resolved by the Supervised Entity before submitting the notification to the CSSF.

- "**Actions**": These are action buttons that represent actions that can be taken by the user at any given point in time. Actions could be for example Submit, Delete or Modify. When actions are "greyed", the action button cannot be clicked. This may be because the report is incomplete, or the incident has already been closed on the CSSF side.

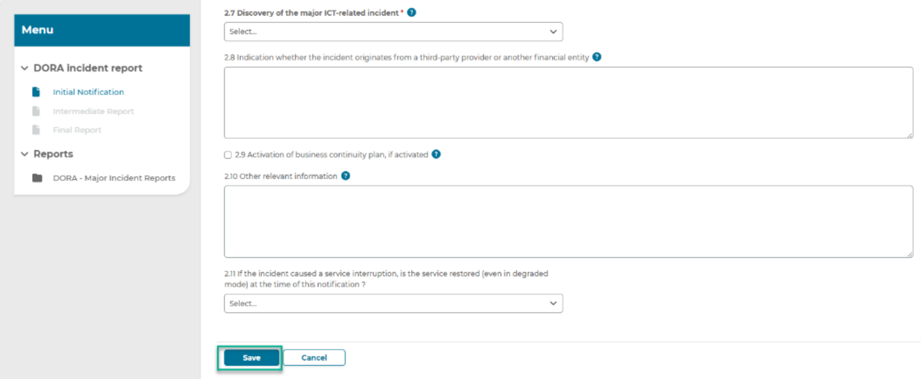
2.4.2.2. Filling in the first draft of a notification

Once a new incident notification form is created, the user can fill in the information requested. The user can complete and submit the relevant sections of the notification form.

Each section of a notification form can be accessed by clicking on the corresponding name of the section in the navigation Menu.

- **Initial notification**: This section gathers the general information about the incident.
- **Intermediate report**: This second section provides a more detailed description of the incident, its consequences and the corrective measures that were taken to recover.
- **Final report**: This third section provides information regarding the root cause analysis and the resolution of the incident. When submitting this information, the Supervised Entity shall review the other sections and update these, where appropriate.

The user shall always save the information filled-in by clicking on the "**Save**" button at the bottom of the section prior to submitting any section of an incident notification.



2.7 Discovery of the major ICT-related incident *
Select...

2.8 Indication whether the incident originates from a third-party provider or another financial entity

□ 2.9 Activation of business continuity plan, if activated

2.10 Other relevant information

2.11 If the incident caused a service interruption, is the service restored (even in degraded mode) at the time of this notification ?
Select...

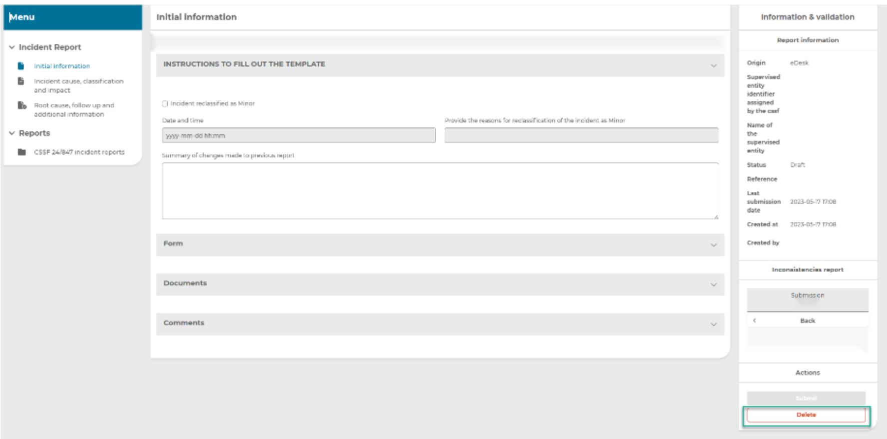
Any saved section will have the status "Draft" and will **not yet be visible by the CSSF**.

The draft data already saved can be deleted any time before the information is submitted to the CSSF via the dedicated "Delete" action button.

2.4.2.3. Deletion of a draft notification

A notification at status "Draft" can be deleted by the Supervised Entity by clicking on the "**Delete**" action button in the "Information & validation" section.

Any deleted notification cannot be restored and shall be started over.



□ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor

Summary of changes made to previous report

Origin: eDesk

Supervised entity identifier assigned by the cssf:

Name of the supervised entity:

Status: Draft

Reference:

Last submission date: 2023-05-17 17:08

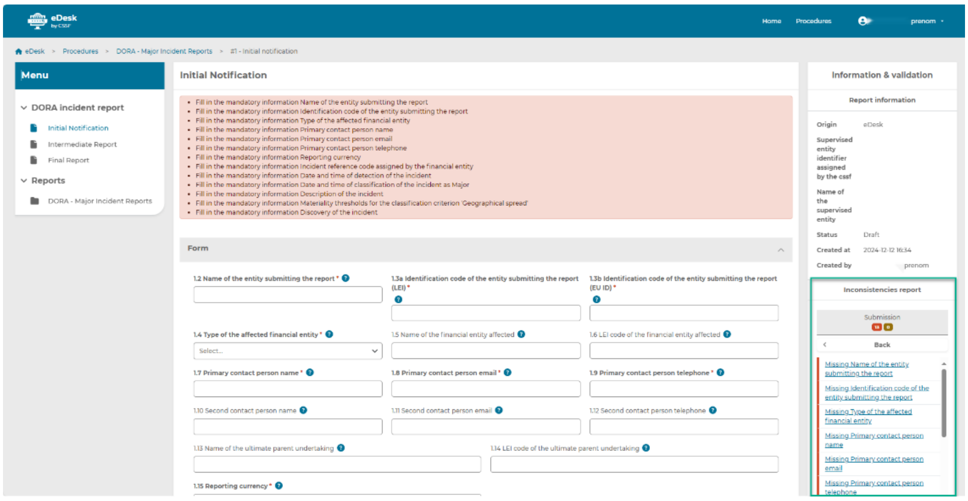
Created at: 2023-05-17 17:08

Created by:

2.4.2.4. Submission of a draft notification

A notification can be submitted by clicking the “**Submit**” action button in the “Information & validation” section.

The system automatically prevents the user from submitting any incomplete notification form to the CSSF. In such case, the system will display a list of the missing data at the top of the form, as well as in the “Inconsistencies report” in the right section.



Initial Notification

- Fill in the mandatory information Name of the entity submitting the report
- Fill in the mandatory information Identification code of the entity submitting the report
- Fill in the mandatory information Type of the affected financial entity
- Fill in the mandatory information Primary contact person name
- Fill in the mandatory information Primary contact person email
- Fill in the mandatory information Primary contact person telephone
- Fill in the mandatory information Reporting currency
- Fill in the mandatory information Incident reference code assigned by the financial entity
- Fill in the mandatory information Date and time of detection of the incident
- Fill in the mandatory information Date and time of classification of the incident as Major
- Fill in the mandatory information Description of the incident
- Fill in the mandatory information Materiality thresholds for the classification criterion 'Geographical spread'
- Fill in the mandatory information Discovery of the incident

Form

1.2 Name of the entity submitting the report *
1.3a Identification code of the entity submitting the report (LEI) *
1.3b Identification code of the entity submitting the report (EU ID) *
1.4 Type of the affected financial entity * Select...
1.5 Name of the financial entity affected
1.6 LEI code of the financial entity affected
1.7 Primary contact person name *
1.8 Primary contact person email *
1.9 Primary contact person telephone *
1.10 Second contact person name
1.11 Second contact person email
1.12 Second contact person telephone
1.13 Name of the ultimate parent undertaking
1.14 LEI code of the ultimate parent undertaking
1.15 Reporting currency *

Report information

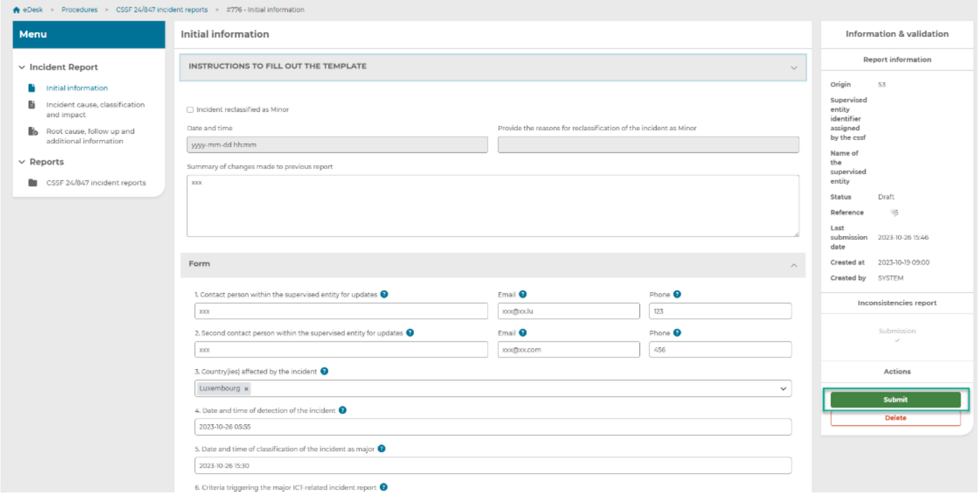
Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Created at	2024-12-12 16:34
Created by	prenom

Inconsistencies report

Submission 13 0

- Missing Name of the entity submitting the report
- Missing Identification code of the entity submitting the report
- Missing Type of the affected financial entity
- Missing Primary contact person name
- Missing Primary contact person email
- Missing Primary contact person telephone

Once the form is filled-in with the mandatory information and the changes are saved, the “**Submit**” button will be enabled.


eDesk > Procedures > CSSF 24/847 incident reports > #776 - Initial information
Menu
Incident Report
Initial information
Incident cause, classification and impact
Root cause, follow up and additional information
Reports
CSSF 24/847 incident reports
INSTRUCTIONS TO FILL OUT THE TEMPLATE
Information & validation
Actions
Submit
Delete

Initial information

□ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor

Summary of changes made to previous report: xxx

Form

1. Contact person within the supervised entity for updates: xxx — Email: xxx@xx.lu — Phone: 123
2. Second contact person within the supervised entity for updates: xxx — Email: xxx@xx.com — Phone: 456
3. Country(ies) affected by the incident: Luxembourg
4. Date and time of detection of the incident: 2023-10-26 05:55
5. Date and time of classification of the incident as major: 2023-10-26 15:30
6. Criteria triggering the major ICT-related incident report

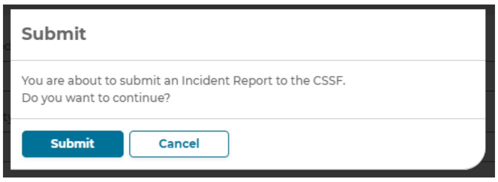
Report information

Origin	S3
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Reference	
Last submission date	2023-10-26 15:46
Created at	2023-10-19 09:00
Created by	SYSTEM

Inconsistencies report

Submission ✓

When clicking on the “Submit” button, a confirmation window will pop up for the user to confirm the requested action. The user will have to confirm this action for the notification to be submitted to the CSSF.

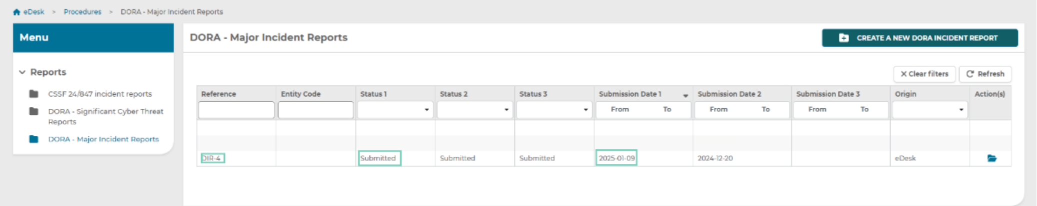


Submit

You are about to submit an Incident Report to the CSSF.
Do you want to continue?

Once confirmed, the status of this submitted section of the notification will change to "Submitted" and its respective submission date will be automatically displayed in the "Report information" section, as well as in the dashboard.

A dedicated reference will also be automatically assigned to this submitted notification. Unlike the status, the filing reference is unique for the 3 sections of an incident notification.


eDesk > Procedures > DORA - Major Incident Reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
CREATE A NEW DORA INCIDENT REPORT
Clear filters
Refresh

DORA - Major Incident Reports

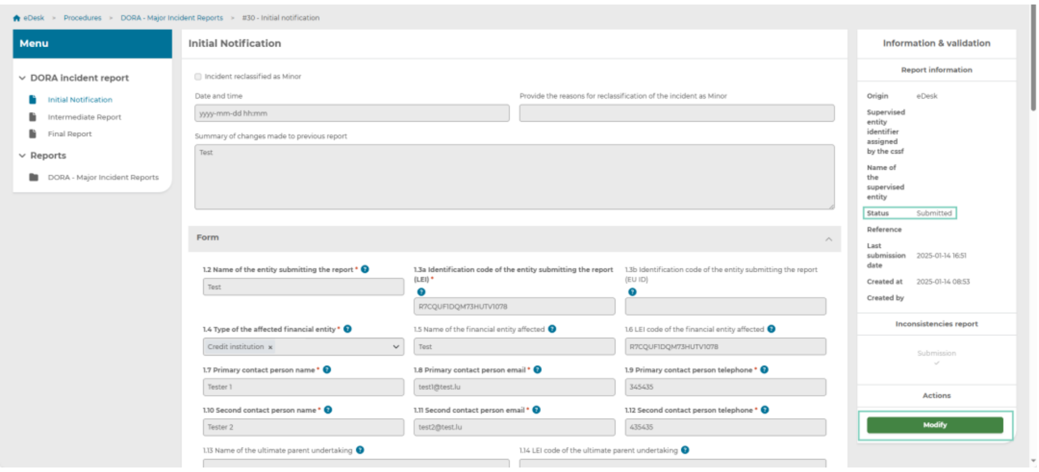
Reference	Entity Code	Status 1	Status 2	Status 3	Submission Date 1	Submission Date 2	Submission Date 3	Origin	Action(s)
					From To	From To	From To		
DIR-4		Submitted	Submitted	Submitted	2025-01-09	2024-12-20		eDesk	

Important: The section "Initial information" or "Initial notification" of a notification shall be submitted first, followed by the section "Incident cause, classification and impact" or "Intermediate report", and lastly the section "Root cause, follow up and additional information" or "Final report.

2.4.3. Modification of a submitted notification

If the Supervised Entity has updates to an incident report already submitted, an updated version of the form may be submitted.

In this case, the user shall click on the action "Modify", that is only available at status "Submitted".



Initial Notification

□ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor:

Summary of changes made to previous report: Test

1.2 Name of the entity submitting the report *: Test

1.3a Identification code of the entity submitting the report (LEI) *: R7CQUFIDQM73HUTV1078

1.3b Identification code of the entity submitting the report (EU ID):

1.4 Type of the affected financial entity *: Credit institution

1.5 Name of the financial entity affected: Test

1.6 LEI code of the financial entity affected: R7CQUFIDQM73HUTV1078

1.7 Primary contact person name *: Tester 1

1.8 Primary contact person email *: test1@test.lu

1.9 Primary contact person telephone *: 345435

1.10 Second contact person name *: Tester 2

1.11 Second contact person email *: test2@test.lu

1.12 Second contact person telephone *: 435435

1.13 Name of the ultimate parent undertaking

1.14 LEI code of the ultimate parent undertaking

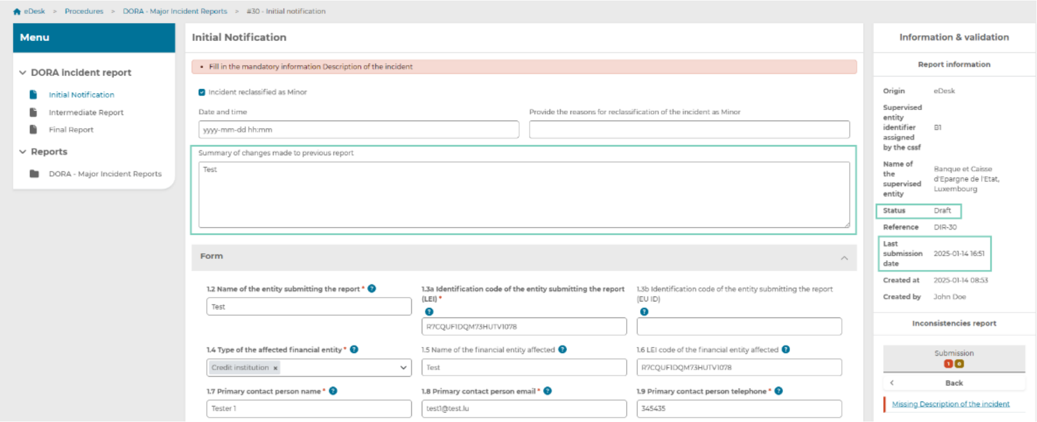
Report information

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Submitted
Reference	
Last submission date	2025-01-14 16:51
Created at	2025-01-14 08:53
Created by	

A new information "Last submission date" is then displayed in the "Report information" for the user to easily differentiate a new form from an update of an already submitted one.

For any modification of an already submitted form, the user must complete the section "Summary of changes made to previous report".

A modified form reverts to the status "Draft" and must be saved and submitted again via the "**Submit**" action, for the CSSF to receive the updated information.



Initial Notification

- Fill in the mandatory information Description of the incident

☑ Incident reclassified as Minor

Date and time: yyyy-mm-dd hh:mm

Provide the reasons for reclassification of the incident as Minor:

Summary of changes made to previous report: Test

1.2 Name of the entity submitting the report *: Test

1.3a Identification code of the entity submitting the report (LEI) *: R7CQUF1DQM73HUTV1078

1.3b Identification code of the entity submitting the report (EU ID):

1.4 Type of the affected financial entity *: Credit institution

1.5 Name of the financial entity affected: Test

1.6 LEI code of the financial entity affected: R7CQUF1DQM73HUTV1078

1.7 Primary contact person name *: Tester 1

1.8 Primary contact person email *: test1@test.lu

1.9 Primary contact person telephone *: 345435

Origin	eDesk
Supervised entity identifier assigned by the cssf	B1
Name of the supervised entity	Banque et Caisse d'Epargne de l'Etat, Luxembourg
Status	Draft
Reference	DIR-30
Last submission date	2025-01-14 16:51
Created at	2025-01-14 08:53
Created by	John Doe

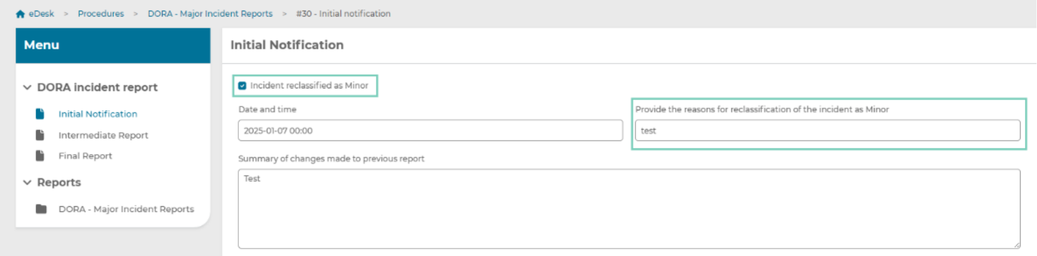
Missing Description of the incident

Any new ongoing version of a form can be deleted via the "Delete" action, which, if confirmed via the usual popup window, brings the user back to its previous submitted version.

Important: An incident notification with the status "Closed" can no longer be modified. New document(s) or comment(s) can however still be added and submitted.

2.4.4. Reclassification of an incident

In case the incident no longer fulfils the criteria to be considered as major, the user can reclassify the incident notification in the system. The incident shall then be reclassified as minor by ticking the dedicated box at the top of the "Initial information" or "Initial notification" section of the notification form. Supervised entities must provide the date and an explanation of the reasons for this reclassification. This option is only available after the initial submission of the notification form.


eDesk > Procedures > DORA - Major Incident Reports > #30 - Initial notification
Menu
DORA Incident report
Initial Notification
Intermediate Report
Final Report
Reports
DORA - Major Incident Reports

Initial Notification

☑ Incident reclassified as Minor

Date and time: 2025-01-07 00:00

Provide the reasons for reclassification of the incident as Minor: test

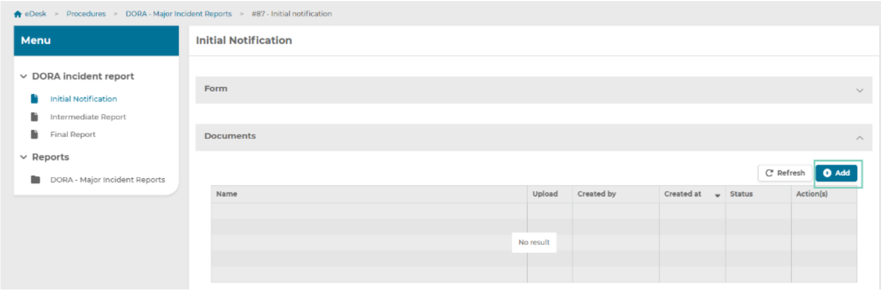
Summary of changes made to previous report: Test

2.4.5. Addition of document(s) to the notification form

The “**Documents**” part allows the user to attach document(s) to its notification where applicable.

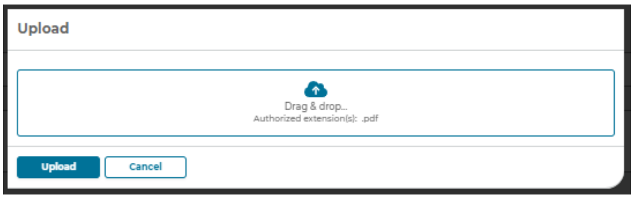
To add a document, follow the steps below:

1. Click on the “Add” button.



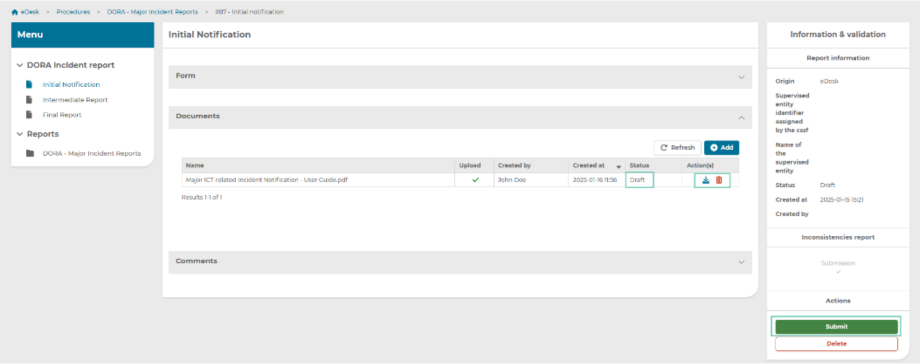
Name	Upload	Created by	Created at	Status	Action(s)
No result					

2. A new window will open allowing the user to upload a new document. <u>Note</u>: only pdf extension is authorized.



The document is then uploaded and attached to the dedicated section with status “Draft” and can be downloaded or deleted by the user.

Document(s) attached to a specific section of an incident notification are submitted to the CSSF together with the corresponding section of the “Form”, via the action “**Submit**”. Document(s) added to closed files shall be submitted individually.

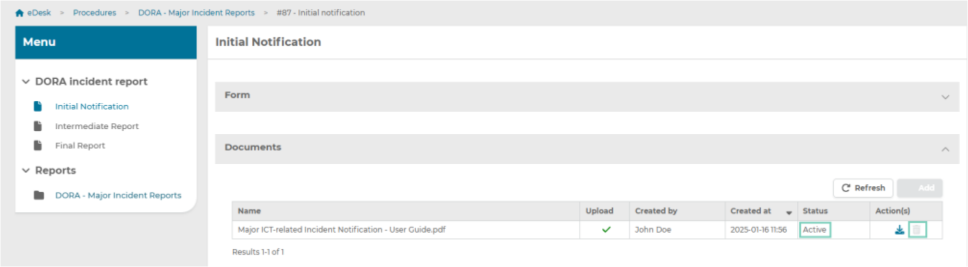


Name	Upload	Created by	Created at	Status	Action(s)
Major ICT-related Incident Notification - User Guide.pdf	✓	John Doe	2025-01-16 11:56	Draft	

Results 1-1 of 1

Origin eDesk
Supervised entity identifier assigned by the cssf
Name of the supervised entity
Status Draft
Created at 2025-01-15 15:21
Created by

The deletion action remains available until the section is submitted to the CSSF, changing the status of the document to “Active”.



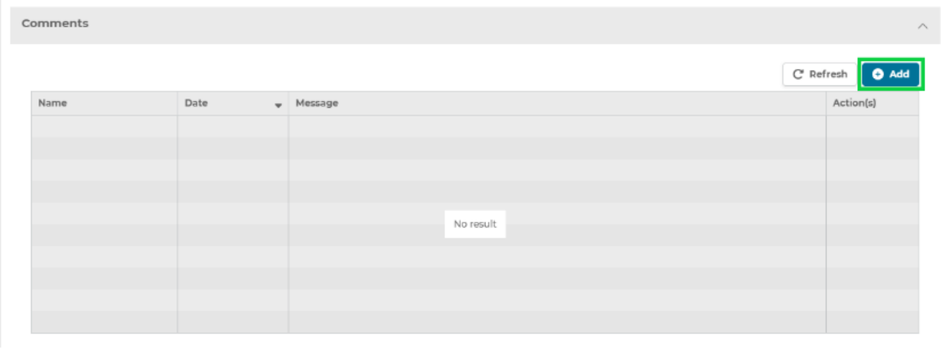
Name	Upload	Created by	Created at	Status	Action(s)
Major ICT-related Incident Notification - User Guide.pdf	✓	John Doe	2025-01-16 11:56	Active	

Results 1-1 of 1

2.4.6. Exchange of comment(s) with the CSSF

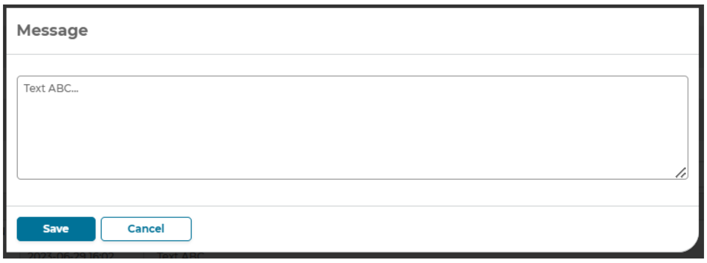
The "**Comments**" part allows the CSSF and supervised entities to exchange comments about the information submitted in the form.

New comments can be created by clicking on "**Add**".



Name	Date	Message	Action(s)
		No result	

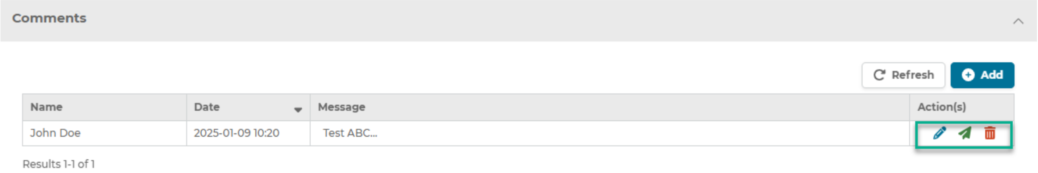
A new window will be displayed, allowing the user to write a text. The user shall then click on the "**Save**" button to save the entered text.



Message

Text ABC...

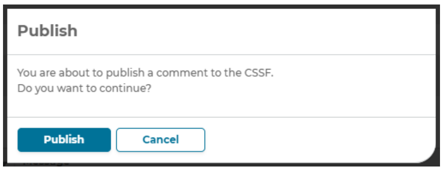
The comment will then be displayed in the dedicated "Comments" section and can be respectively "**Edited**", "**Published to the CSSF**", or "**Deleted**" via the action buttons.



Name	Date	Message	Action(s)
John Doe	2025-01-09 10:20	Test ABC...	

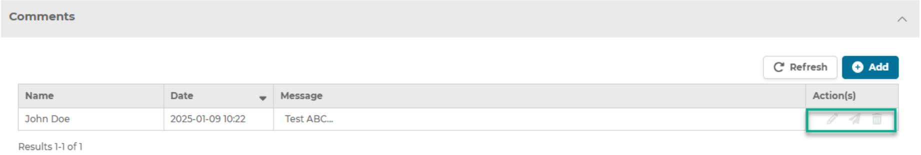
Results 1-1 of 1

Important: The "**Save**" button will only save a draft version of a comment but will not send the comment to the CSSF. To send a comment to the CSSF, the user shall click on the "**Publish**" icon and confirm the action in the popup window. Once the comment is published to the CSSF it can no longer be edited or deleted.



Publish

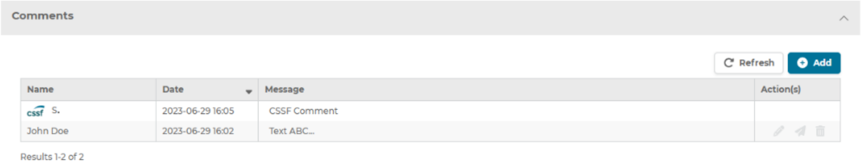
You are about to publish a comment to the CSSF.
Do you want to continue?



Name	Date	Message	Action(s)
John Doe	2025-01-09 10:22	Test ABC...	

Results 1-1 of 1

The comments published by the CSSF to the Supervised Entity will be visible in the same section. Those comments have the CSSF logo before the name of the CSSF agent who published it.



Name	Date	Message	Action(s)
cssf S.	2023-06-29 16:05	CSSF Comment	
John Doe	2023-06-29 16:02	Text ABC...	

Results 1-2 of 2

Comments can be added and published any time after the initial submission of the "Initial information" or "Initial notification" section.

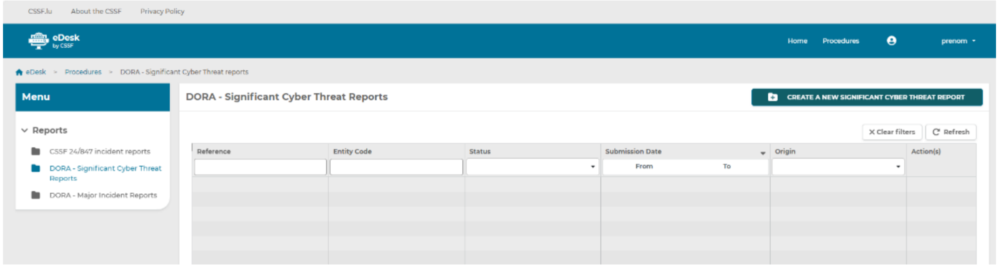
2.5. DORA - Significant Cyber Threat Reports

The following actions are possible:

- Creation of a new notification
- Modification of a submitted notification
- Addition of document(s) to the notification form
- Exchange of comment(s) with the CSSF

2.5.1. Dashboard of DORA - Significant Cyber Threat Reports notifications

When connecting to the modules, the main part of the page is a dashboard providing a general view of all the notifications created by the Supervised Entity, with usual filtering and sorting functionalities.


CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > DORA - Significant Cyber Threat reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
DORA - Significant Cyber Threat Reports
CREATE A NEW SIGNIFICANT CYBER THREAT REPORT
Clear filters
Refresh

Reference	Entity Code	Status	Submission Date	Origin	Action(s)
			From To		

The dashboard for **DORA - Significant Cyber Threat Reports** contains the following columns:

- **Reference:** Reference of the major ICT-related incident notification, automatically assigned once a notification is submitted,
- **Entity code**: CSSF code of the Supervised Entity,
- **Status:** Status of the form. The value of each status can be either "Draft", "Submitted" or "Closed",
- **Submission Date**: Date of the form submission,
- **Origin**: The submission channel through which the incident was submitted to the CSSF. The value will be either "eDesk" or "S3",
- **Action(s):** The Supervised Entity can "open" the notification form by clicking on the "folder" icon. The entity can also double-click on a given line to consult a form.

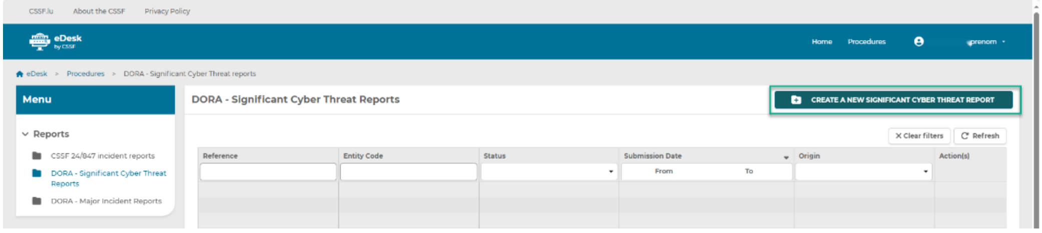
Above the dashboard, a top banner contains several links and useful information:

- a link to the **global eDesk** dashboard (by clicking on the eDesk logo or “**Home**”),
- a link to the procedures accessible by the connected Supervised Entity user (by clicking on “**Procedures**”),
- the **name** of the user connected and corresponding Supervised Entity name *(not visible in the above illustration)*, with a small arrow on the right which can be used to access:
  - the “User profile” by clicking “Manage profile”,
  - the “Entity management” (available only for the advanced users), and
  - the Logout functionality.

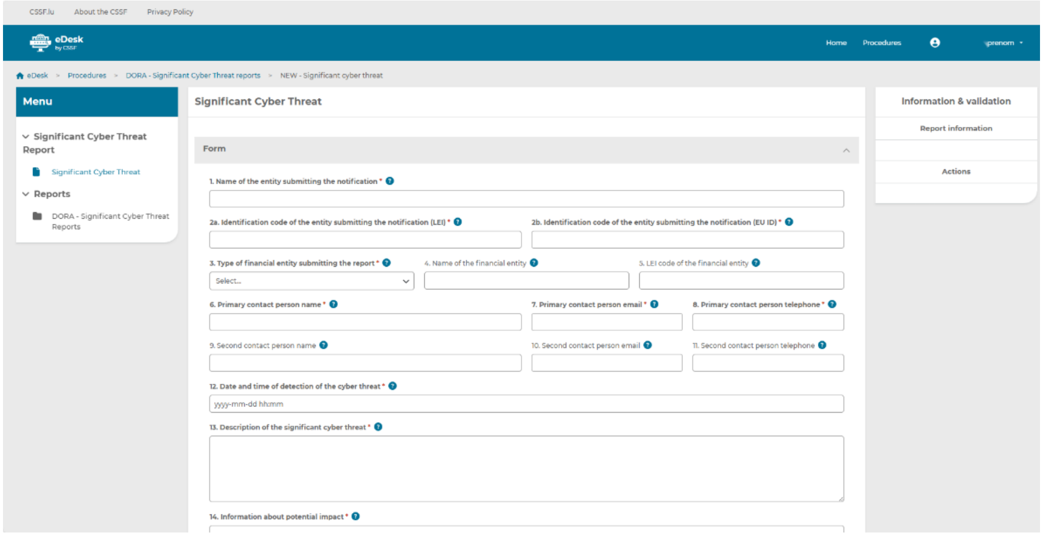
Below the top banner is a button labelled “**CREATE A NEW SIGNIFICANT CYBER THREAT REPORT**” which allows the Supervised Entity to create a new incident notification. Further details are provided in the next section.

2.5.2. Creation of a new notification

To create a new Significant Cyber Threat report, the user shall click on the “**CREATE A NEW SIGNIFICANT CYBER THREAT REPORT**” button on the dashboard page.

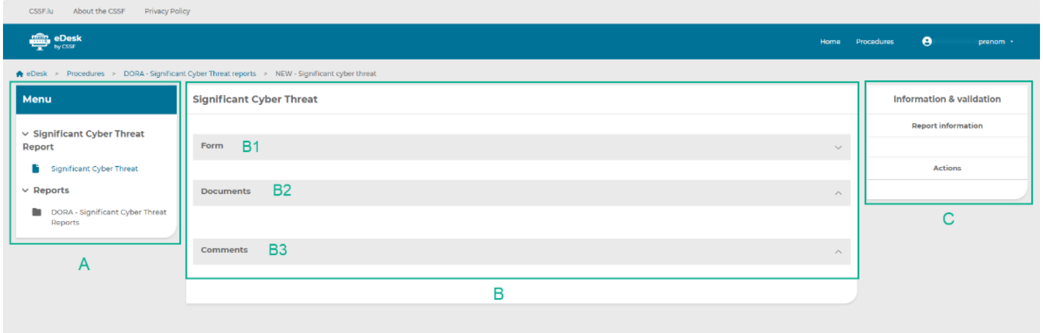

CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > DORA - Significant Cyber Threat reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
DORA - Significant Cyber Threat Reports
CREATE A NEW SIGNIFICANT CYBER THREAT REPORT
Clear filters
Refresh
Reference
Entity Code
Status
Submission Date
From
To
Origin
Action(s)

Once the button is clicked, a new incident notification page opens.

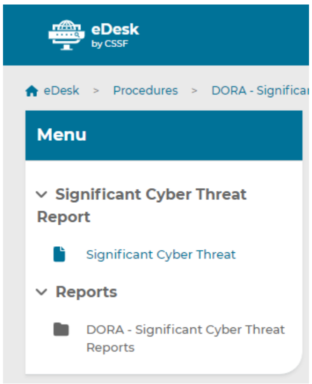

CSSF.lu
About the CSSF
Privacy Policy
eDesk by CSSF
Home
Procedures
prenom
eDesk > Procedures > DORA - Significant Cyber Threat reports > NEW - Significant cyber threat
Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports
Significant Cyber Threat
Form
1. Name of the entity submitting the notification *
2a. Identification code of the entity submitting the notification (LEI) *
2b. Identification code of the entity submitting the notification (EU ID) *
3. Type of financial entity submitting the report *
Select...
4. Name of the financial entity
5. LEI code of the financial entity
6. Primary contact person name *
7. Primary contact person email *
8. Primary contact person telephone *
9. Second contact person name
10. Second contact person email
11. Second contact person telephone
12. Date and time of detection of the cyber threat *
yyyy-mm-dd hh:mm
13. Description of the significant cyber threat *
14. Information about potential impact *
Information & validation
Report information
Actions

To ease the navigation within the form, sub-sections can be reduced by clicking on the greyed out sub-section’s title.

2.5.2.1. Description of the notification form structure



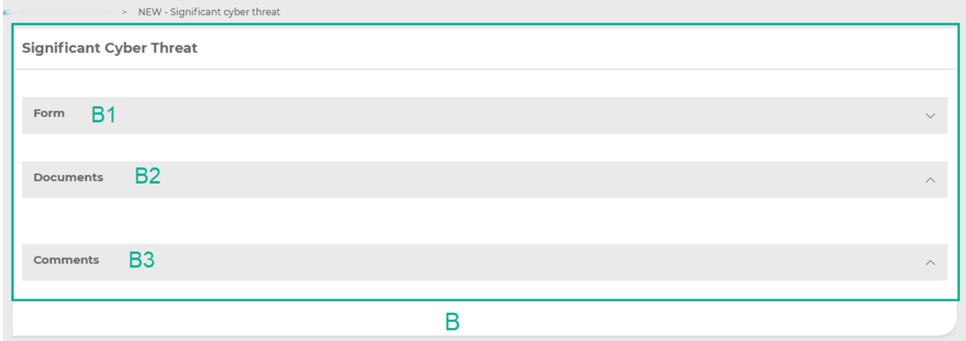
2.5.2.1.1. Navigation Menu (A)


eDesk
by CSSF
eDesk > Procedures > DORA - Significa
Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports

The left part of the screen is dedicated to:

- the navigation within the notification form,
- "DORA - Significant Cyber Threat Reports": this allows the Supervised Entity to return to the main dashboard and access the ongoing or completed notifications.

2.5.2.1.2. The information to be filled in by the Supervised Entity (B)

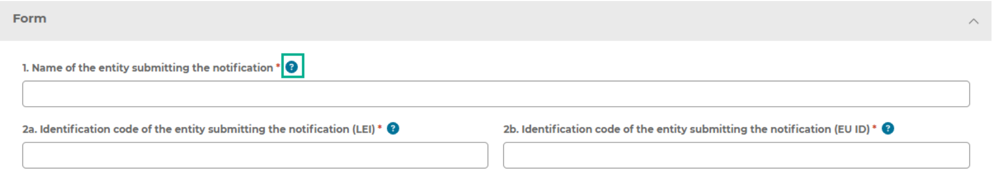


The main part of the notification page devoted to form information, identified in the figure above as "B", is the part of the screen where the metadata relating to the incident notification is displayed. This part is made up of the following sub-sections:

- **B1**: "**Form**",
- **B2**: "**Documents**", and
- **B3**: "**Comments**"

The "**Form**" (B1) part contains the questions related to the incident, to be answered by the Supervised Entity.

Explanatory notes are available by hovering over the "question mark" symbol to provide further explanations regarding the information to be provided by the Supervised Entity.

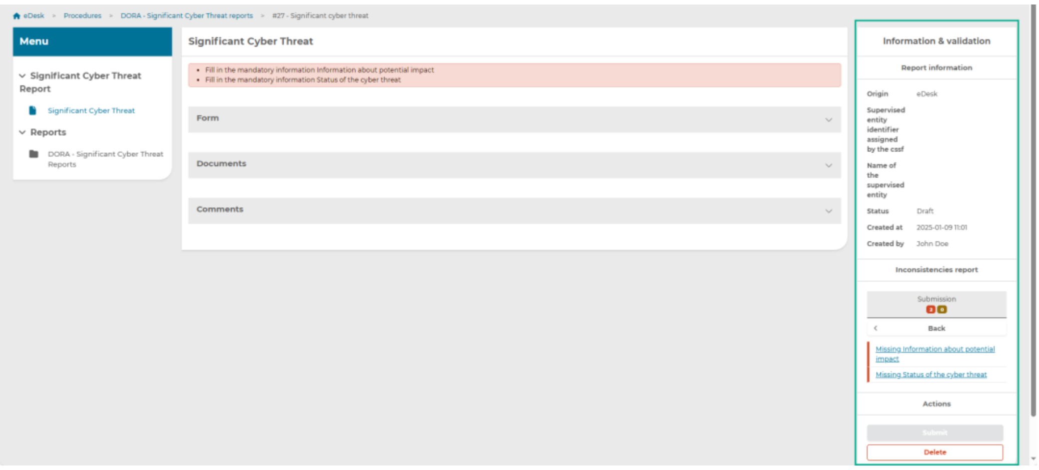


1. Name of the entity submitting the notification * ?

2a. Identification code of the entity submitting the notification (LEI) * ?

2b. Identification code of the entity submitting the notification (EU ID) * ?

2.5.2.1.3. Information and validation (C)



- Fill in the mandatory information Information about potential impact
- Fill in the mandatory information Status of the cyber threat

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Created at	2025-01-09 11:01
Created by	John Doe

Missing Information about potential impact

Missing Status of the cyber threat

The "**Information & validation**" section of the screen covers the following:

- "**Report information**": Provides general information of the Supervised Entity such as the Supervised Entity's name, and code, the status of the notification, the creation date and the user who created the notification.

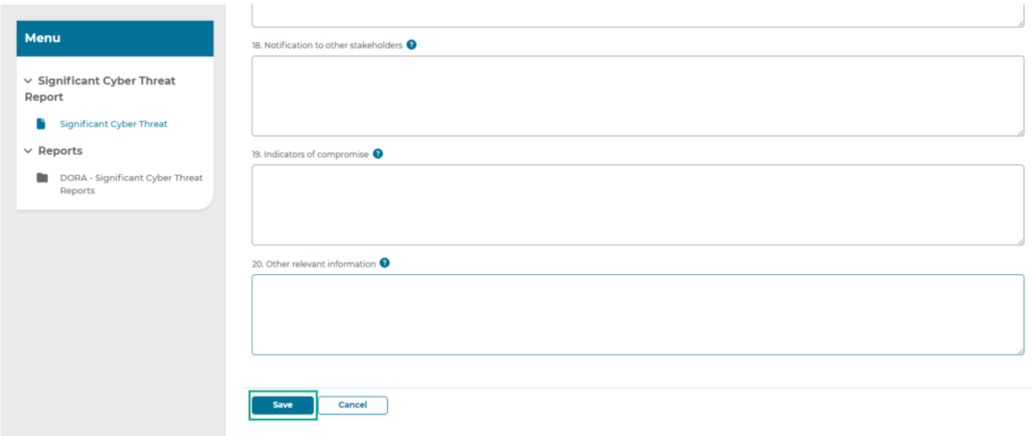
- "**Inconsistencies report**": Displays the potential missing information and inconsistencies to be resolved by the Supervised Entity before submitting the notification to the CSSF.

- "**Actions**": These are action buttons that represent actions that can be taken by the user at any given point in time. Actions could be for example Submit, Delete or Modify. When actions are "greyed", the action button cannot be clicked. This may be because the report is incomplete, or the incident has already been closed on the side of the CSSF.

2.5.2.2. Filling in the first draft of a notification

Once a new Significant Cyber Threat report form is created, the user can fill in the information requested. The user can complete and submit the relevant sections of the notification form.

> The user shall always save the information filled-in by clicking on the "**Save**" button at the bottom of the section prior to submitting any section of an incident notification.


Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports
Save
Cancel

18. Notification to other stakeholders

19. Indicators of compromise

20. Other relevant information

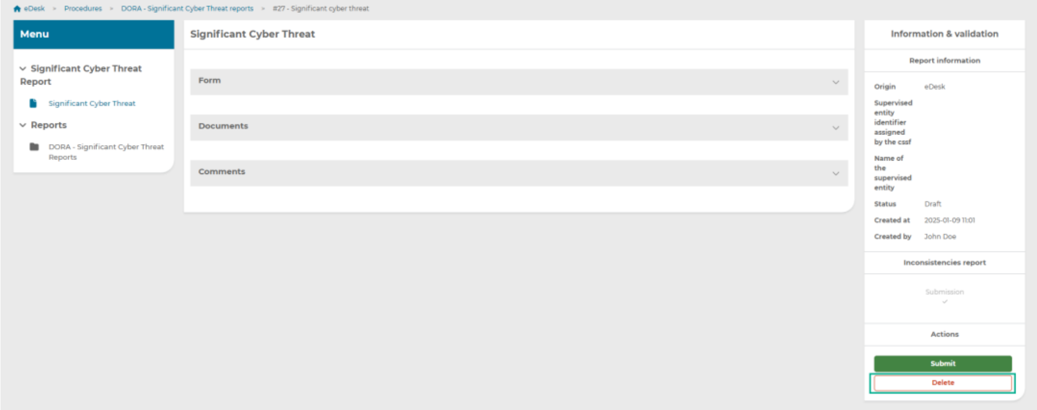
Any saved section will have the status “Draft” and will **not yet be visible by the CSSF**.

The draft data already saved can be deleted any time before the information is submitted to the CSSF via the dedicated “Delete” action button.

2.5.2.3. Deletion of a draft notification

A notification at status “Draft” can be deleted by the Supervised Entity by clicking on the “**Delete**” action button in the “Information & validation” section.

Any deleted notification cannot be restored and shall be started over.

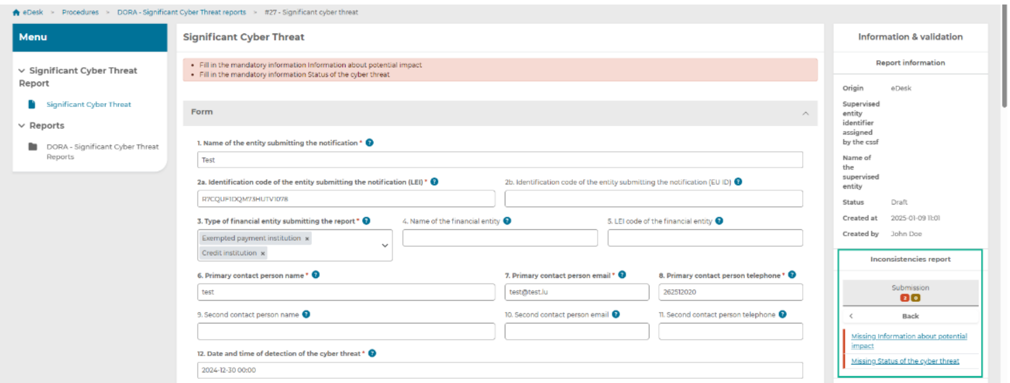


Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Created at	2025-01-09 11:01
Created by	John Doe

2.5.2.4. Submission of a draft notification

A notification can be submitted by clicking the “**Submit**” action button in the “Information & validation” section.

The system automatically prevents the user from submitting any incomplete notification form to the CSSF. In such case, the system will display a list of the missing data at the top of the form, as well as in the “Inconsistencies report” in the right section.


eDesk > Procedures > DORA - Significant Cyber Threat reports > #27 - Significant cyber threat
Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports
Form
Information & validation
Report information
Inconsistencies report
Submission
2
0
Back

Significant Cyber Threat

- Fill in the mandatory information Information about potential impact
- Fill in the mandatory information Status of the cyber threat

1. Name of the entity submitting the notification *: Test

2a. Identification code of the entity submitting the notification (LEI) *: R7CQUF1DQM73HUTV1078

2b. Identification code of the entity submitting the notification (EU ID):

3. Type of financial entity submitting the report *: Exempted payment institution ×, Credit institution ×

4. Name of the financial entity:

5. LEI code of the financial entity:

6. Primary contact person name *: test

7. Primary contact person email *: test@test.lu

8. Primary contact person telephone *: 262512020

9. Second contact person name:

10. Second contact person email:

11. Second contact person telephone:

12. Date and time of detection of the cyber threat *: 2024-12-30 00:00

Origin: eDesk

Supervised entity identifier assigned by the cssf:

Name of the supervised entity:

Status: Draft

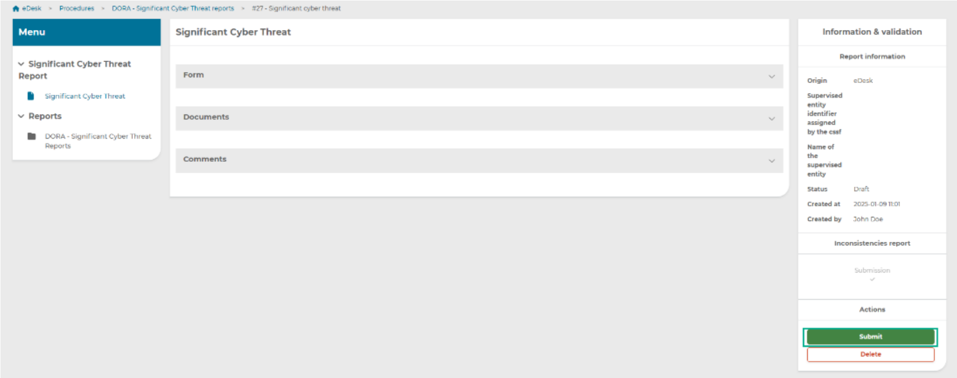
Created at: 2025-01-09 11:01

Created by: John Doe

Missing Information about potential impact

Missing Status of the cyber threat

Once the form is filled-in with the mandatory information and the changes are saved, the "**Submit**" button will be enabled.



Origin: eDesk

Supervised entity identifier assigned by the cssf:

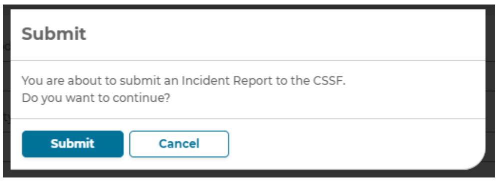
Name of the supervised entity:

Status: Draft

Created at: 2025-01-09 11:01

Created by: John Doe

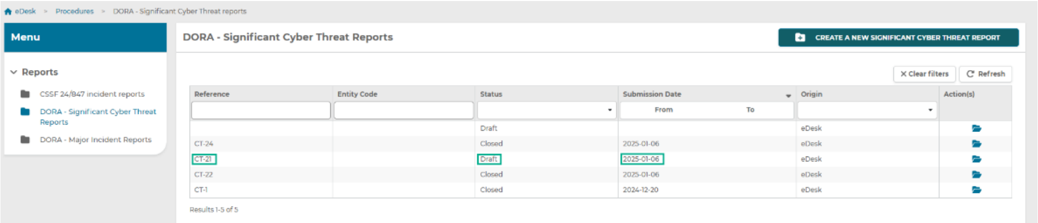
When clicking on the "Submit" button, a confirmation window will pop up for the user to confirm the requested action. The user will have to confirm this action for the notification to be submitted to the CSSF.



You are about to submit an Incident Report to the CSSF.
Do you want to continue?

Once confirmed, the status of this section of the notification will change to "Submitted" and its submission date will be automatically displayed in the "Report information" section, as well as in the dashboard.

A dedicated reference will also be automatically assigned to this submitted notification.


eDesk > Procedures > DORA - Significant Cyber Threat reports
Menu
Reports
CSSF 24/847 incident reports
DORA - Significant Cyber Threat Reports
DORA - Major Incident Reports
CREATE A NEW SIGNIFICANT CYBER THREAT REPORT
Clear filters
Refresh
From
To

DORA - Significant Cyber Threat Reports

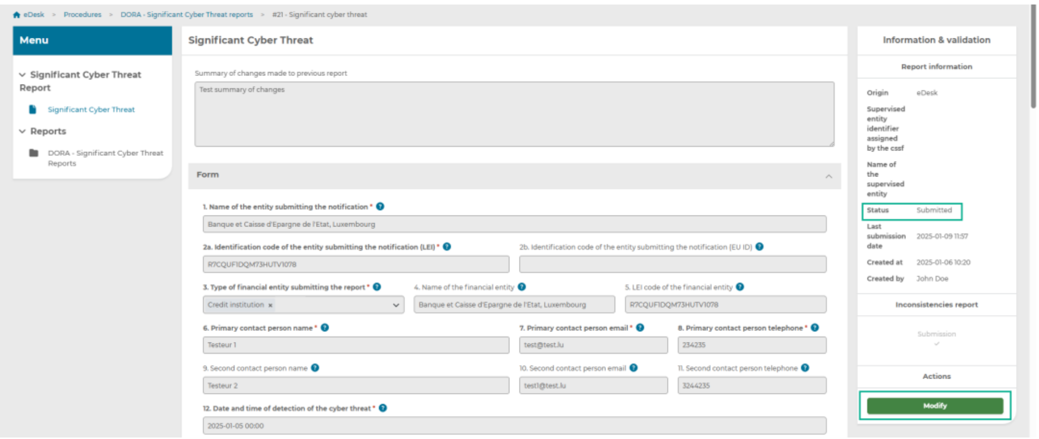
Reference	Entity Code	Status	Submission Date	Origin	Action(s)
		Draft		eDesk	
CT-24		Closed	2025-01-06	eDesk	
CT-21		Draft	2025-01-06	eDesk	
CT-22		Closed	2025-01-06	eDesk	
CT-1		Closed	2024-12-20	eDesk	

Results 1-5 of 5

2.5.3. Modification of a submitted notification

If the Supervised Entity has updates to a Significant Cyber Threat report already submitted, an updated version of the form may be submitted.

In this case, the user shall click on the action "Modify", that is only available at status "Submitted".


eDesk > Procedures > DORA - Significant Cyber Threat reports > #21 - Significant cyber threat
Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports
Form
Information & validation
Report information
Inconsistencies report
Submission
Actions
Modify

Significant Cyber Threat

Summary of changes made to previous report: Test summary of changes

1. Name of the entity submitting the notification *: Banque et Caisse d'Epargne de l'Etat, Luxembourg

2a. Identification code of the entity submitting the notification (LEI) *: R7CQUFIDQM73HUTV1078

2b. Identification code of the entity submitting the notification (EU ID):

3. Type of financial entity submitting the report *: Credit institution

4. Name of the financial entity: Banque et Caisse d'Epargne de l'Etat, Luxembourg

5. LEI code of the financial entity: R7CQUFIDQM73HUTV1078

6. Primary contact person name *: Testeur 1

7. Primary contact person email *: test@test.lu

8. Primary contact person telephone *: 234235

9. Second contact person name: Testeur 2

10. Second contact person email: test1@test.lu

11. Second contact person telephone: 3244235

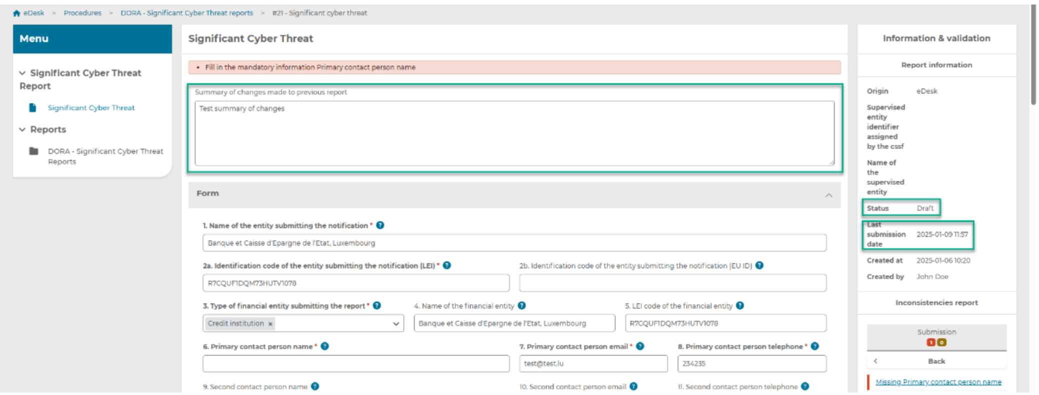
12. Date and time of detection of the cyber threat *: 2025-01-05 00:00

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Submitted
Last submission date	2025-01-09 11:57
Created at	2025-01-06 10:20
Created by	John Doe

A new information "Last submission date" is then displayed in the "Report information" for the user to easily differentiate a new form from an update of an already submitted one.

For any modification of an already submitted form, the user must complete the section "Summary of changes made to previous report".

A modified form reverts to the status "Draft" and must be saved and submitted again via the "**Submit**" action, for the CSSF to receive the updated information.


eDesk > Procedures > DORA - Significant Cyber Threat reports > #21 - Significant cyber threat
Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports
Form
Information & validation
Report information
Inconsistencies report
Submission
1
0
Back

Significant Cyber Threat

- Fill in the mandatory information Primary contact person name

Summary of changes made to previous report: Test summary of changes

1. Name of the entity submitting the notification *: Banque et Caisse d'Epargne de l'Etat, Luxembourg

2a. Identification code of the entity submitting the notification (LEI) *: R7CQUFIDQM73HUTV1078

2b. Identification code of the entity submitting the notification (EU ID):

3. Type of financial entity submitting the report *: Credit institution

4. Name of the financial entity: Banque et Caisse d'Epargne de l'Etat, Luxembourg

5. LEI code of the financial entity: R7CQUFIDQM73HUTV1078

6. Primary contact person name *:

7. Primary contact person email *: test@test.lu

8. Primary contact person telephone *: 234235

9. Second contact person name

10. Second contact person email

11. Second contact person telephone

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Last submission date	2025-01-09 11:57
Created at	2025-01-06 10:20
Created by	John Doe

Missing Primary contact person name

Any new ongoing version of a form can be deleted via the "Delete" action, which, if confirmed via the usual popup window, brings the user back to its previous submitted version.

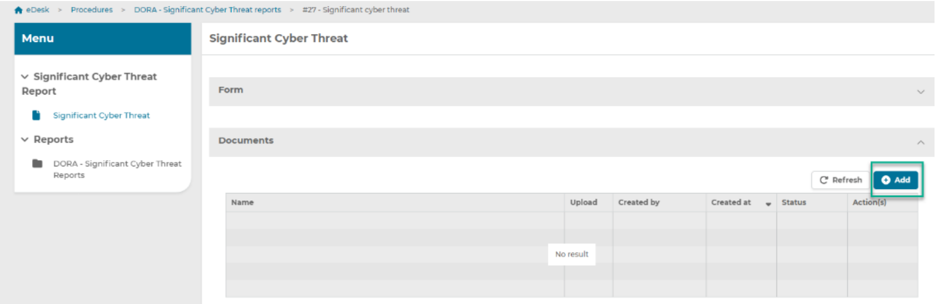
Important: A Significant Cyber Threat report with the status "Closed" can no longer be modified. New document(s) or comment(s) can however still be added and submitted.

2.5.4. Addition of document(s) to the notification form

The “**Documents**” part allows the user to attach document(s) to its notification where applicable.

To add a document, follow the steps below:

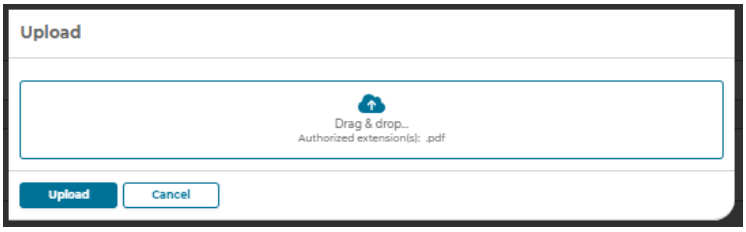
1. Click on the “Add” button.



eDesk > Procedures > DORA - Significant Cyber Threat reports > #27 - Significant cyber threat

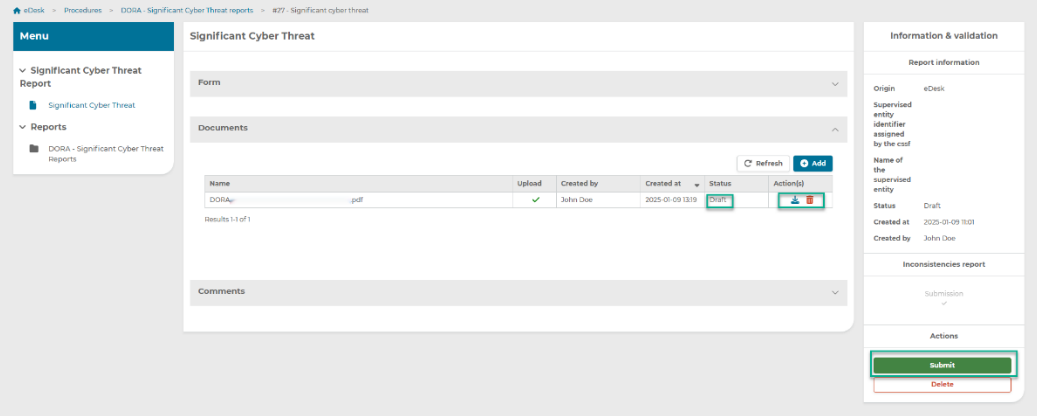
Name	Upload	Created by	Created at	Status	Action(s)
No result					

2. A new window will open allowing the user to upload a new document. **Note**: only pdf extension is authorized.



The document is then uploaded and attached to the dedicated section with status “Draft” and can be downloaded or deleted by the user.

Document(s) attached to a specific section of an incident notification are submitted to the CSSF together with the corresponding section of the “Form”, via the action “**Submit**”. Document(s) added to closed files shall be submitted individually.



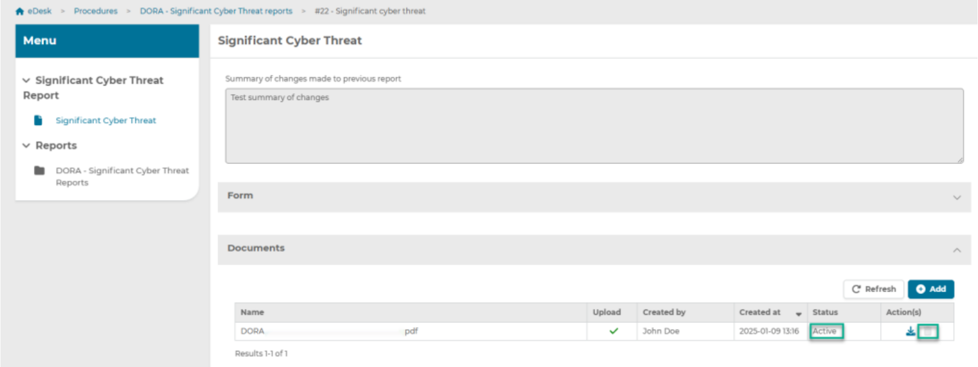
eDesk > Procedures > DORA - Significant Cyber Threat reports > #27 - Significant cyber threat

Name	Upload	Created by	Created at	Status	Action(s)
DORA[redacted].pdf	✓	John Doe	2025-01-09 13:19	Draft	

Results 1-1 of 1

Origin	eDesk
Supervised entity identifier assigned by the cssf	
Name of the supervised entity	
Status	Draft
Created at	2025-01-09 11:01
Created by	John Doe

The deletion action remains available until the section is submitted to the CSSF, changing the status of the document to "Active".



eDesk > Procedures > DORA - Significant Cyber Threat reports > #22 - Significant cyber threat

Menu
Significant Cyber Threat Report
Significant Cyber Threat
Reports
DORA - Significant Cyber Threat Reports

Significant Cyber Threat

Summary of changes made to previous report

Test summary of changes

Form
Documents
Refresh
Add

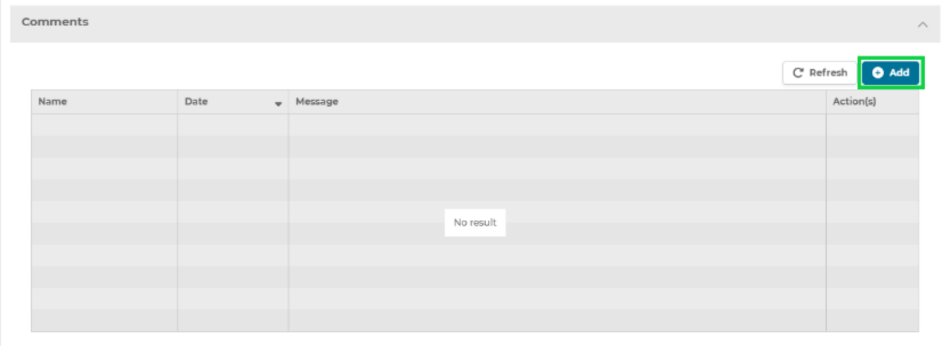
Name	Upload	Created by	Created at	Status	Action(s)
DORA pdf	✓	John Doe	2025-01-09 13:16	Active	

Results 1-1 of 1

2.5.5. Exchange of comment(s) with the CSSF

The "**Comments**" part allows the CSSF and supervised entities to exchange comments about the information submitted in the form.

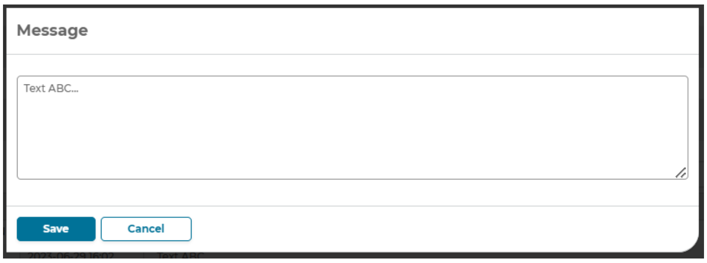
New comments can be created by clicking on "**Add**".



Name	Date	Message	Action(s)

No result

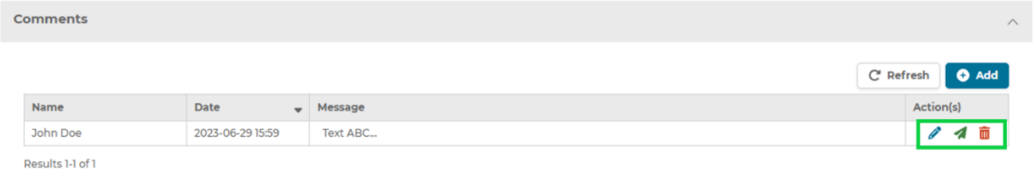
A new window will be displayed, allowing the user to write a text. The user shall then click on the "**Save**" button to save the entered text.



Message

Text ABC...

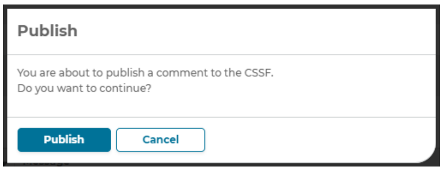
The comment will then be displayed in the dedicated "Comments" section and can be respectively "**Edited**", "**Published to the CSSF**", or "**Deleted**" via the action buttons.



Name	Date	Message	Action(s)
John Doe	2023-06-29 15:59	Text ABC...	

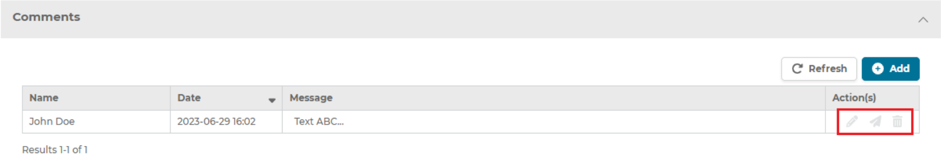
Results 1-1 of 1

Important: The "**Save**" button will only save a draft version of a comment but will **not** send the comment to the CSSF. To send a comment to the CSSF, the user shall click on the "**Publish**" icon and confirm the action in the popup window. Once the comment is published to the CSSF it can no longer be edited or deleted.



Publish

You are about to publish a comment to the CSSF.
Do you want to continue?

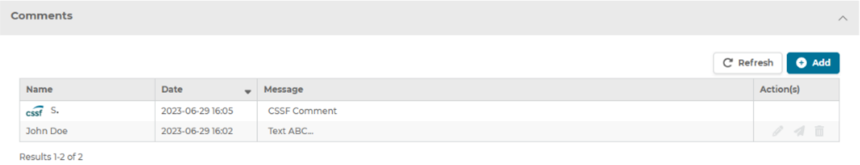


Comments

Name	Date	Message	Action(s)
John Doe	2023-06-29 16:02	Text ABC...	

Results 1-1 of 1

The comments published by the CSSF to the Supervised Entity will be visible in the same section. Those comments have the CSSF logo before the name of the CSSF agent who published it.



Comments

Name	Date	Message	Action(s)
S.	2023-06-29 16:05	CSSF Comment	
John Doe	2023-06-29 16:02	Text ABC...	

Results 1-2 of 2

Comments can be added and published any time after the initial submission of the Significant Cyber Threat report.

3. Notification via the S3 solution

3.1Overview of the S3 solution and prerequisite

S3 or "simple storage service" is the object storage protocol (through a web service interface) used by the CSSF for the file exchange through a S3 compatible transfer client. S3 stores data as objects within buckets.

In S3, Supervised Entities will use the following folders:

- The "**submission**" folder to upload reporting files;
- The "**feedback**" folder to retrieve feedback.

Depending on the transfer client used, the "submission" folder may have to be manually created.

Important: To submit data using S3, Supervised Entities must enrol themselves using the "IT Expert" role. Please refer to the S3 User Guide "Methods of transmitting reports via S3 Application Programming Interface - Technical guidance" available here for detailed explanations on how S3 works and the enrolment process: https://www.cssf.lu/en/methods-of-transmitting-reports-via-api/

3.2Reporting file

3.2.1 Reporting format and naming convention

Data concerning the 3 forms (CSSF 24/847 incident reports, DORA – Major incident reports and DORA – Significant cyber threat reports) for Supervised Entities shall be reported in JavaScript Object Notation (JSON) format file with the extension ".json".

The respective JSON schemas are available here:

- CSSF 24/847 Incident Reports: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/mictir-input-jsonschema-v1_0_0
- DORA - Major Incident Reports: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/dictir-input-jsonschema-v1_0_0
  DORA – Significant Cyber Threat Report: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/ctr-input-jsonschema-v1_0_0

The mandatory naming convention for JSON files is UUID format (universally unique identifier). The files shall be named:

- **MICTIR-ENNNNNNNN-YYYY-MM-DD.json for CSSF 24/847 Incident Reports**
- **DICTIR-ENNNNNNNN-YYYY-MM-DD.json for DORA – Major Incident Reports**
- **CTR-ENNNNNNNN-YYYY-MM-DD.json for DORA – Significant Cyber Threat Reports**

with each component of the name described in the below table:

Code	Meaning	Structure	Authorised value
TYPE	Reporting type	Char(N)	'MICTIR' for CSSF 24/847 Incident Reports 'DICTIR' for DORA – Major Incident Reports 'CTR' for DORA – Significant Cyber Threat Reports
-	Separator	Char(1)	'**-**' (constant)
E	Entity type	Char(1)	**&, A, B, I, F, K, O, P, S, W, Z**
NNNNNNNN	Identification number	Number(8)	**00000001…99999999** (CSSF code of the entity)
-	Separator	Char(1)	'**-**' (constant)
YYYY-MM-DD	Date of the reporting generation	Date	**Date in the specified format**
.json	Extension	Char(5)	**.json** (constant)

The same naming convention also applies for ZIP files, the only difference being the extension of the file.

3.2.2 Submission process

The JSON file and any potential PDF attachments shall be transmitted within a compressed .ZIP file.

The ZIP file shall be uploaded into the "**submission**" folder in the S3 bucket of the Supervised Entity. The upload in other folders is not allowed (e.g.: the "**feedback**" folder is solely dedicated to the CSSF feedback files).

The S3 bucket is only intended to submit data to the CSSF's system, it is not intended for long term storage. Regular cleaning might be performed by CSSF. Supervised Entities are therefore required to, where applicable, take appropriate measures to store the original version of the file they submit via S3.

Important: The S3 submission can either be done via a single file containing the 3 sections[1] of the form, or via separated files containing only certain sections of the form.

3.2.3 Modification of a submitted notification

Via the S3 protocol, Supervised Entities may also submit updates to an already submitted report.

To submit updates, the "**TrackingCode**" provided by the CSSF and corresponding to the notification to be modified shall be indicated in the name of the new file transmitted to the CSSF.

The following naming convention is applicable for the updates:

MICTIR-ENNNNNNNN-YYYY-MM-DD**-TrackingCode**.json for CSSF 24/847 Incident Reports

DICTIR-ENNNNNNNN-YYYY-MM-DD**-TrackingCode**.json for DORA – Major Incident Reports

CTR-ENNNNNNNN-YYYY-MM-DD**-TrackingCode**.json for DORA – Significant Cyber Threat Reports

The "**Summary of changes made to previous report**" shall be completed within the respective submitted section of the JSON file (summaryOfChanges).

Note that an update can neither be submitted on a "**Rejected**" incident notification (see section 3.3.2.1.1), nor on an already "**Closed**" one.

3.2.3.1 Reclassification of an incident

In case the incident no longer fulfils the criteria to be considered as major, the user can reclassify the incident notification via a new S3 submission. The incident shall then be reclassified as minor by indicating "**true**" in the field "**incidentReclassifiedAsMinor**". Supervised entities must provide the **date** (reclassificationDate) and an **explanation** of the reasons for this reclassification (reclassificationReasons). This option is only accepted after the initial submission of the notification.

[1] For CSSF 24/847 Incident Reports: "**initialInfo**" corresponds to the Initial notification ("Initial information" in eDesk); "**detail**" corresponds to the Intermediate notification ("Incident cause, classification and impact" in eDesk); and "**followUp**" corresponds to the Final notification ("Root cause, follow up and additional information" in eDesk)
For DORA – Major Incident Reports: "**initialNotification**" corresponds to the Initial notification in eDesk; "**intermediateReport**" corresponds to the Intermediate report in eDesk; and "**finalReport**" corresponds to the Final report in eDesk)

Important: The reclassification of an incident is not applicable for DORA – Significant Cyber Threat reports.

3.2.3.1 Addition of document(s) to the updated notification

Any document that is listed and attached to the submitted JSON file will be newly created and attached to the existing notification in the CSSF system.

Accordingly, in case the documents already submitted to the CSSF shall not be replaced, the updated JSON file shall not contain the already submitted documents. A document shall only be added to the updated JSON file when a new document is submitted to the CSSF.

In case the same document is re-submitted, duplicate files will be created in the system.

3.2.4 Consistency verification rules

The CSSF will evaluate the files submitted by the Supervised Entity, which entails a series of consistency verifications to ensure compliance. Several **technical** and **business validation rules** will be applied as described in section 3.3. below.

Important: All reports submitted through S3 can also be completed or corrected via the eDesk platform and vice-versa.

3.3CSSF feedback file

It is up to the submitting entity to monitor transmission correctness.

A feedback file in JSON format is systematically generated for each file submitted to the CSSF via the S3 protocol and is made available in the "feedback" folder of the Supervised Entity. This "feedback" folder is automatically created after an initial transmission of file to the CSSF.

The JSON schemas for the feedback file are available here:

- CSSF 24/847 Incident Reports: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/mictir-feedback-jsonschema-v1_0_0
- DORA - Major Incident Reports: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/dictir-feedback-jsonschema-v1_0_0
- DORA – Significant Cyber Threat Report: https://edesk.apps.cssf.lu/edesk-dashboard/docs/epi/jsonschema/v1_0_0/ctr-feedback-jsonschema-v1_0_0

The Supervised Entity shall ensure that a feedback file has been received for the last file sent to the CSSF before submitting a new file.

Note that feedback generation could take some time. If the Supervised Entity does not receive a response within one working day, please contact our dedicated technical support team at edesk@cssf.lu.

3.3.1 Naming convention

The naming convention for the CSSF feedback files is specified below:

FDBMICTIR-(SourceFileName)-IR-XXX.json for CSSF 24/847 Incident Reports

FDBDICTIR-(SourceFileName)-DIR-XXX.json for DORA – Major Incident Reports

FDBCTR-(SourceFileName)-CT-XXX.json for DORA – Significant Cyber Threat Reports

Code	Meaning	Structure	Authorised value
TYPE	Reporting type	Char(N)	**'FDBMICTIR' for CSSF 24/847 Incident Reports** **'FDBDICTIR' for DORA – Major Incident Reports** **'FDBCTR' for DORA – Significant Cyber Threat Reports**
-	Separator	Char(1)	'**-**' (constant)
SourceFileName	Name of file received from the Supervised Entity	Char(N)	**Submitted file name** - Refer to the json File naming convention
-	Separator	Char(1)	'**-**' (constant)
TrackingCode	Reference of the incident notification created in the CSSF system	Char(N)	**IR-xxx for CSSF 24/847 Incident Reports** **DIR-xxx for DORA – Major Incident Reports** **CT-xxx for DORA – Significant Cyber Threat Reports**
.json	Extension	Char(5)	**.json** (constant)

3.3.2 CSSF Feedback file content

A feedback file contains several information about the report identification:

- The unique tracking code assigned to the submitted report;
- The report reception date (in UTC);

And the following information about the report:

- The status of the S3 submission ("**Rejected**" if report is rejected, otherwise "**Accepted**");
- The status of each section of the notification (i.e. Initial, Detail and FollowUp and Initial, Intermediate and Final);

- The potential list of errors which have been raised during the application of the validation rules, and their respective description.

3.3.2.1 Technical validation

3.3.2.1.1 “Rejected” Status

When at least one of the technical validation rules has not been met, the “status” is “Rejected”.

Explicit error messages are provided within the feedback file under “rules” and then “description”.

Note that even though a CSSF file reference (i.e. Tracking code) is assigned to the rejected notification, it is not considered as being correctly submitted to the CSSF. **A rejected notification cannot be updated, the Supervised Entity shall correct the file and upload it again.** In such case, a new CSSF file reference will be assigned to the new submission.

Example:

```
{
  "header" : {
    "schemaVersion" : "1.0.0",
    "trackingCode" : "IR-001",
    "receptionDate" : "2024-02-01T14:29:07.887184Z"
  },
  "payload" : {
    "status" : "REJECTED",
    "initialInfoStatus" : "REJECTED",
    "detailStatus" : "REJECTED",
    "followUpStatus" : "REJECTED",
    "rules" : [ {
      "code" : "IR001",
      "description" : "The file name does not respect the expected naming
convention."
    } ]
  }
```

3.3.2.1.1 “Accepted” Status

When no technical error is identified, the “status” in the feedback file is “**Accepted**”. The file has been successfully transmitted to the CSSF and the business validation rules are applied to the file, as detailed in the following section.

3.3.2.2 Business validation

Following the technical acceptance of the file, several business validation rules are applied.

3.3.2.2.1 "Draft" status

Incorrect business content can be identified and listed in the feedback file. These are blocking errors preventing the correct submission to the CSSF.

In such case, the status "**Draft**" is reported in the feedback file either under:

- "initialInfoStatus", "detailStatus" or "followUpStatus" for CSSF 24/847 Incident Reports.
- "initialNotification", "intermediateReport" or "finalReport" for DORA – Major Incident Notification.

The concerned section[2] of the notification remains in status "**Draft**" in eDesk and is **not yet visible by the CSSF**. It is the responsibility of the Supervised Entity to correct the content of the form and resubmit it to the CSSF.

Example:

```
{
  "header" : {
    "schemaVersion" : "1.0.0",
    "trackingCode" : "IR-002",
    "receptionDate" : "2024-02-01T15:39:04.131723Z"
  },
  "payload" : {
    "status" : "ACCEPTED",
    "initialInfoStatus" : "DRAFT",
    "detailStatus" : "DRAFT",
    "followUpStatus" : "DRAFT",
    "rules" : [ {
      "code" : "IR035",
      "description" : "Field DetectorOther is not allowed"
    }, {
      "code" : "IR023",
      "description" : "Part 1 \"Initial information\" must be submitted prior
submitting the Part 2 \"Incident cause, classification and impact\""
    }, {
      "code" : "IR027",
      "description" : "Part 2 \"Incident cause, classification and impact\" must
be submitted prior submitting the Part 3 \"Root cause, follow up and additional
information\""
    } ]
  }
}
```

[2] For CSSF 24/847 Incident Reports, "**initialInfo**" corresponds to the Initial notification ("Initial information" in eDesk); "**detail**" corresponds to the Intermediate notification ("Incident cause, classification and impact" in eDesk); and "**followUp**" corresponds to the Final notification ("Root cause, follow up and additional information" in eDesk)
For DORA – Major Incident Reports: "**initialNotification**" corresponds to the Initial notification in eDesk; "**intermediateReport**" corresponds to the Intermediate report in eDesk; and "**finalReport**" corresponds to the Final report in eDesk)

3.3.2.2.1 “Submitted” status

The notification is correctly submitted to the CSSF when neither technical nor business rules are raised. In such case, the status “Submitted” is indicated in the feedback file for the concerned section of the notification that has been submitted to the CSSF.

Note that although sections can be submitted together via S3, they are treated independently by the system. This means that, the “InitialInfo” (or “initialNotification”) section might be correct and “Submitted”, while the second section “Detail” (or “intermediateReport”) still contains errors and stays in “Draft” status.

Examples:

```
{
  "header" : {
    "schemaVersion" : "1.0.0",
    "trackingCode" : "IR-003",
    "receptionDate" : "2024-02-01T18:02:31.211643Z"
  },
  "payload" : {
    "status" : "ACCEPTED",
    "initialInfoStatus" : "SUBMITTED",
    "detailStatus" : "SUBMITTED",
    "followUpStatus" : "SUBMITTED",
    "rules" : [ ]
  }
}
```

```
{
  "header" : {
    "schemaVersion" : "1.0.0",
    "trackingCode" : "IR-004",
    "receptionDate" : "2024-01-25T14:55:56.076212Z"
  },
  "payload" : {
    "status" : "ACCEPTED",
    "initialInfoStatus" : "SUBMITTED",
    "detailStatus" : "SUBMITTED",
    "followUpStatus" : "DRAFT",
    "rules" : [ {
      "code" : "IR028",
      "description" : "Fill in the mandatory information Additional information"
    }, {
      "code" : "IR029",
      "description" : "Fill in the mandatory information Root cause identified"
    } ]
  }
}
```