Commission de Surveillance du Secteur Financier

User Guide for XBRL reports – Bank prudential reporting

Version 1.0

User Guide for XBRL reports – Bank prudential reporting

Version 1.0

TABLE OF CONTENTS

1. Glossary & objectives

1.1. Glossary

Notion	Definition
S3	S3 – or "simple storage service" – is the object storage protocol (through a web service interface) used by the CSSF for the file exchange. In this context, S3 simply refers to the protocol for managing object storage and does not rely on any services provided by commercial cloud providers.
Bucket	A bucket is a container for objects. S3 stores data as objects within buckets. An object is a file and any metadata that describes the file. Each entity manages its own separate buckets to be used for each report type.
IT Expert	The "IT Expert" is in charge of collecting the S3 credentials. This role, as any other eDesk specific role, is granted by the "Advanced User" from the entity.
Bank prudential reporting	recurring prudential banking reporting modules defined by the EBA
Bank Prudential Reporting Responsible	The "Bank Prudential Reporting Responsible" is in charge of managing the contact list dedicated the EBA ITS reports communication.

1.2. Objectives of this document

This document is a guide that explains to the concerned entities how the bank prudential reporting modules must be technically reported to the CSSF.

The information detailed herein relates to:

- Technical overview of the reporting system
- Data and file format of the reports
- Data validation and feedbacks

2. Context and reporting principles

2.1. Context

This user guide relates to the EBA reporting framework applicable to all credit institutions established in Luxembourg, to Luxembourg branches of EU credit institutions and to Luxembourg branches of third country credit institutions.

It covers monthly, quarterly and annual reporting modules stemming from EBA ITS (Implementing Technical Standards)[1] or EBA Guidelines[2].

The document specifies requirements for concerned credit institutions to provide their XBRL reports to the CSSF at defined reference periods.

The remittance timeframes for first submissions will be updated as reporting modules are gradually migrated from historical submission channels to the new direct submission method.

2.2. Reporting and reference dates

Reporting type	Frequency	Submission type	Reference date	Remittance timeframe for first submission via eDesk/S3
ALM, LCRDA	Monthly	Corrective data	All reference periods within the previous 3 years	At any time from the 1st September 2024
ALM, LCRDA	Monthly	Initial version	As of 2024-08,	At any time from the 1st September 2024
IRRBB	Quarterly	Initial version	As of 2024-09	At any time from the 1st October
IRRBB	Quarterly	Corrective data	As of 2024-09	At any time from the 1st October
COREP, LAREX, LEVER, NSFR, FINREP, AE, FRTB	Quarterly	Corrective data	All reference periods within the	TBC

[1] COMMISSION IMPLEMENTING REGULATION (EU) 2021/451 as amended, COMMISSION IMPLEMENTING REGULATION (EU) 2021/453 as amended

[2] All EBA guidelines in relation with the supervisory reporting

			previous 3 years	
COREP, LAREX, LEVER, NSFR, FINREP, AE, FRTB	Quarterly	Initial version	TBC	TBC

3. Reporting - technical specifications

3.1. Means of communication

XBRL report submission

The entities in scope of the EBA reporting framework may submit the XBRL report through the following means:

- A solution based on the submission of a structured file through S3 ("simple storage service") protocol;
- An online solution through dedicated eDesk procedures.

XBRL report review – WARNING explanations

Once the XBRL report is submitted, the entities shall review the results and make sure of a proper validation. The entities must provide explanations regarding any remaining WARNINGs.

Bank prudential reporting mailing list

The entities shall maintain their mailing contact lists for the bank prudential reporting. For more information on different roles please refer to section 3.6.

3.2. Standard requirements

3.2.1. eDesk prerequisites

Regardless of the means of communication used for the reporting submission, an eDesk[3] enrolment process is required. Therefore, unless you already have an eDesk user account, we invite you to enrol.

[3] Link to eDesk platform: https://edesk.apps.cssf.lu/

Context information	Necessary actions
• To set up their account, every eDesk user needs a valid LuxTrust certificate for identification and authentication purposes. The certificate can either be private or professional. Any LuxTrust product (token, smartcard, app…) can be used.	1. Ensure to have a **LuxTrust certificate**. If necessary, information on how to order a LuxTrust certificate can be found in chapter 2 of the *eDesk Authentication User Guide*[4]. 2. Go to the eDesk homepage, click on "Log in" in the upper right corner, then, click on "Log in with LuxTrust" and **create your eDesk account.** Further information can be found in chapter 4.1 of the *eDesk Authentication User Guide*.
• Once a user account is created, it has to be linked to the entity/entities the user is working for.	3. Once you have created your eDesk account, start a "**New entity link request**" as explained in chapter 4.2.2 of the *eDesk Authentication User Guide*. Even if you would like to apply to become advanced user, you have to start a "new entity link request" first.
• The "New entity link requests" are treated (accepted or rejected) by an advanced user of your company. • Therefore, each entity using eDesk needs (at least) one advanced user. To become an advanced user, the candidate has to send a "New advanced user request" including a mandate and some accompanying documents to the CSSF via the eDesk Portal. The request will be accepted (or rejected) after verification performed by the CSSF.	4. If your firm has not yet an advanced user or if the firm wants to set-up additional advanced user roles, it should designate (at least) one and the latter should start a **"New advanced** user **request"**. The exact application procedure is described in chapter 4.2.3 of the *eDesk Authentication User Guide*. 5. The advanced user has to **approve** (or reject) **the "new entity link requests"** as explained in chapter 4.3 of the *eDesk Authentication User Guide.*

All key information on the eDesk authentication is available in the **eDesk Authentication User Guide** on the eDesk homepage.

[4] On the eDesk Portal homepage, the eDesk Authentication User Guide (pdf file) is a guide that describes how to configure authentication and that can be found in the "Getting started" menu.

3.2.2. Reporting file

3.2.2.1. Technical format

The professional in the scope of the EBA reporting framework applicable to credit institutions must report the reporting modules according to the taxonomy version (Data Point Model) that applies.

The professional shall report the initial version of the reports according to the submission deadline and provide with any corrective version of the report when required. The CSSF allows corrective data for the previous 3 years. (i.e. in September 2024, the professional may submit corrective report back to the reference period of 09-2021).

Any corrective report should be reported according to the taxonomy version (Data Point Model) that applies for the reference period.

The following tables summarize the expected taxonomy versions and the corresponding periods :

Module	Taxonomy version	Start date	End date
ALM	3.0.0	2021-06	2023-05
ALM	3.2.0	2023-06	entry in force of framework 4.0
LCRDA	3.0.0	2021-06	2022-11
LCRDA	3.2.0	2022-12	entry in force of framework 4.0
IRRBB	3.4.0	2024-09	TBC

In addition, all XBRL instances to be sent to the CSSF have to be fully compliant with the XBRL guidelines defined by the EBA.

Reporting file must be transmitted via a compressed .zip format containing one single .xbrl file.

As described in section below, the submitted file names should comply with the mandatory file naming convention for .zip file and .xbrl file.

3.2.2.2. Naming convention

The mandatory file naming convention for .zip files is specified below.

For reports submitted through the eDesk channel, the naming convention is the following:

Format: TYPE-ENNNNNNNN-YYYY-MM-SUBTYPE-A-R.ext

Code	Meaning	Authorised value
TYPE	Reporting type	CFEREP’ (constant)
-	Separator	‘-’ (constant)
E	Reporting entity	‘B’
NNNNNNNN	Identification number	00000001…99999999 (CSSF code of the entity)
-	Separator	‘-’ (constant)
YYYY-MM	Reference period end date	Date in the specified format
-	Separator	‘-’ (constant)
SUBTYPE	*Reporting type	Monthly modules: - ALMXXX - LCRDAX Quarterly modules: - AEXXXX - COREPX - FINREP - FRTBXX - IRRBBX - LAREXX - LEVERX - NSFRXX
-	Separator	‘-’ (constant)
Accounting version	Accounting version	C', 'N', 'L' or ‘S’
-	Separator	‘-’ (constant)
Report version	**Report version**	‘D’, N (constant)
.ext	Extension	.zip (constant)

The same naming convention will apply for the XBRL report included in the zip file, but with .xbrl as extension: TYPE-ENNNNNNNN-YYYY-MM-SUBTYPE-AV-RV.xbrl

Examples:

.ZIP	XBRL
CFEREP-B00000999-2024-08-ALMXXX-N-N.zip	CFEREP-B00000999-2024-08-ALMXXX-N-N**.xbrl**
CFEREP-B00000999-2024-08-LCRDAX-N-N.zip	CFEREP-B00000999-2024-08-LCRDAX-N-N**.xbrl**

For report submitted through S3, the zip file and the XBRL file should be suffixed with an UUID as followed:

Format: TYPE-ENNNNNNNN-YYYY-MM-SUBTYPE-A-R**_UUid** .ext

Code	Meaning	Authorised value
	TYPE-ENNNNNNNN-YYYY-MM-SUBTYPE-A-R	
_	Separator	'_' (constant)
UUID	Reporting unique identifier	Unique identifier following the RFC4122 norm
.ext	Extension	.zip (constant)

Examples:

.ZIP	XBRL
CFEREP-B00000999-2024-08-ALMXXX-N-N**_a6fca981-2f2c-2a98-ddba-b241c2366a1a.zip**	CFEREP-B00000999-2024-08-ALMXXX-N-N**_a6fca981-2f2c-2a98-ddba-b241c2366a1a.xbrl**
CFEREP-B00000999-2024-08-LCRDAX-N-N**_a6fca981-2f2c-2a98-ddba-b241c2366a1a.zip**	CFEREP-B00000999-2024-08-LCRDAX-N-N**_a6fca981-2f2c-2a98-ddba-b241c2366a1a.xbrl**

Please note that a file cannot be uploaded twice with the same UUID as file name.

3.2.2.3. Formal verification rules

The CSSF will check the submitted ZIP file which entails formal verifications in order to ensure its compliance. This will be done whatever the channel used to submit the files.

An indicative table of the rules to which a notification file may be subject is available in "Annex 1 – Formal verification rules" (in section 6). This does apply to all XBRL reports submitted through eDesk and through S3.

The following controls are made:

- Technical controls (nomenclature check, entity in-scope, reporting period, …);
- EBA Taxonomy controls (validation rules and other taxonomy checks referring to the applicable framework);

- EBA Filing rules controls (referring to the EBA document : [EBA Filing Rules 5.3]
- The errors and warnings will be displayed either when uploading the report or into the detail's pages.

  When submitting the reporting via S3, the feedback will contain all the warnings and errors related to technical and XBRL validation performed by the CSSF detected as well as the status of the report.

  The entity is responsible to provide an ACCEPTED report (ACCEPTED feedback).

  When errors (either technical or functional XBRL) are triggered, the report is in REJECTED status and a correction is expected.

  If the remaining errors are warnings only, the report is still in REJECTED status. The entity shall provide a valid explanation or amend its submission to solve the remaining warnings. Please refer to the chapter 3.5 that provides with all information on how to justify through the eDesk dashboard.

  Where explanations have been provided, the CSSF may:

  - Accept the report.
    - The feedback status will then change into ACCEPTED;
    - If the report has been submitted through the S3 channel, a new FEEDBACK with the status ACCEPTED will then be sent to the entity.
  - Not accept and ask the entity to provide with a corrective report.

3.2.2.4. Transmission to the ECB

Once the report has been processed by the CSSF and no technical error has been encountered, for the entities covered by the ECB decision on the provision to the ECB of supervisory data reported to the NCAs by the supervised entities, the report will be automatically forwarded to the ECB. The ECB will revert with their XBRL validation and errors. The ECB validation status as well as the list of errors or warnings if any will be then displayed into the eDesk portal in the report details section.

A global CSSF and ECB acceptance status, that depends on the triggering of validation rules at CSSF and ECB levels, will also be displayed into the eDesk portal. Only files with an "accepted" CSSF acceptance status and an "accepted" ECB acceptance status will be associated with an "accepted" global CSSF and ECB acceptance status.

CSSF technical validation	CSSF Acceptance status	ECB acceptance status	Global CSSF & ECB Acceptance status
Failed	**N/A**	**N/A**	**N/A**
OK	**Not-Accepted (with errors)**	**Accepted**	**Not-Accepted**
OK	**Not-Accepted (with errors)**	**Not-Accepted (warnings)**	**Not-Accepted**
OK	**Not-Accepted (with errors)**	**Not-Accepted (errors)**	**Not-Accepted**
OK	**Not-Accepted (with errors)**	**Rejected**	**Rejected**
OK	**Not-Accepted (warnings only)**	**Accepted**	**Not-Accepted**
OK	**Not-Accepted (warnings only)**	**Not-Accepted (warnings)**	**Not-Accepted**

OK	**Not-Accepted (warnings only)**	**Not-Accepted (errors)**	**Not-Accepted**
OK	**Not-Accepted (warnings only)**	**Rejected**	**Rejected**
OK	**Accepted**	**Accepted**	**Accepted**
OK	**Accepted**	**Not-Accepted**	**Not-Accepted**
OK	**Accepted**	**Not-Accepted**	**Not-Accepted**
OK	**Accepted**	**Rejected**	**Rejected**

3.3. eDesk online solution

The access is made through a secured connection module after being authenticated with a Luxtrust certificate.

The prerequisites enabling connection to eDesk (activation of an entity link, validation of the roles by an advanced user, etc.) are detailed in the "Authentication and user account management" user guide on the eDesk portal home page (https://edesk.apps.cssf.lu/edesk-dashboard/dashboard/).

3.3.1. Follow-up dashboard

For all modules and reports described in this user guide, a common dashboard lists all reports created and sent:

- Either through the eDesk channel by a user linked to the entity of the authentified user;
- Or through the S3 system.

It is possible to get the validation details of any report via the eDesk dashboard.

Report dashboard

The reports are displayed by module, reference period, accounting version, and whether it is definitive or not definitive version. Any corrective report submitted following the initial submission is considered as a new version of the report.

The dashboard lists all the reports submitted either by eDesk or S3. The status provides the result of the formal validation of the last version submitted.

The action button allows the entity to access the details of the submissions (all subsequent versions submitted) and for each version, the validation result (e.g. list of ERROR(s) and/or WARNING(s) if any).

The 'Warning only' column indicates whether the validation result does only contain WARNING(S).

Orphan submission

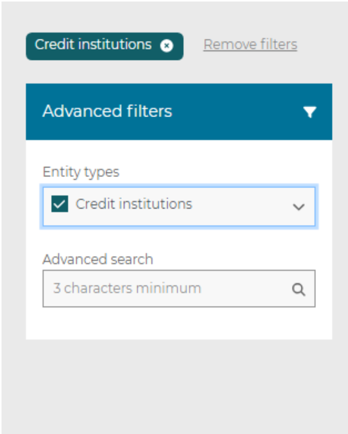
In case of technical rejection (i.e., submission via S3 with a naming convention that does not comply with the requirements), the CSSF might not be able to link the report submitted to the expected report (entity code, reference, accounting version, and whether it is definitive or not definitive version).

All orphan submissions are listed in a dedicated dashboard. The entity may consult the reason of rejection.

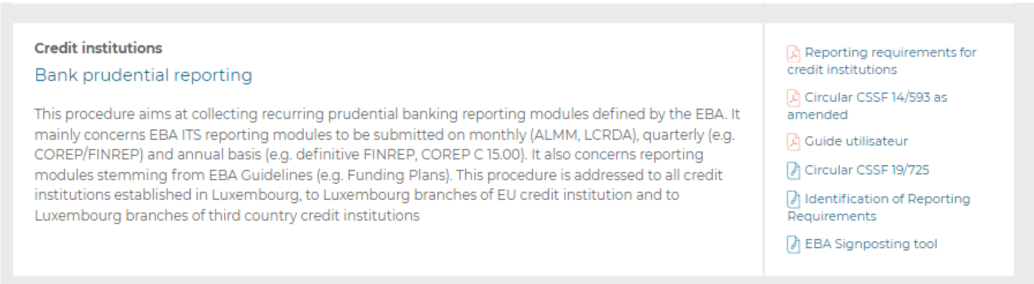
3.3.2. Creation and submission of a report

3.3.2.1. Access the report dashboard

a - In the list of procedures, select your entity type

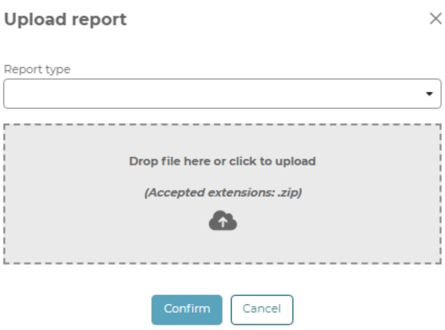


b- Select the correct reporting type



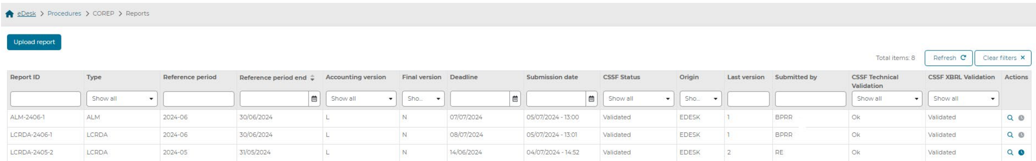
3.3.2.2. Upload a report

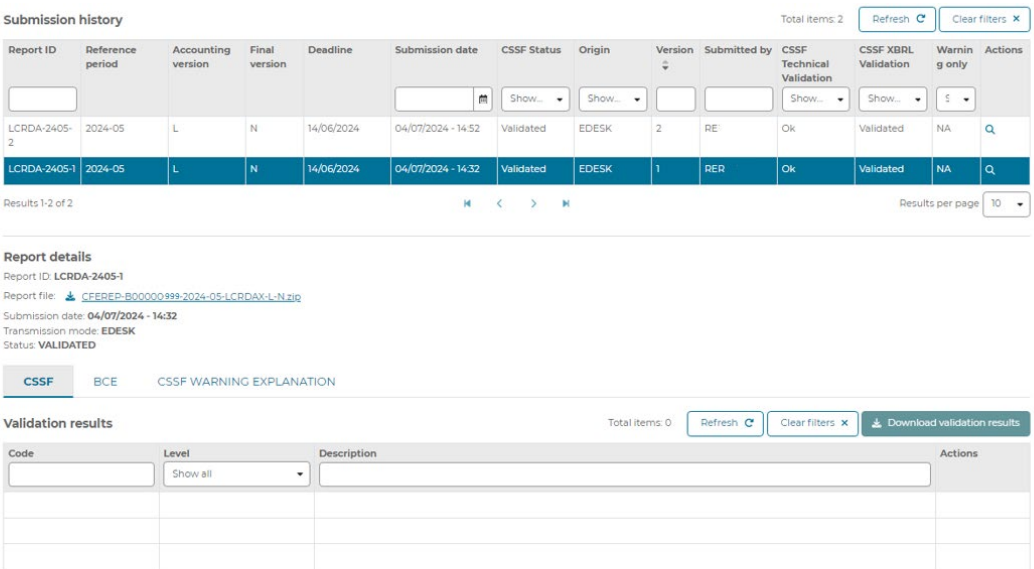
The upload of XBRL report is possible via the "Upload report" button available on the dashboard homepage of the dedicated procedure and after choosing the report type.



Please note that for each data collection exercise, the entity may submit several XBRL reports if required to correct some data already provided, for example.

For each valid submission, the report will be considered as a new version of the previous one. The professional may consult the previous version by accessing the reports details.





As mentioned in section 3.2.2.2, the submitted file names should comply with the mandatory file naming convention for .zip file and .xbrl file.

Reporting file must be transmitted via a compressed .zip format containing one single .xbrl file.

Following controls are performed on the uploaded file:

- Technical control (nomenclature check, file validity…);
- EBA Taxonomy control (validation rules and other taxonomy checks);
- EBA Filing rules control.

Firstly, technical checks are performed on the filename and the file itself. In case an error is raised, the report cannot be uploaded.

Once those checks are successfully passed, a report is created and the XBRL report is automatically analysed by the system.

Secondly, once the XBRL analysis is performed:

- Either at least one error is raised. In this case, the report gets the status "NOT-ACCEPTED" and the "Warning only" column is set up to "NO": a new corrected report must be submitted by the entity.
- Or only warnings are raised. In this case, the report gets the status " NOT-ACCEPTED" and the Warning only" is set up to "YES": no error has been detected in the report, however all warnings must be explained to the CSSF by the reporting entity (Please refer to the chapter 3.5 that provides with all information on how to justify through the eDesk dashboard).
- Or no warning/error is raised. In this case, the report gets the status "ACCEPTED" and the column "Warning only" is set up to "NA". The report will be reviewed by the CSSF.

For the report with warnings only, the CSSF will analyse the explanations provided by the entity and may:

- either validate the report based on the information provided: the report gets the status "ACCEPTED" and no further action is expected on the entity side);
- or reject the report (the report status does not change and remains " NOT-ACCEPTED", a new corrected report must be submitted by the entity).

3.4. S3 system submission

3.4.1.1. About the S3[5] solution

S3 ("simple storage service") solution is the object storage 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. An object is a file and any metadata that describes the file. A bucket is a container for objects. An entity will be linked to one bucket divided into two folders:

- *"submission"*: for the reporting files;
- *"feedback"*: for the feedback files.

Please refer to the S3 User Guide "Methods of transmitting reports via S3 Application Programming Interface - Technical guidance - Version 1.0" available here:

https://www.cssf.lu/en/methods-of-transmitting-reports-via-api/

[5] Note that S3 simply refers to the protocol for managing object storage and not to any service provided by commercial cloud providers.

3.4.2. Reporting submission

The ZIP file MUST be uploaded to the "submission" folder in S3. No upload is allowed into other folders (e.g., "feedback" folder is only dedicated to CSSF feedbacks).

Reporting file must be transmitted via a compressed .zip format containing one single .xbrl file.

The responsibility of the bucket is to grant access to our system. It is not intended for long term storage. Regular cleaning might be performed by the CSSF.

Please refer to the section 3.2.2.1 for more detail about the naming convention.

As mentioned, please note that a file cannot be uploaded twice with the same UUID as file name.

As mentioned, each submission will create a new report. Those reports are available for consultation in the dashboard.

3.4.3. CSSF feedback file

It is up to the submitter to monitor transmission correctness.

A feedback file in JSON format is systematically generated for each file transmitted via S3 system and made available in the "feedback" folder.

An entity must ensure that it has correctly received a feedback file for the last file sent, before submitting a new file. Feedback generation could take some time. In case of not receiving any feedback within a working day, please contact our dedicated support team (edesk@cssf.lu).

3.4.3.1. Naming convention

The naming convention for the feedback is the following one:

Code	Meaning	Authorised value
File Name : TYPE-ENNNNNNNN-YYYY-MM-SUBTYPE-A-R_UUID.zip		
_	Separator	'_' (constant)
FEEDBACK	FEEDBACK	'FEEDBACK' (constant)
.ext	Extension	.json (constant)

<u>Example</u>

Report file name	FEEDBACK file name
CFEREP-B00000999-2024-08-ALMXXX-N-N_**a6fca981-2f2c-2a98-ddba-b241c2366a1a.zip**	CFEREP-B00000999-2024-08-ALMXXX-N-N_**a6fca981-2f2c-2a98-ddba-b241c2366a1a.zip_FEEDBACK.json**

3.4.3.2. File content

Beside the header, a feedback file contains some information about the report:

- The status of the S3 submission ("Rejected" if report status is "Rejected", otherwise "accepted");
- The processed file Name;
- The list of errors and/or warnings which have been raised during the analysis performed by the system;

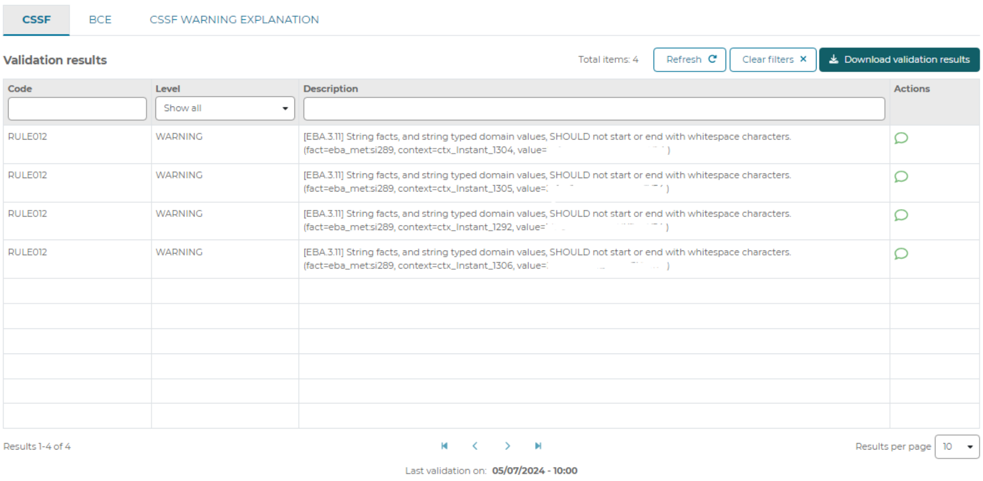
The list of errors and/or warnings contains the results of the validation against the formal verification rules as mentioned in section 3.2.2.2.

It is the responsibility of the entity to monitor the feedback reception and bring accurate corrections in case of REJECTED feedback.

3.5. Warning explanations through eDesk

The entities must explain all remaining WARNINGs in the last submission. This can be done through the detail's dashboard in eDesk, "CSSF" sheet.

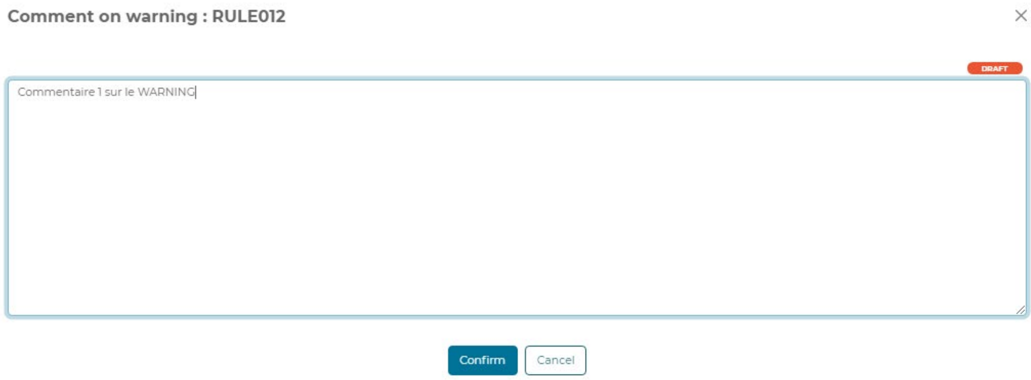
1) Access the XBRL validation results

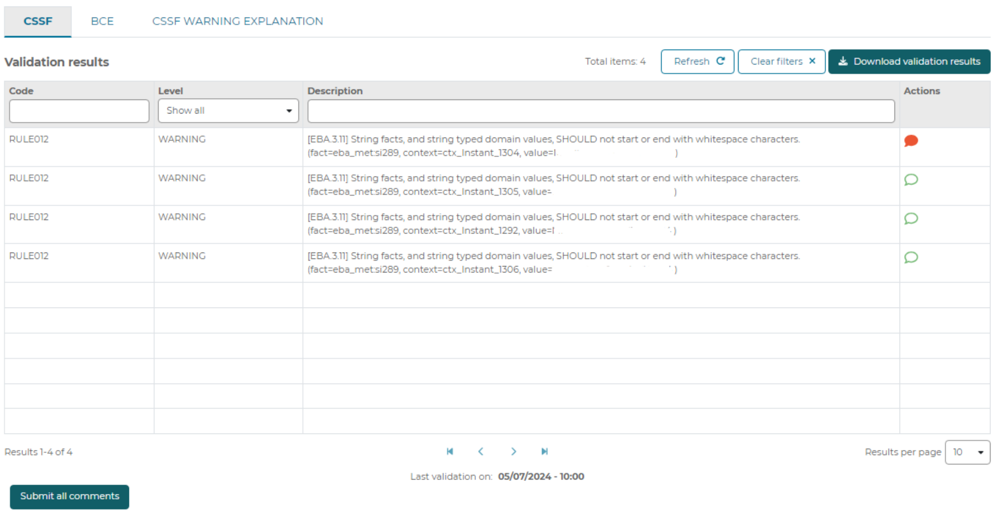


2) Draft the explanation

When clicking on the comment action, a pop up enables the entity to draft a comment.

The action column enables the entity to draft the comment.

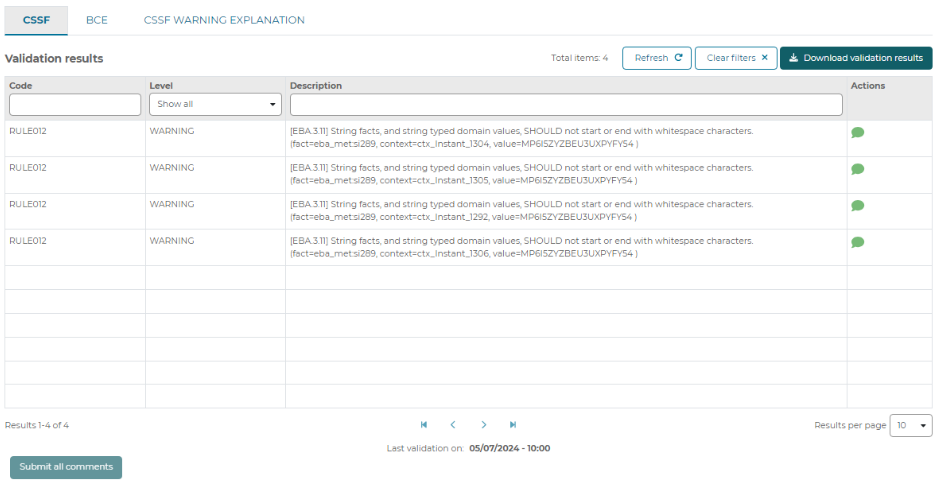




Each warning must be explained.

3) Submit the explanations

The entities must then submit all the explanations to the CSSF via the “Submit all comments” action.



Comment icon signification

No comment has been drafted.

A comment has been drafted and is not yet submitted to the CSSF.

The comment has been submitted to the CSSF.

More details are available in the "CSSF WARNING EXPLICATION" sheet.

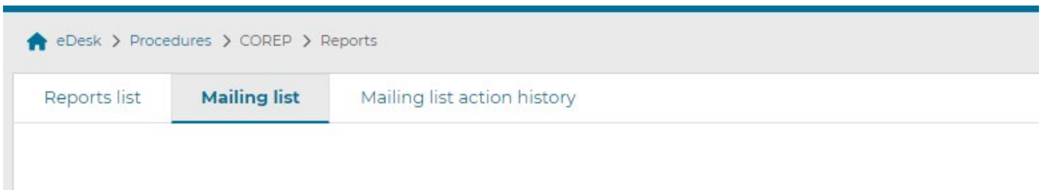
3.6. Reminder notifications

3.6.1. Management of the mailing list

The new role "Bank Prudential Reporting Responsible" is in charge of managing the entity contact list dedicated to the Bank prudential reporting communications.

The role will be granted by the advanced user of the entity. It can be granted to one or several users within the company.

The user with this specific role has access to the Mailing list sheet.



The user can add any registered eDesk user linked to the entity as part of the mailing contact list either as:

- « Responsible level 1 » : the person/group of persons recorded in the mailing list as "Responsible level 1" shall be in charge of the day-to-day production and/or sending of the bank prudential reporting of the entity.
- Or « Responsible level 2 » : the person/group of persons recorded in the mailing list as "Responsible level 2" shall be member of the management of the reporting entity, and as a consequence, be hierarchically above the persons recorded in the mailing list as "Responsible level 1" (escalation process).

At least one user must be added to each category.

Users can be deleted directly from the dashboard.

3.6.2. Type of reminder notifications

When the professional does not submit the expected report or submit an erroneous report (errors or un-(or mis-)explained warnings) by the applicable deadline, the following notifications will be sent:

- Reminder 1: a first reminder will be sent the day following the remittance deadline. It will be addressed to the users with the Bank Prudential Reporting Responsible role as well as to all users part of the mailing list as Responsible level 1;
- Reminder 2: if an accepted report has still not be submitted 2 days after the Reminder 1, a second reminder will be sent to the users with the Bank Prudential Reporting Responsible role, to all users part of the mailing list as Responsible level 1 as well as to all users part of the mailing list as Responsible level 2.

3.7. Reporting entities obligations

3.7.1. Data quality

Entities are strongly advised to review and validate their ZIP file and its XBRL file before any submission.

Files must be validated against the XBRL schema provided by the EBA.

3.7.2. Review the report status, correct a report and explain WARNINGs

Entities must ensure that the report status is ACCEPTED and that all potential errors are properly analysed. In addition, entities must ensure that any rejected/non-accepted reports are corrected and re-submitted.

Any remaining warnings have to be explained and all explanations submitted to the CSSF.

3.7.3. Maintaining the mailing list

The entity is entitled to maintain a proper contact list so that any reminder or notifications will be addressed within the entity.

4. Testing with CSSF

4.1. Connectivity check

A connectivity check is highly recommended before the Go-Live.

A dedicated "Echo Service" is at your disposal to ensure the good connectivity between your entity and our systems.

The "IT Expert" has to create a new access on the "Echo" bucket that is presented below in order to get the right S3 credentials.

You can upload a dummy file. If the connectivity check is completed, you will get a dummy feedback file proving it.

Please note that this service always remains available.

In case you are unable to connect to the Echo Service or that you are not receiving any feedback, please contact edesk@cssf.lu.

5. Contact information

In case of business questions, please contact reportingbanques@cssf.lu

For any technical question please contact edesk@cssf.lu.

6. Annexes

6.1. Annex I – Formal verification rules

Error Code	Explanation	Error level
RULE001	The filename is not compliant with the naming convention	ERROR
RULE002	The file is too large (max 20 MB)	ERROR
RULE003	The zip file should contain one and only one XBRL file	ERROR
RULE004	The entity linked to the logged user (BXXXX) does not match the entity provided in filename (BXXXX)	ERROR
RULE005	A file with the same name has already been received	ERROR
RULE006	The file has been rejected for security reason	ERROR
RULE008	The accounting version is not the one expected	ERROR
RULE009	You already submitted a file for this period that has not yet been processed and validated	ERROR
RULE010	Your entity is not authorised to send this type of reporting for the defined reporting period	ERROR
RULE011	XBRL error	ERROR
RULE012	XBRL warning	WARNING
CSSF_0	XBRL file is not parsable	ERROR
CSSF_1	EntryPoint is not compatible with Reporting Type and Reporting period, value found is *XXX*, expected value is: *YYY*	ERROR