

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

SERIMA SECURITY OBJECTIVES MODULE - USER GUIDE FOR OPERATORS

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

Table des matières

1. Introduction 3
2. Access the Module 4
3. Security Objectives Module – step by step 5
   3.1. Create a New Declaration 5
   3.2. Complete the Declaration 6
   3.3. Track Progress and Submit the Declaration 8
   3.4. View the Review Result and Update Your Declaration 10
4. Support 13

1. Introduction

The Security Objectives (SO) module allows operators to perform a self-assessment against the security requirements of the applicable regulatory framework.

Under the NIS 2 framework, operators use the module to assess how their organisation meets the applicable security objectives, describe the security measures they have implemented and provide supporting information.

Please note that completing and submitting a self-assessment does not result in NIS 2 certification or any equivalent form of formal approval. Instead, the assessment should be understood as a benchmarking and gap analysis tool that helps you evaluate your organisation's cybersecurity maturity in the context of the NIS 2 framework.

Its purpose is to help you identify areas for improvement, plan the necessary measures and monitor your organisation's progress over time. By completing the assessment annually, you can keep track of implemented measures, planned improvements and changes in your overall security posture.

Please note that submitting the declaration to the ILR is not mandatory if you are using the module solely for internal self-assessment, benchmarking or gap analysis purposes. **You can complete the assessment and use the results internally without submitting it.**

The NIS 2 evaluation framework contains 50 security objectives. While this may seem like a considerable amount of work at first, you do not need to start from scratch every year. The recommended approach is to complete the declaration once and then use the **Duplicate** function each year to create a new declaration based on the previous year's answers. You can then review and update the information to reflect your organisation's current situation.

This guide explains how to create, complete, submit and duplicate a Security Objectives declaration.

2. Access the Module

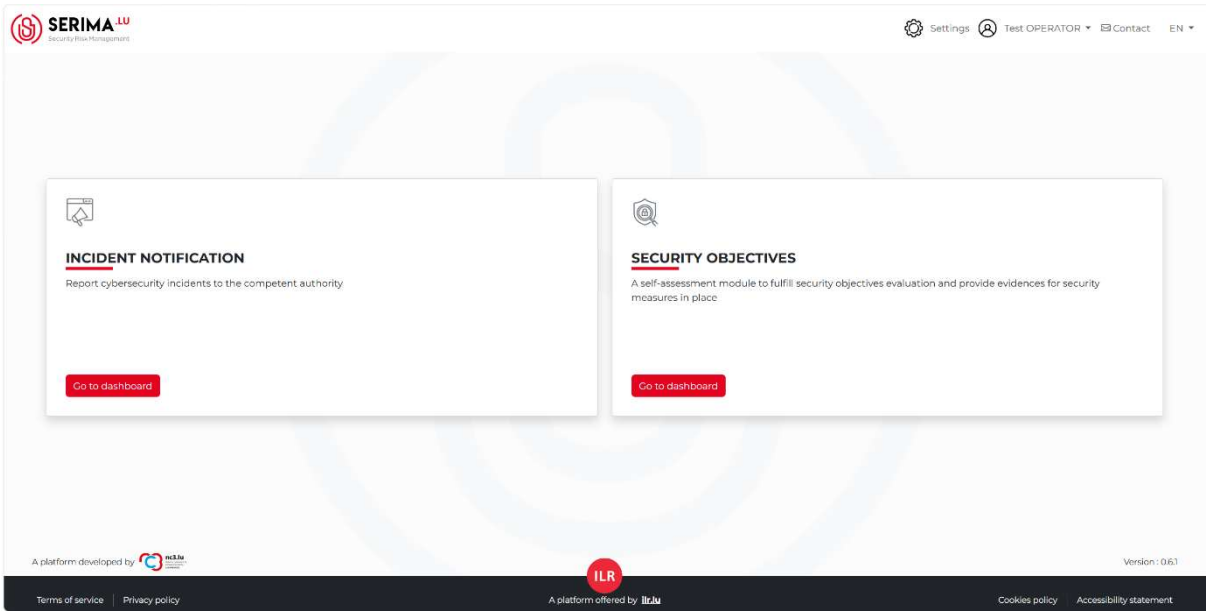
Log in to the platform using your verified and approved operator account.

If your entity already has a SERIMA instance, but your account cannot access it, please contact the administrator of your SERIMA instance to receive access.

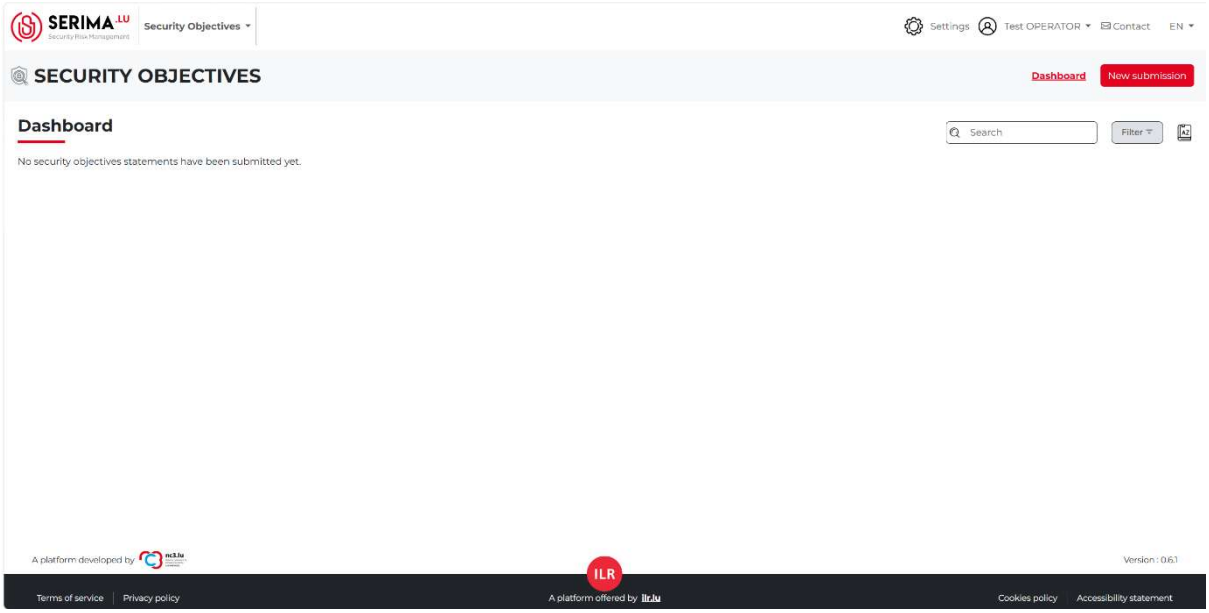
If your entity does not have a SERIMA instance yet, please contact us at serima@ilr.lu to request one.

You can open the **Security Objectives** module in one of two ways:

- Use the module selector at the top of the page, next to the SERIMA.lu logo.
- Click **Go to dashboard** on the **Security Objectives** module card on the overview page.



The dashboard provides an overview of your declarations. From here, you can create new declarations, continue working on existing ones and track their status. If you have not yet created a declaration, the dashboard will be empty.



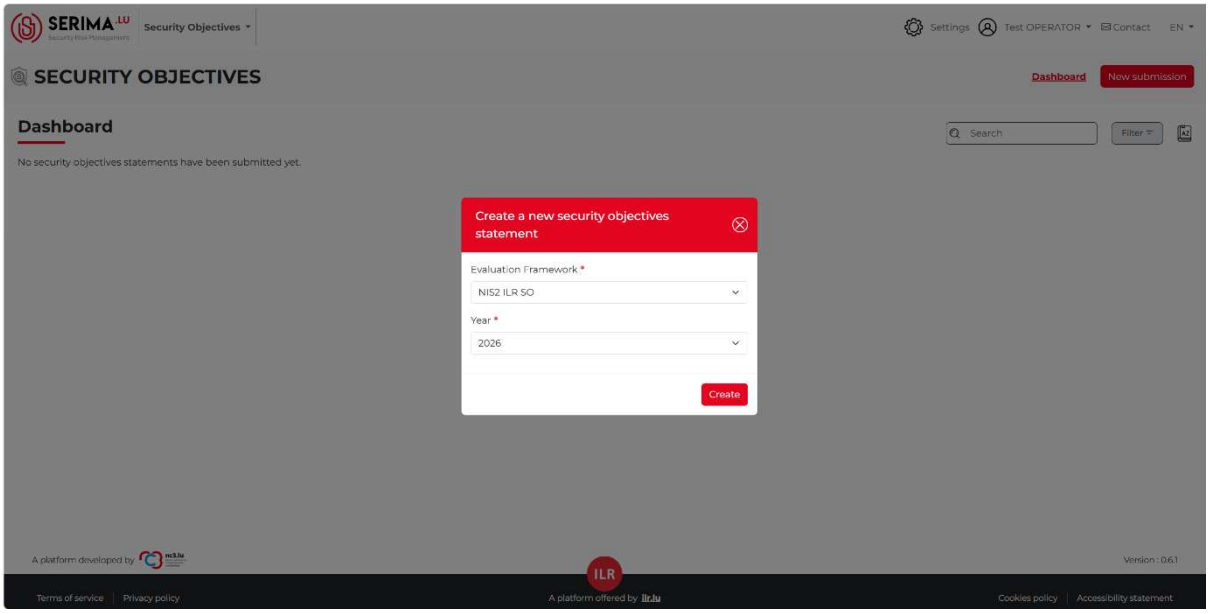
3. Security Objectives Module – step by step

3.1. Create a New Declaration

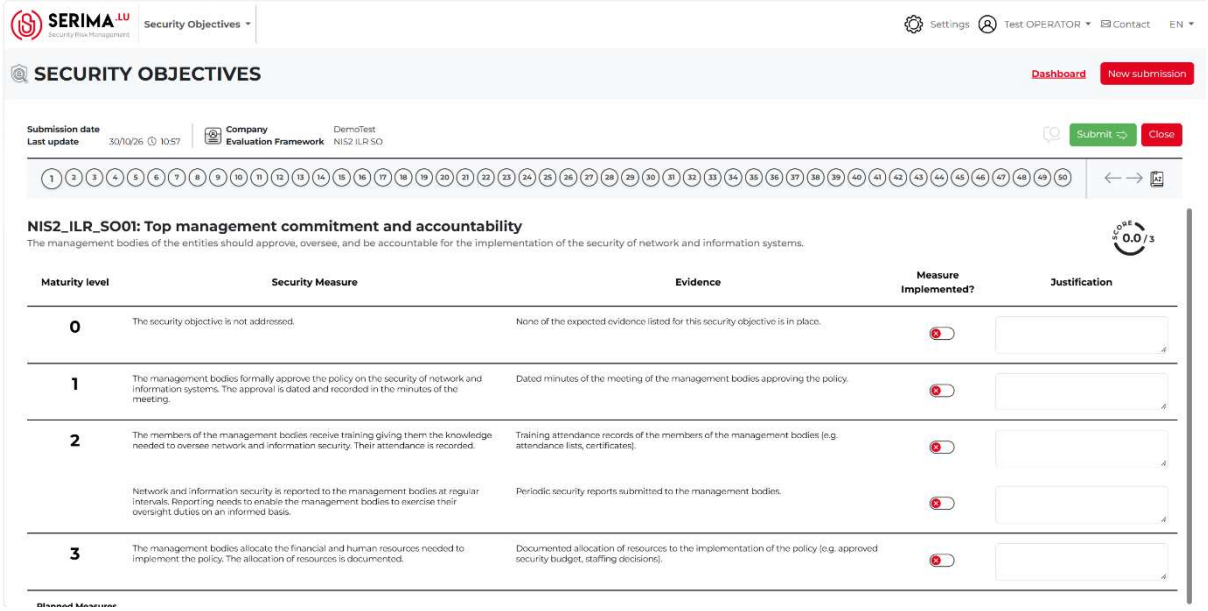
To create a new declaration, click **New submission** on the Security Objectives Dashboard.

In the **Create a new security objectives statement** pop-up:

1. Select the applicable **Evaluation Framework** (the set of security objectives against which your organisation is assessed).
2. Select the relevant **Year** of the self-assessment.
3. Click **Create**.



The newly created declaration opens automatically in the detailed view, displaying the 50 security objectives of the NIS 2 evaluation framework. Its initial status is **Unsubmitted**.



The declaration consists of several security objectives. Each objective contains a number of security measures

grouped by maturity level, ranging from the lowest to the highest level. The declaration displays one security objective at a time. Use the objective selector or the **Previous** and **Next** arrows to navigate between objectives.

Saving your work: Your answers are saved automatically as you work. There is no separate **Save** button. Changes to switches are saved immediately, while text entries are saved when you leave the field.

You can use **Close** at any time to return to the dashboard and continue working on the declaration later.

3.2. Complete the Declaration

For each objective:

Step 1 – Indicate implemented security measures

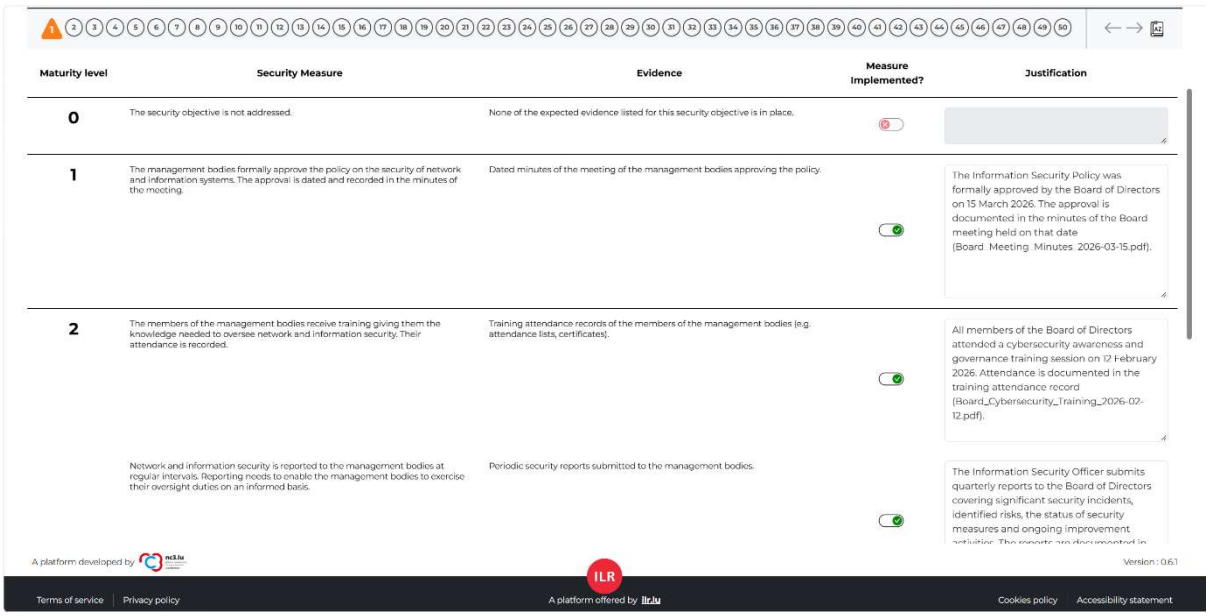
Review the security measures listed under each maturity level. Activate the **Measure Implemented?** switch for every measure already implemented in your organisation. Each selected measure contributes to the overall score for the respective security objective.

Maturity level 0 represents a situation where no security measures are in place and is mutually exclusive with higher maturity levels.

Measures at levels above 0 are not mutually exclusive. This means you can select implemented measures across different levels, even if some measures at lower levels have not yet been implemented.

Step 2 – Provide a justification

For each implemented measure, enter a justification in the Justification field explaining how the measure is implemented and identifying the supporting evidence. Providing a justification is mandatory for every implemented measure.

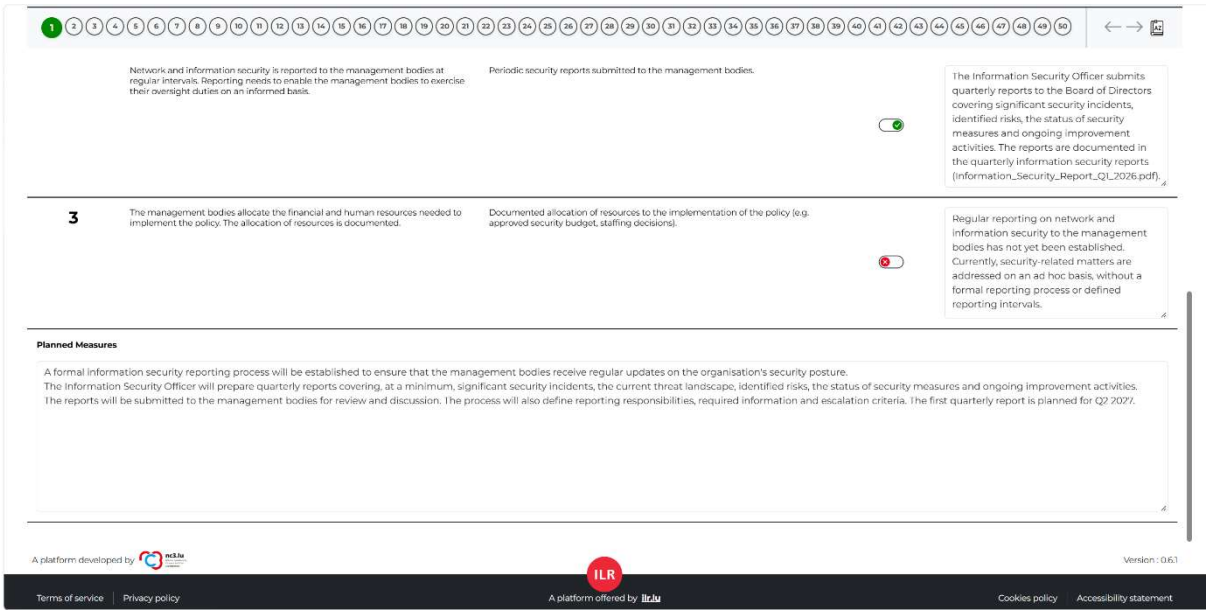


For example, if the expected evidence is a policy, specify its exact document name (e.g. *Policy.pdf*), including its publication date, author and version number, where applicable. You may also use the field to provide additional comments or explanations about how the measure has been implemented.

Make sure that the information you provide allows the ILR to uniquely identify and retrieve the referenced evidence at a later stage, for example in response to an information request, during an audit or whenever

further clarification is required. Avoid vague references that do not allow a specific document or piece of evidence to be identified.

If a measure has not been implemented, you may also use the **Justification** field to explain why. If planned actions relate to a specific security measure rather than the overall security objective, you may also describe them in the Justification field instead, provided that the measure has not yet been implemented.



Step 3 – Describe planned measures

Use the **Planned Measures** field to describe how your organisation intends to further improve its security posture in relation to the respective security objective. This field provides an overall view of your planned improvements, including the actions to be taken, the expected milestones and their anticipated timeline.

Your planning should cover the coming months and, where appropriate, the period until the next annual submission. Longer-term plans may also be included, particularly for larger projects or measures requiring more time to implement.

Providing planned measures is mandatory if not all security measures of this security objective have been out in place. For instance, if the score is lower than 3/3.

The field may only be left empty if all measures across all three maturity levels have been implemented.

Remember: The assessment is intended as an annual exercise. When creating your declaration for the following year, you can use the **Duplicate** function to carry over your previous submission, including the text entered in this field. This allows you to review your previous plans, assess the progress made and update your planned measures, implementation status and justifications accordingly.

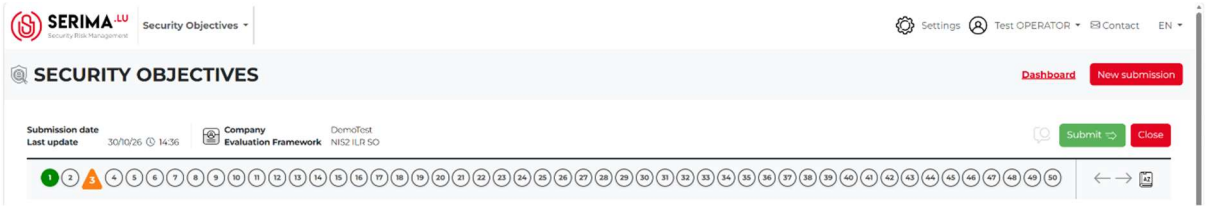
3.3. Track Progress and Submit the Declaration

Progress Tracking

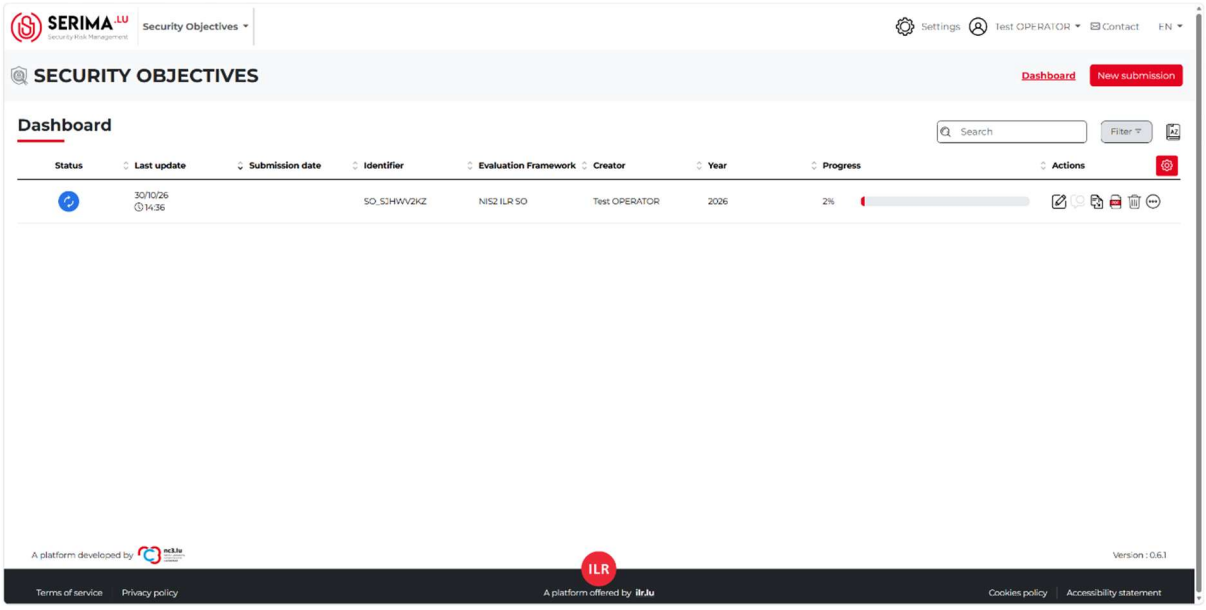
The detailed declaration view includes visual indicators in the objective selector to help you identify which objectives have been completed and which still require attention.

The objective selector uses the following indicators:

- **Grey outlined circle:** The objective has not yet been completed.
- **Orange triangle:** The objective is partially completed. Required information, such as a justification or planned measures, is still missing.
- **Green circle:** All information required for the objective has been provided.



As you complete the workflow, your work is saved automatically. You can return to the dashboard at any time by clicking **Dashboard** next to **New submission**. The dashboard displays all your declarations, including those that are still **Unsubmitted**.



The **Progress** column on the dashboard provides an overview of how much of the declaration has been completed, based on the proportion of objectives that are fully completed.

To return to the detailed declaration view and continue editing, click the pencil icon in the **Actions** column.

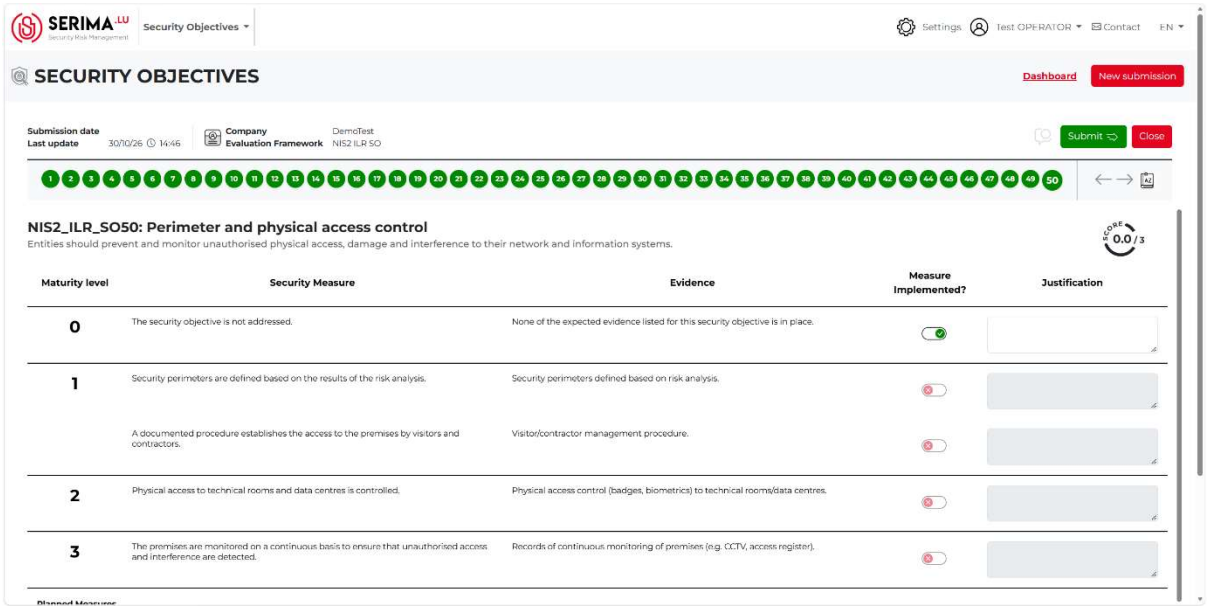
Submitting the declaration

Once all objectives are fully completed, the **Submit** button becomes available.

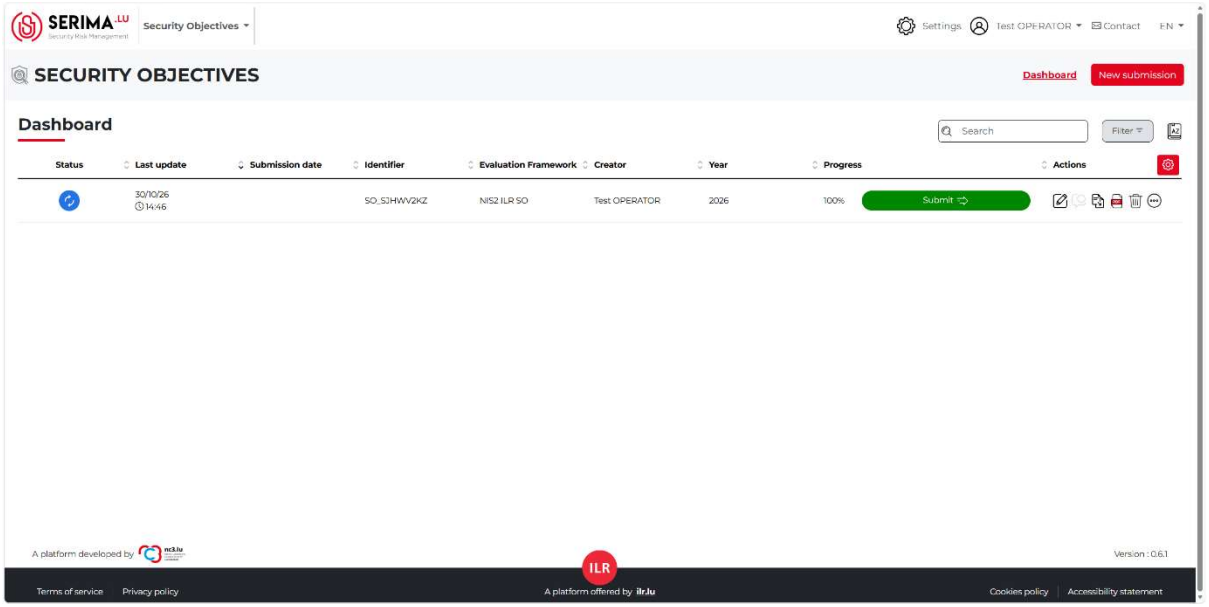
Please note: Submitting the declaration to the ILR is not mandatory if you are using the module solely for internal self-assessment, benchmarking or gap analysis purposes. You can complete the assessment and use the results internally without submitting it.

If your organisation is legally required to submit a declaration to the ILR on an annual basis, you can do so in either of two ways:

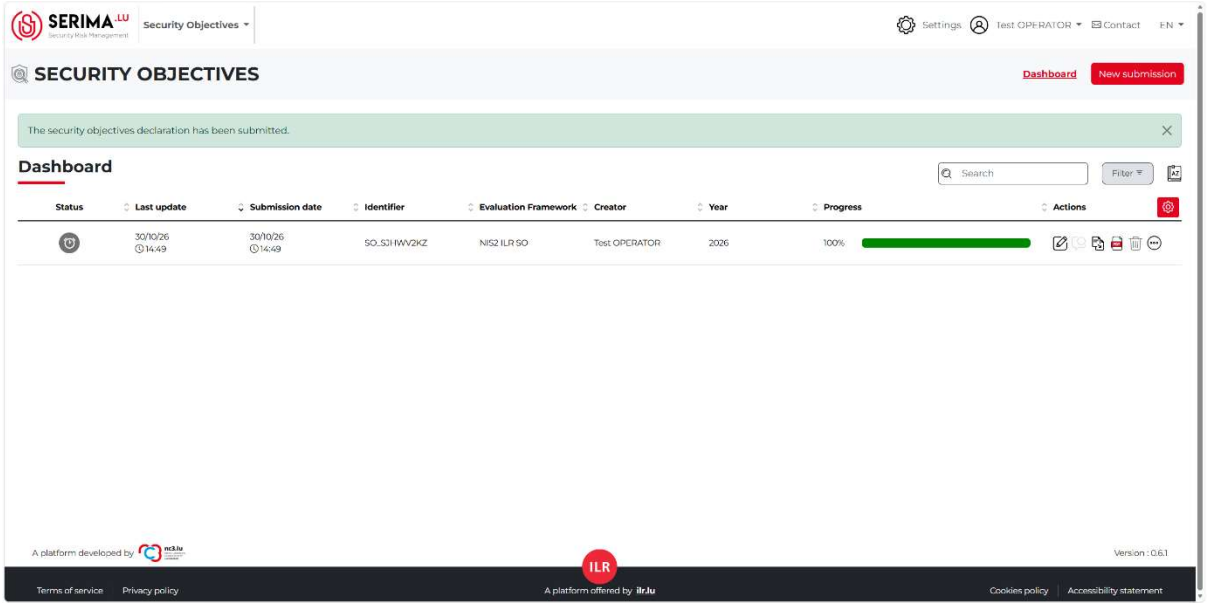
1. Directly from the detailed declaration view, displaying the 50 questions.



2. From the dashboard, using the **Submit** button in the **Progress** column.



Click **Submit** to send your completed declaration to the ILR for review.



After submission:

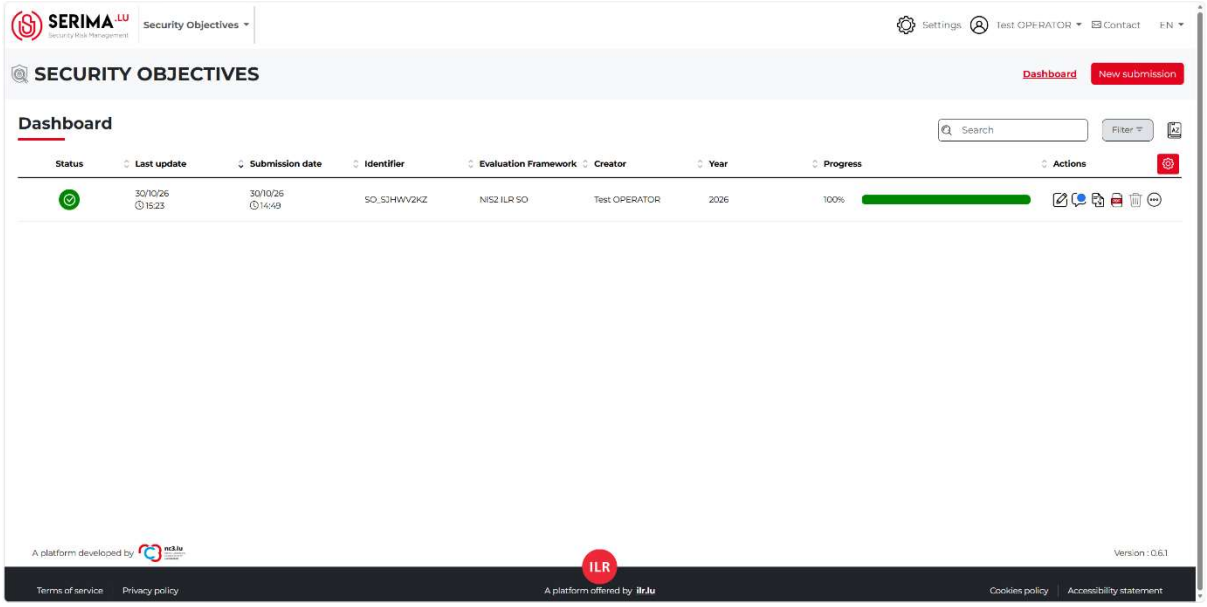
- The declaration receives the status **Under review**.
- The submission date is displayed on the dashboard.
- The declaration becomes read-only and can no longer be edited or deleted.
- A confirmation e-mail of submission is send to both, the ILR and the operator.
- The ILR reviews the submitted declaration.

3.4. View the Review Result and Update Your Declaration

View the Review Result and Update Your Declaration

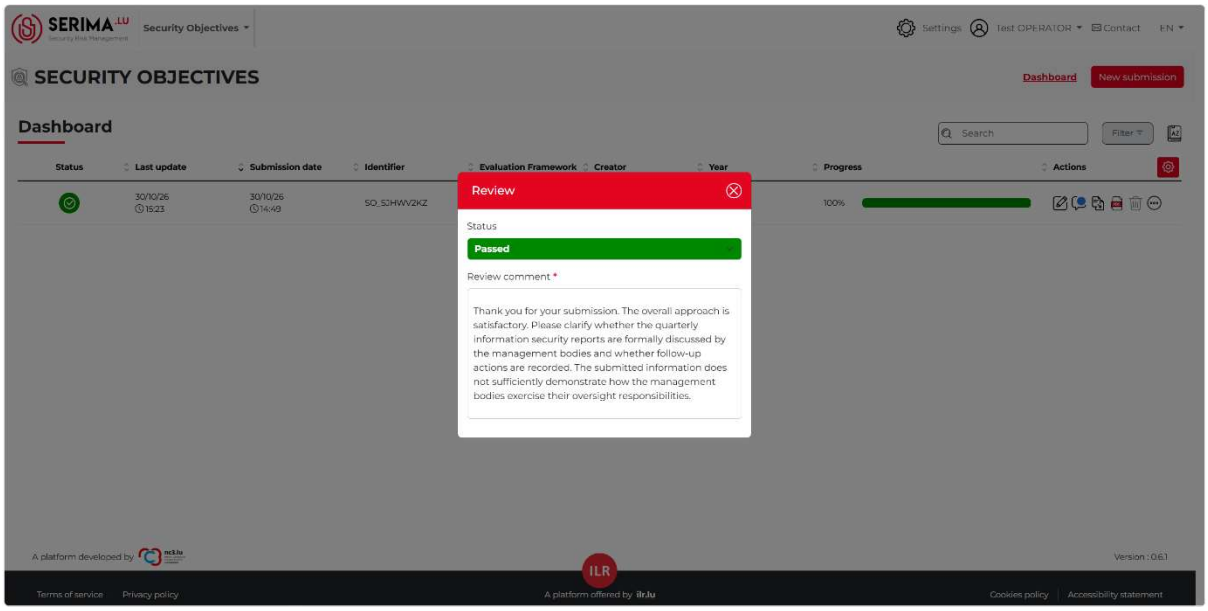
Once the ILR has completed and sent its review, the declaration status changes to one of the following:

- **Passed:** The ILR has accepted the declaration.
- **Revision required:** The ILR requires changes to one or more security objectives.



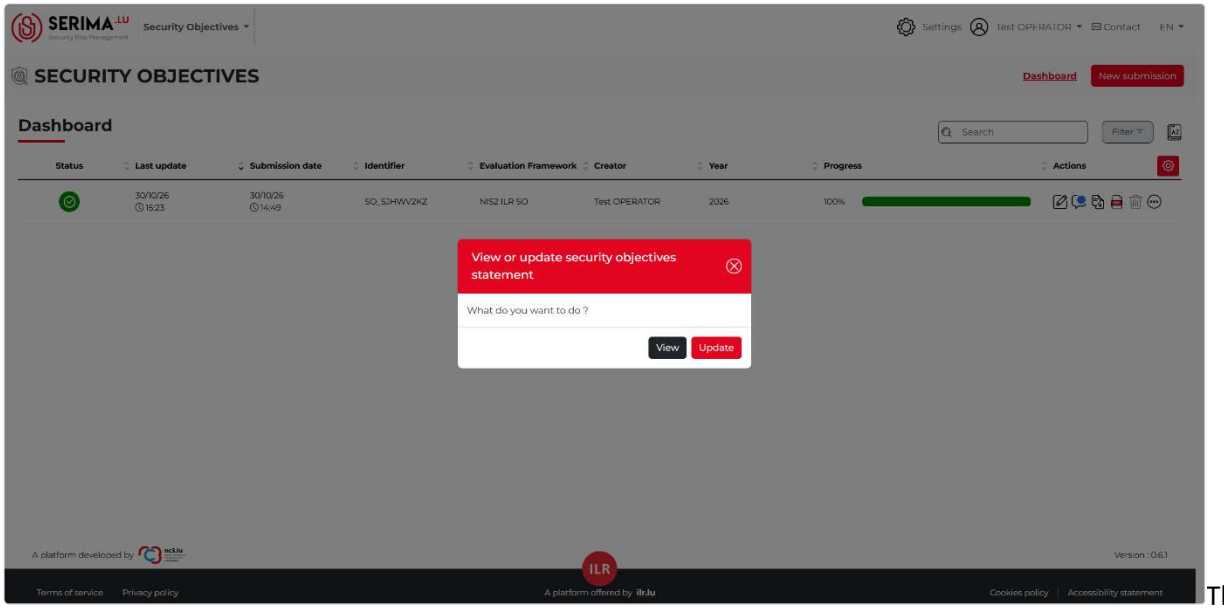
Accessing the ILR's comments

To quickly access the ILR's overall feedback, click the speech bubble icon in the dashboard, next to the edit pencil icon. A blue indicator on the icon signals that a new review comment is available. A pop-up window displays the comment.



Please note that this shortcut only provides access to the ILR's overall comment. It does not display comments relating to individual security objectives or their respective security measures.

To view both the overall review comment and any comments relating to individual security measures, open the detailed declaration view by clicking the edit pencil icon in the dashboard's **Actions** column.



The **Update or review security objectives statement** pop-up will appear, offering two options:

- **View:** Opens the submitted declaration in read-only mode. You can review your answers for each security objective, see the ILR's assessment and access all comments. The overall review comment is available via the **Review comment** icon, while comments relating to individual security measures are displayed in the corresponding **Review comment** column.
- **Update:** Creates a new, unsubmitted version of your declaration, allowing you to make changes or provide additional information in response to the ILR's feedback.
- **Please note:** Even if the ILR has not yet reviewed your submission but you would like to modify your submission, you may submit a new version.

Updating Your Declaration

If you wish to address the ILR's feedback or provide additional information, select **Update**.

The platform creates a new, unsubmitted version of your declaration, automatically carrying over your previous answers and the ILR's comments. The previously submitted version remains unchanged.

Review the comments, make the necessary changes to the relevant security objectives and submit the updated declaration again for the ILR's review.

4. Support

For any support, please contact serima(at)ilr(dot)lu or (+352) 28 228 380.