ENISA Certification Tool Manual

Introduction

ENISA supports the work of CERT-SIG on certification under the EU Cloud computing strategy. The resilience portal contains the tool to support the work of CERT-SIG (on cloud certification). The current document is the manual for the Cloud Certification Schemes List (CCSL) users. You can access the tool here: https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes

1.1 Funtionalities

The tool offers the following functionalities to the users:

Public users:

- View scheme

Only for logged in users:

- Add new scheme
- Edit scheme
- Delete scheme

2 Scheme principles

2.1 Brief (not too long text)

Short answers are easier to read, understand and compare. We do not want to replace existing websites and literature about the schemes.

Issue:

- *Most schemes have such a short description of at most a paragraph, around 500 chars.*
- *Some schemes have very long descriptions of the content of the standard, spanning more than a page.*

Example: What is the underlying information security standard or best practice

Exemplar reply: "ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements"

In most cases we will need only the name of the standard. If not a characters' limit will be implemented.

We introduce three different scales for answers' length: 250, 500 and 1250 characters.

2.2 Completeness (answer the question)

The answer should cover briefly all points of a question, providing completeness (in link with the above mentioned principle). The more complete each reply is, the more comprehensive will the total presentation of the scheme be.

Issue: Most schemes do not provide a complete answer or provide information irrelevant to the question. Some schemes provide the types of requirements or some keywords in bullets.

Example: What is the structure of the standard or best practice?

*Exemplar reply: "*Cloud Control Matrix is a security framework currently structured in 13 domains and composed of 98 security controls. Security controls included in CCM are cloud relevant controls and are mapped against the most relevant information security controls framework: ISO 27001-2005, Nist SP 800-53, FedRAMP, PCI DSS, Cobit v4.1, AICPA Trust Principle. CCM v3 includes also the mapping against ENISA IAF and German BSI Cloud Security Catalogue.*"*

The briefest the text is the most comprehensive it can be to the readers. The long text rule doesn't apply in this case. The feedback has to give answers to all the aspects refered in the question.

2.3 Relevance and on topic (answer only the question)

The tendency of writing off topic text rather than just answering the question is one more element that can make the content incomprehensive. Such answers should be avoided. Providing answers that are to the point is the main goal when answering a question.

Issue: Most schemes do not answer to the point, other provide a link or a reference or they give some information that are off topic.

Example: Give one or more representative examples of a requirement set in the standard?

Exemplar reply: "The standard is based on 4 steps: Plan (establish the ISMS) Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results inaccordance with an organization's overall policies and objectives. Do (implement and operate the ISMS): Implement and operate the ISMS policy, controls, processes and procedures. Check (monitor and review the ISMS): Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review. Act (maintain and improve the ISMS): Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS."

Our suggestion is to have short answer to the point to make easier for the user to remember and compare with others.

2.4 Factual description (no marketing)

Factual description is required in order to maintain the objectiveness of the Cloud Certification Schemes Lists. Any marketing text that is not relevant to the question or does not reflect the real trust model should be excluded.

Issue: Marketing statements, decrease of objectiveness of the CCSL.

Example: What is the underlying information security standard or best practice?

Reply to avoid: "General information regarding ….Strategic Business plan, Strategic plan for the following 3 years.. "

An answer to that question like the above only serves purposes of marketing and is out of topic.

2.5 Accurate (answer correctly)

Accuracy is also important when describing a scheme. It adds clarity and correctness to the scheme and makes it more easy to understand.

Example: What is the underlying information security standard or best practice ?

Reply to avoid: "Requirements and control catalogues of …, structured in the requirement areas: organizational structure, cloud architecture, data security…"

The answer is not accurate because what is mentioned is not a standard or a best practice. Therefore the answer is not accurate.

The goal is to have all the questions answered correctly and in the most complete but brief manner. In the above example the best approach would be to answer by providing the name of underlying standards or best practices briefly.

2.6 To the present (no promises, but current situation)

Take into consideration only what is valid in the present moment for the scheme when answering. Please, do not announce future publications or implementations.

Issues: Some answers are not providing any useful information rather than just announcing a future date or a future state of a document.

Example: "Link to standard or best practice"

Reply to avoid: "The standard will be published in the version 3 in May, 2014"

Example: " Describe the current adoption of the certification framework."

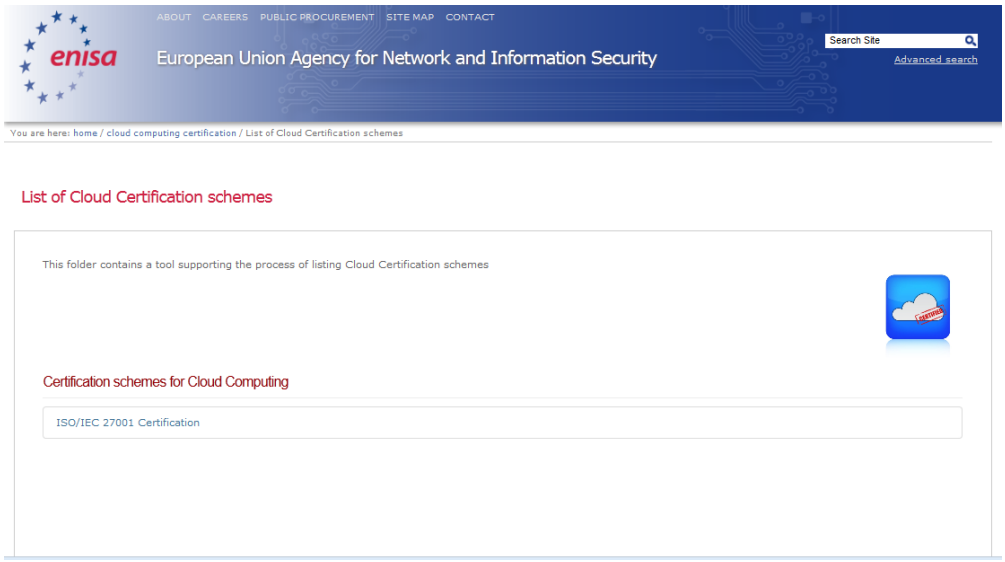
Reply to avoid: "...will be available in Q1 2014 … will be available in 2015"

Such answers should be avoided and be replaced by answers like: "No link" or "Not applicable yet". You can add future steps in the according question in the end section 4: vision and future steps.

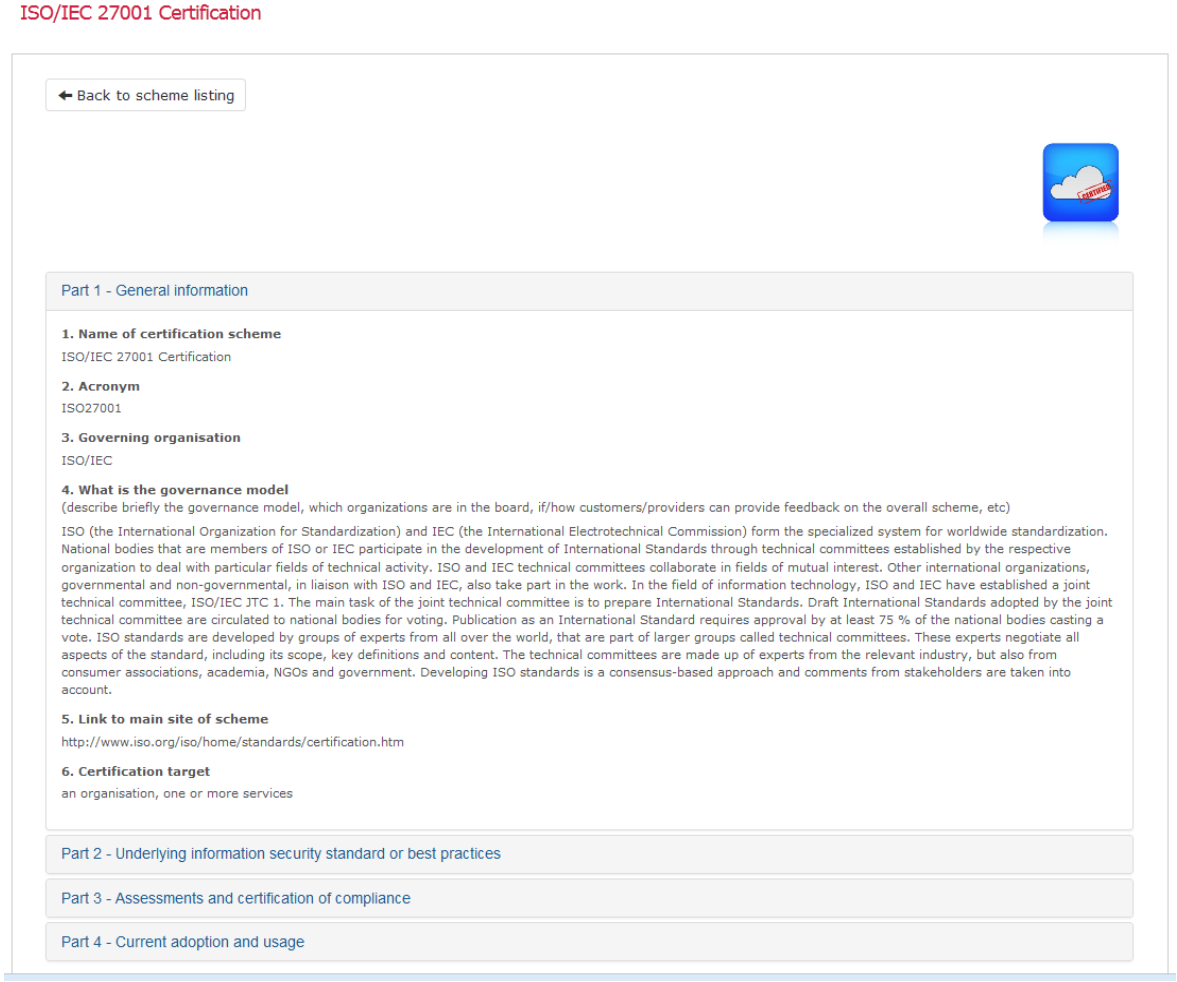
3 View scheme – Public view

Public user can view a list of certification schemes (only the ones that have been approved by ENISA/moderator), select one scheme and view more informationon this scheme. Some visuals below:

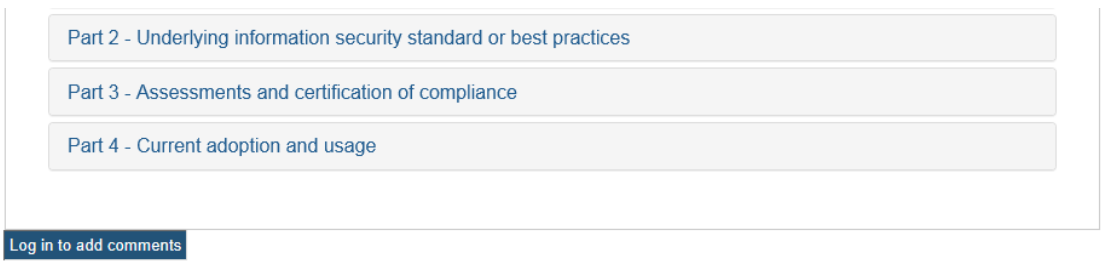
- List of Cloud Certification schemes:


ABOUT CAREERS PUBLIC PROCUREMENT SITE MAP CONTACT
European Union Agency for Network and Information Security
Search Site
Advanced search
You are here: home / cloud computing certification / List of Cloud Certification schemes
List of Cloud Certification schemes
This folder contains a tool supporting the process of listing Cloud Certification schemes
Certification schemes for Cloud Computing
ISO/IEC 27001 Certification

- Scheme has been selected and the public user can view its content. The "Back to scheme listing" button will take the user to the list page:

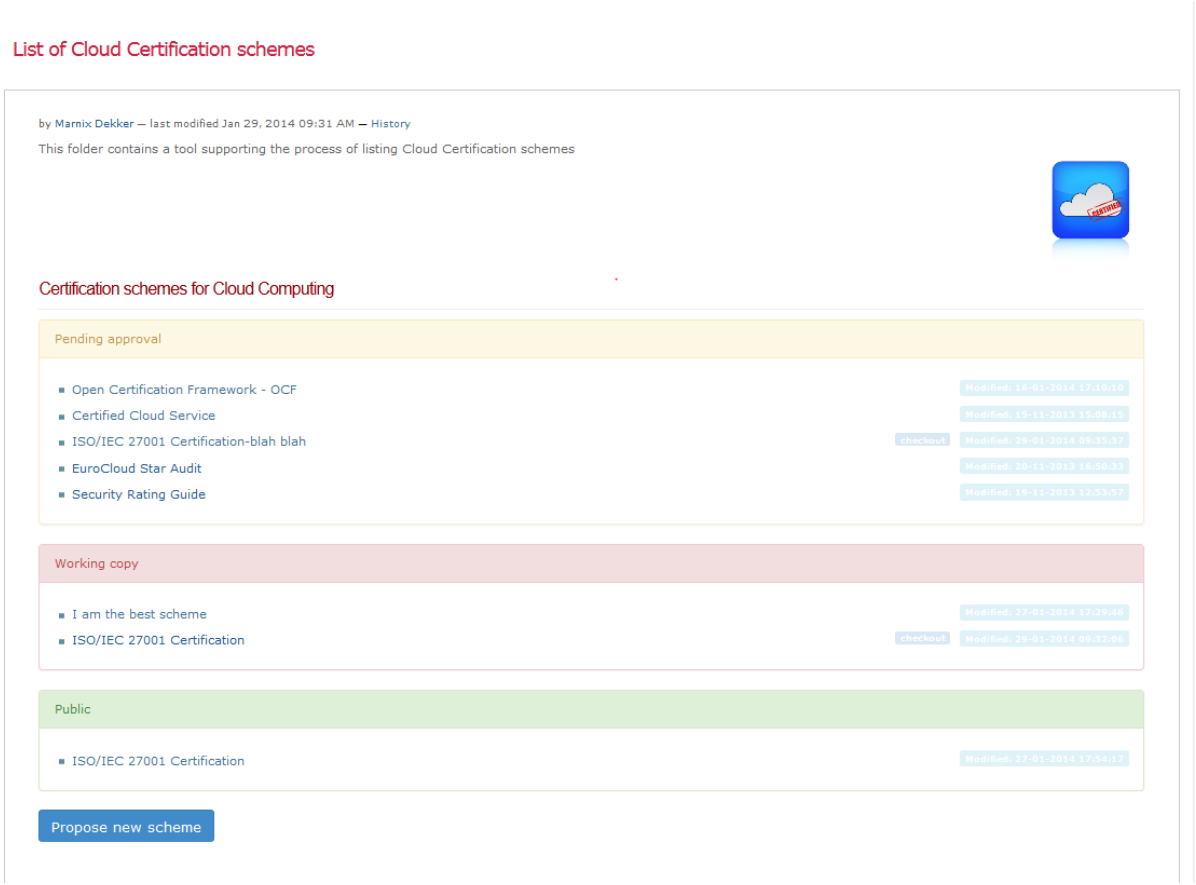


- In the end of the page you can find a button for comments. To provide comments on the certification scheme you will need to have an account and login. For further inquiries you can send an email to Cloud.Security@enisa.europa.eu

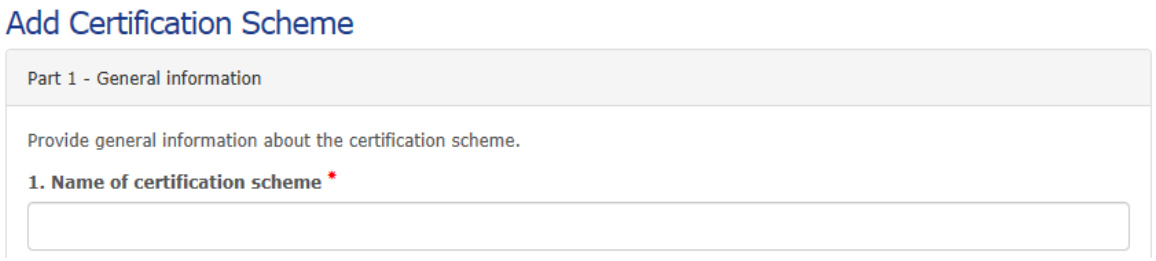


4 Add new scheme

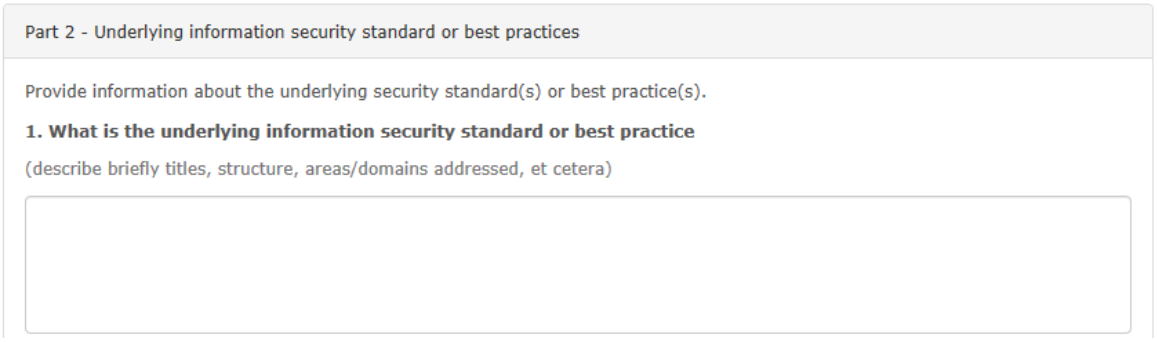
After the user logs in he can see the schemes that are pending approval and the ones that have been approved (Public). He can then add a new scheme by clicking the ''Propose new scheme'' button. Before you start compiling the new scheme, go through the guidelines on how to fill in the questionnaire that can be found in the annex.



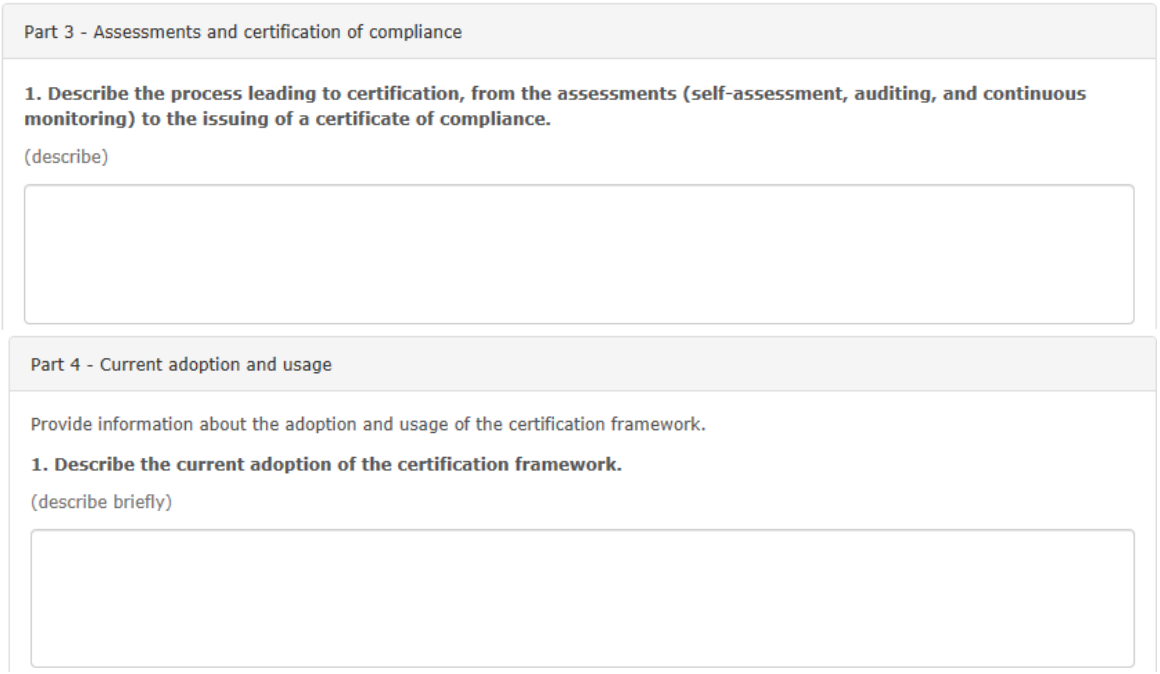
By pressing the ''Propose new scheme'' button an empty form appears and the user has to fill in the 4 different parts according to the template. The user can perform two actions: either "Save" the scheme or "Submit" it. A user can "Save" a form to come back and "Edit" it in future time. If the form is ready, the user can "Submit" it.



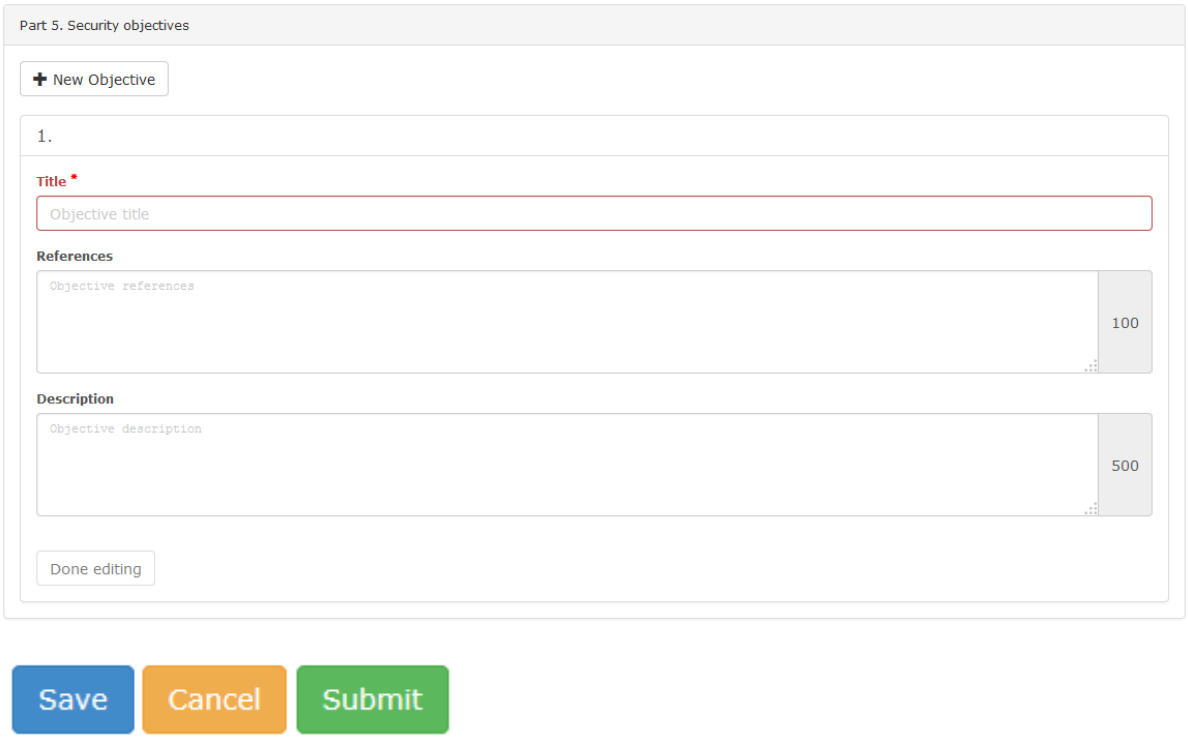
Some fields are obligatory (red dot), other are optional.



In each text field provide an answer according to the principles in conjuction with the corresponding question's guideline (see Annex A). For example, in the above textarea you should provide an answer with maximum length 500 characters as proposed in guidelines (part 2 question 1) and follow the principles as analysed in section 1.



Part 5 is different from the other parts. In part 5 the security objectives are added in the scheme. Creating a new objective is done by pushing the "New security objective" button and then filling in the three fields below; field 1 is the title, field 2 is the reference of this objective to the certification framework (paragraph, section etc) and field 3 is the description. All principles mentioned above apply to these fields as well. Title is the only one marked as obligatory field, but the other fields are also highly recommended to be filled in with the relevant information. When finished the user presses done, and then the user can add more objectives or continue to the rest of the fileds.



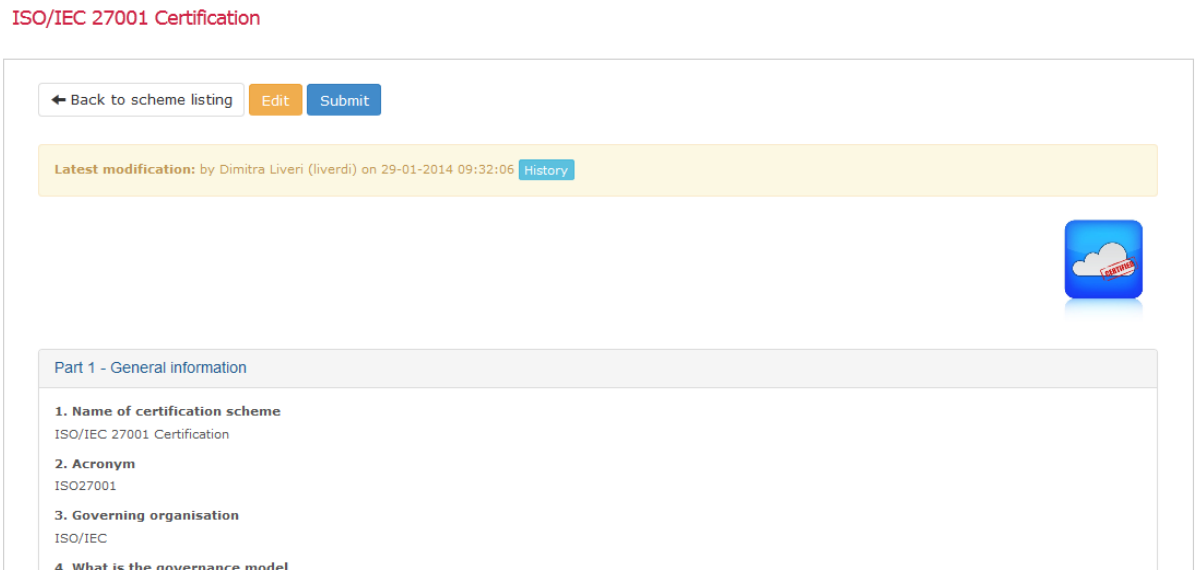
When submitted, the user cannot make anymore editions in the scheme. The scheme will change status to “pending approval”. When submitted the moderator will get a notification of a new scheme, and will be able to approve it or deny the approval.

1. If apoproved the scheme will change status to “Public”.
2. If denied the scheme will be retracted back to “Working Copy”

5 Edit scheme

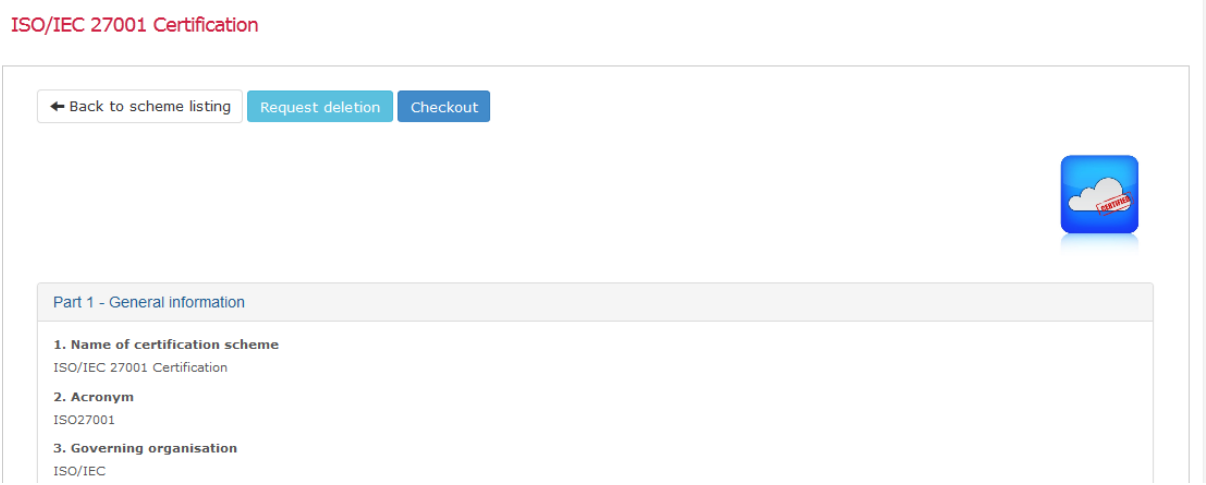
5.1 How to edit a working copy

If the user would like to “Edit” one of the schemes that are in “Working copy” mode, he just needs to select “Edit” button. He can “Save” or “Submit” as described previously. The “Back to scheme listing” button will take the user to the list page.



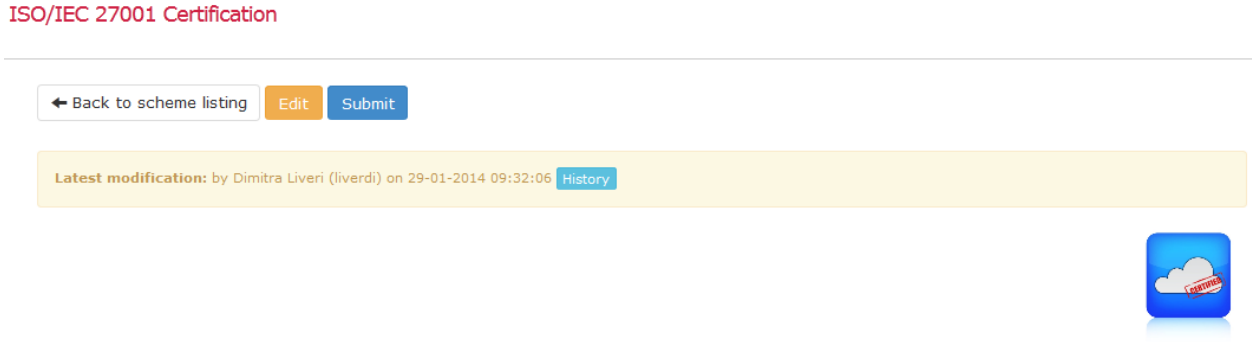
5.2 How to edit a public scheme

If the user selects to edit one of the schemes that are in status “Public”, he needs to press button “Checkout”. This button creates a working copy which then can be edited as discussed before. When the user “Submits” the new copy, a notification email will be sent to the moderator. The moderator will then approve or deny the changes and update the status of the scheme to “Public”.

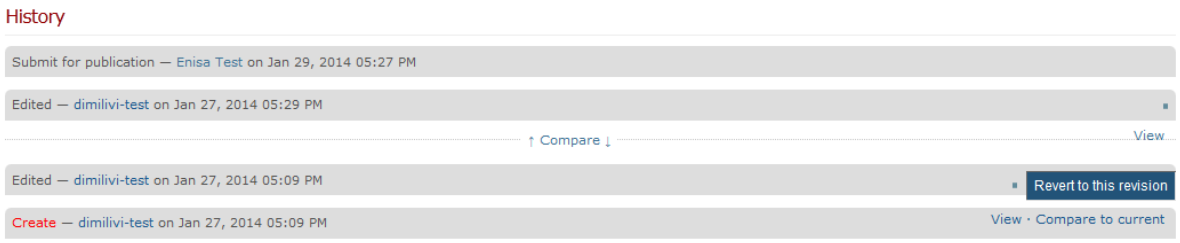


5.3 How to see previous versions

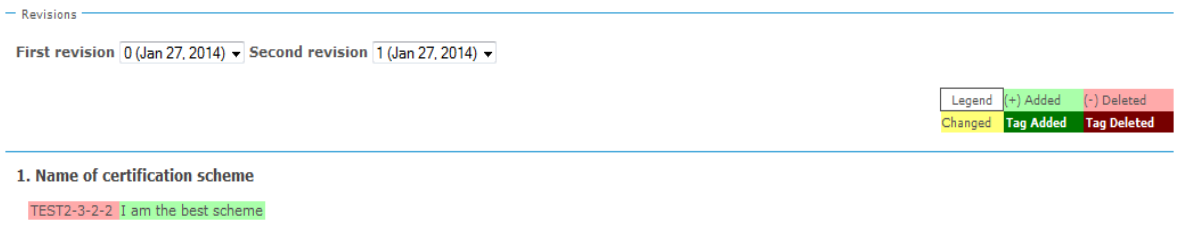
If the user wants to see the previous versions of one working copy, or the history of edits of the scheme, he/she should press the “History button” on top of each scheme:



The next screen will show the history of actions to the specific scheme

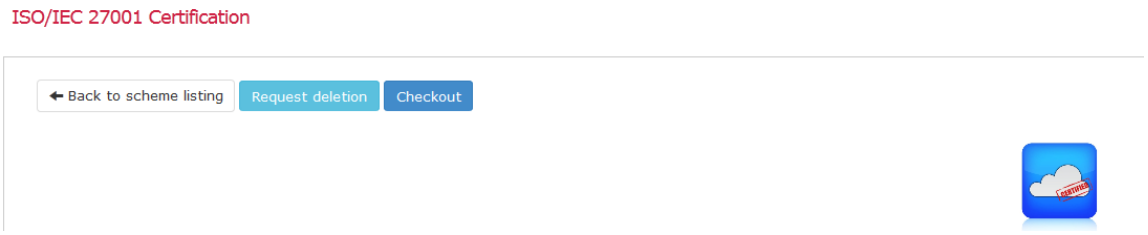


If the user wants to see tha changes he/she will need to press “Compare” and you will see the changes in the according fields:

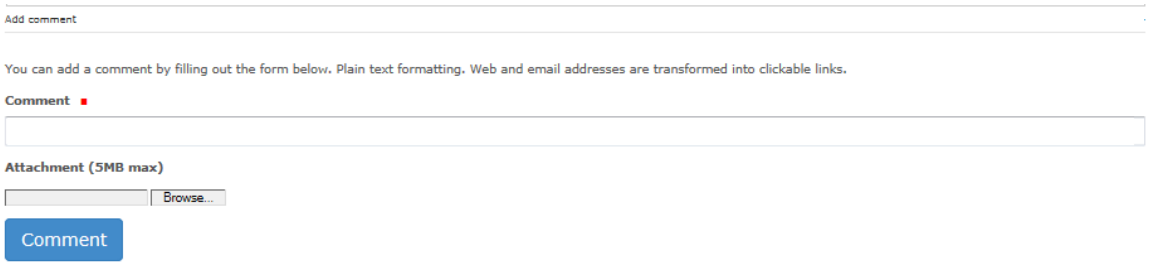


6 Delete scheme

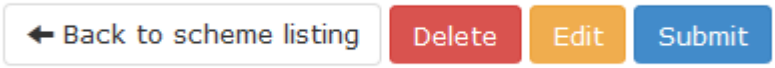
After the user has logged in, he can request deletion of a public scheme. The scheme will be submitted for deletion. The moderator will receive a notification email with the request of the user.



In the botton of the page the user will be able add a comment and explain why the deletion should be accepted.



If the scheme is a working copy, the user can delete it only if he is the creator of the item. If not the user should send a comment justifying the request for deletion so that the moderators can assess it.



Annex A: Scheme Guidelines

Additionaly, apart from the 6 principles mentioned in section 2 we provide a set of guidelines on how to fill in the questionnaire in CCSL. These requirements will be also implemented in the tool.

Part 1-General Information

1. Provide only the name asked and not any description (maximum length: 1line).
2. Provide only the acronym asked (maximum length: 1 line).
3. Provide only governing organizations in bullets format and not any other description.
4. Provide only a description with maximum length 1250 characters.
5. Provide only the link that leads to the main site of scheme.
6. Provide an answer which consists of one or more of the following choices: an organisation, one or more services, set of business processes.

Part 2-Underlying information security standard or best practices

1. Provide only a description with maximum length 500 characters.
2. Provide only the acronym asked with maximum length 1 line.
3. Provide only the link that leads to the standard or best practice.
4. Provide only bullets with small answers/specific choices.
5. Provide only bullets with small answers/specific choices.
6. Provide an answer which consist of the following choices: Yes/No, Free/Paid. *(eg. Yes, Free)*
7. Provide an answer which consist of the following choices: Yes, is based on the x. / No.
8. Describe an example (max. 1250 characters) without adding any links or references.

Part 3-Assessments and certification of compliance

1. Provide only a description with maximum length 1250 characters.
2. Provide only the names of organisations in bullets.
3. Provide only the names of organisations in bullets.
4. Provide only short answers/specific choices in bullets.
5. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
6. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
7. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
8. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
9. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
10. Provide an answer which consist of the following choices: Yes (followed by the link) / No.
11. Provide an answer which consist of the following choices: Yes (followed by a small description - max. 2 lines) /No.

12. Provide an answer which consist of the following choices: Yes (followed by a small description - max. 2 lines) /No.

Part 4-Current adoption and usage

1. Provide only a description with maximum length 500 characters.
2. Provide only an acronym (max. 1 line).
    a. Integer – just the number.
    b. Link – just the link.
    c. Remarks/notes – a small note (max. 50 words).
3. Provide an answer which consist of the following choices: Global / across EU.
4. Provide an answer which consist of the following choices: Global / across EU.
5. Provide a text with maximum length 500 characters.

Part 5-Security objectives

1. Provide a title of the security objective.
2. Provide the corresponding reference of the security objective.
3. Provide a short description of the security objective with maximum length 500 characters.

For example in the image below it is shown a part of ISO27001 annex A. The highlighted text is the one that is used to fill out the part 5 of CCSL.

A.7.2	**During employment**	
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

In CCSL part 5 will be presented as following:

Title: Human resources security - During employment

Reference: A.7.2

Description: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.