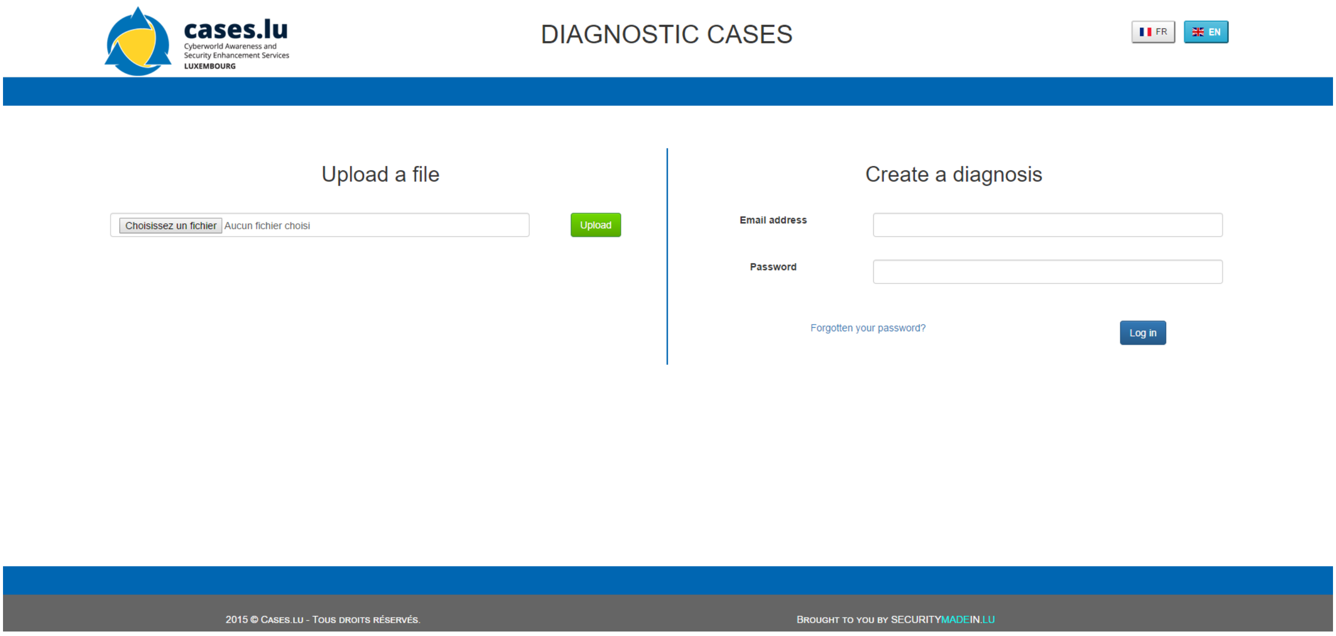
User guide for CASES Diagnostic

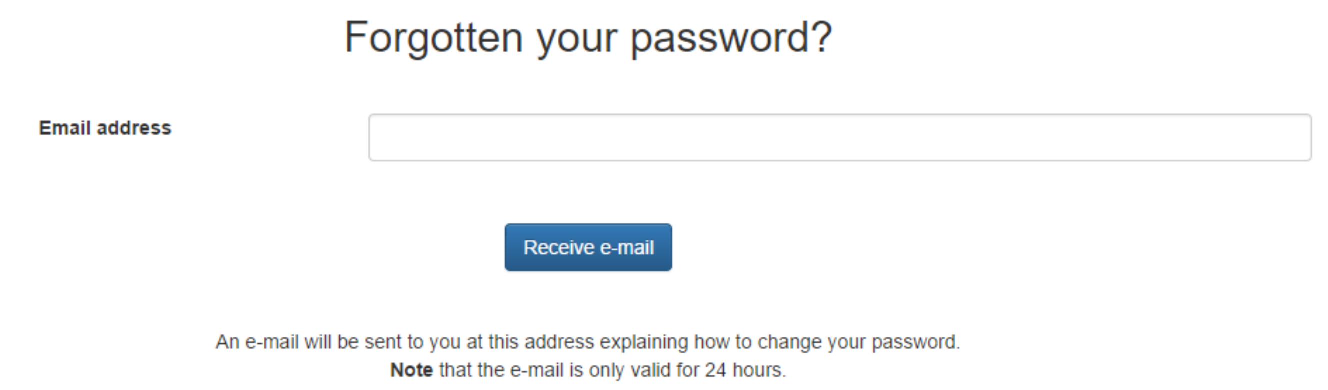
Benjamin Joly

Version 1.0, 2017-09-19

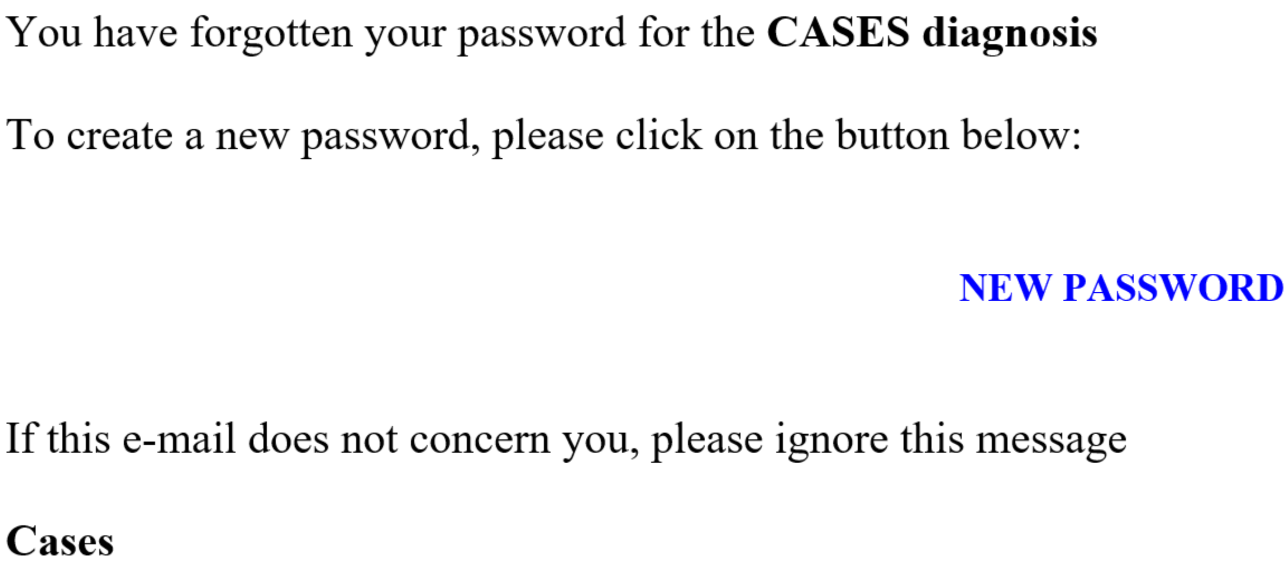
First connexion and Password change



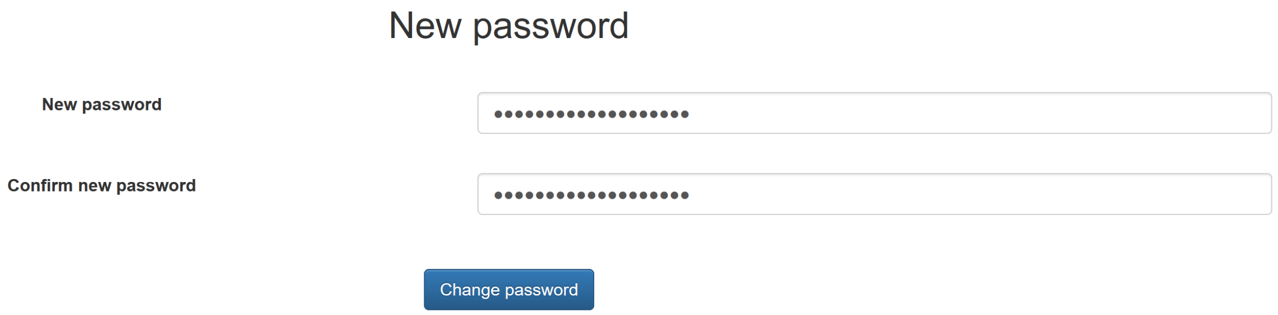
The first step to do is to change the password. For that, just click on the 'Forgotten your Password?' link, and put the mail which should be on the database.



Then mail will be sent to you.



By clicking the link ‘NEW PASSWORD’ in the mail, you will get into a page where you can change your password. You only need to put the new one into the two text fields, and then just click on the ‘Change Password’ button. If the mailing address is not found on the database, the mail will not be sent.

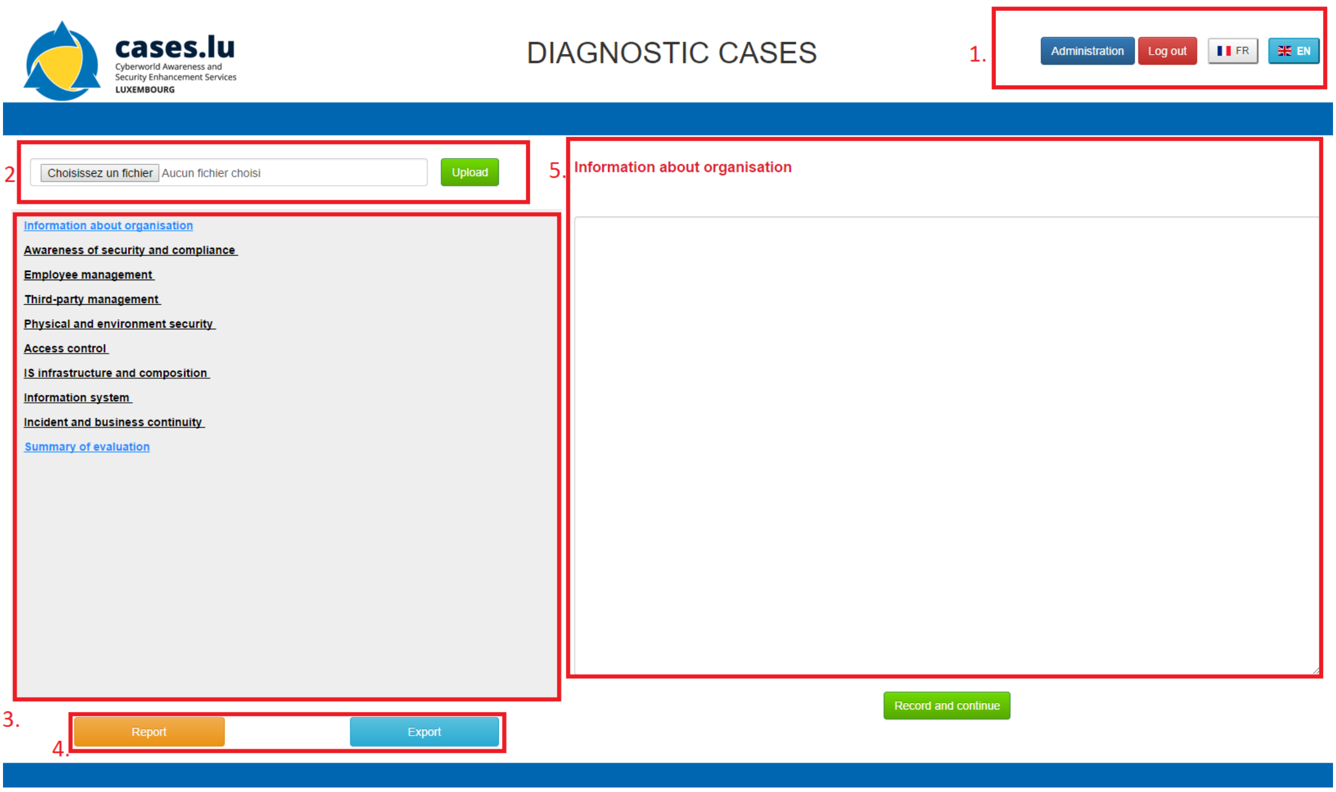


Then, you just need to create your first own diagnostic. For that, just log in to the main connexion screen, by giving your mail and your new password. Then, just click on the ‘Log in’ button.

WARNING	If you are on the Virtual Machine, you will NOT have any mail server installed by default. So you wont receive any mail unless you install one. You can also use a script included in the virtual machine to change manually a password of any user (name_of_script.sh)

TIP	How to use the script, short description.

Begin a Diagnostic as a User

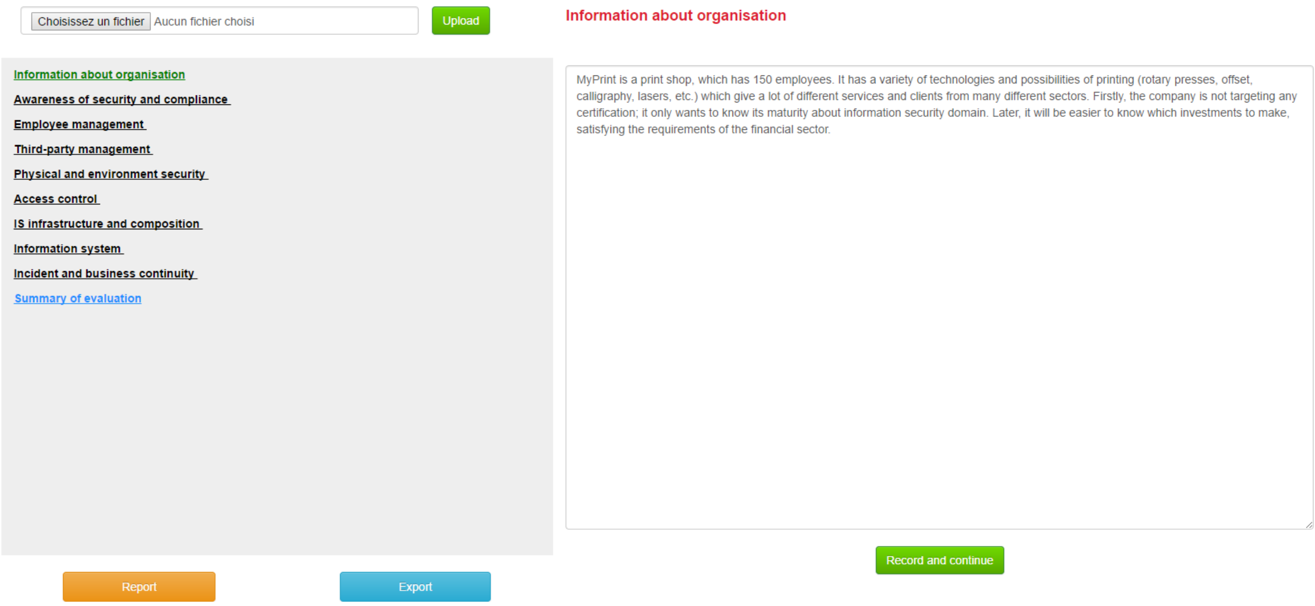


On the header, at the right side (**1.** on the picture), you can set, by clicking on the corresponding button, your language (**French** and **English** are the two only choice right now). You can also disconnect by clicking on the ‘Log out’ button. Also, if you are administrator of the application, you should see the admin menu access button near the red button use to disconnect.

On the top of the screen but below the header, at left, you could see a button where you could just resume form an old diagnostic (**2.** on the picture).

Just below, you have the navigation panel (**3.** on the picture), which we will describe just a little later. Same for the two buttons used to get the report or save the current Diagnostic (**4.** on the picture).

Finally, on the right of the screen, you have a free-text panel, where you should put some text which will be in the report (**5.** on the picture). Most of the time, the introduction is used to give the context of this diagnostic, and some info that could be useful when you read the report.



Then, to save your work, you should just hit 'Record and continue'. In the navigation panel, the theme should be green to indicate that there is already some text.

The summary, which is the last part of the Diagnostic, is a short description of the most important points in it. The most important recommendations, what should be done next…

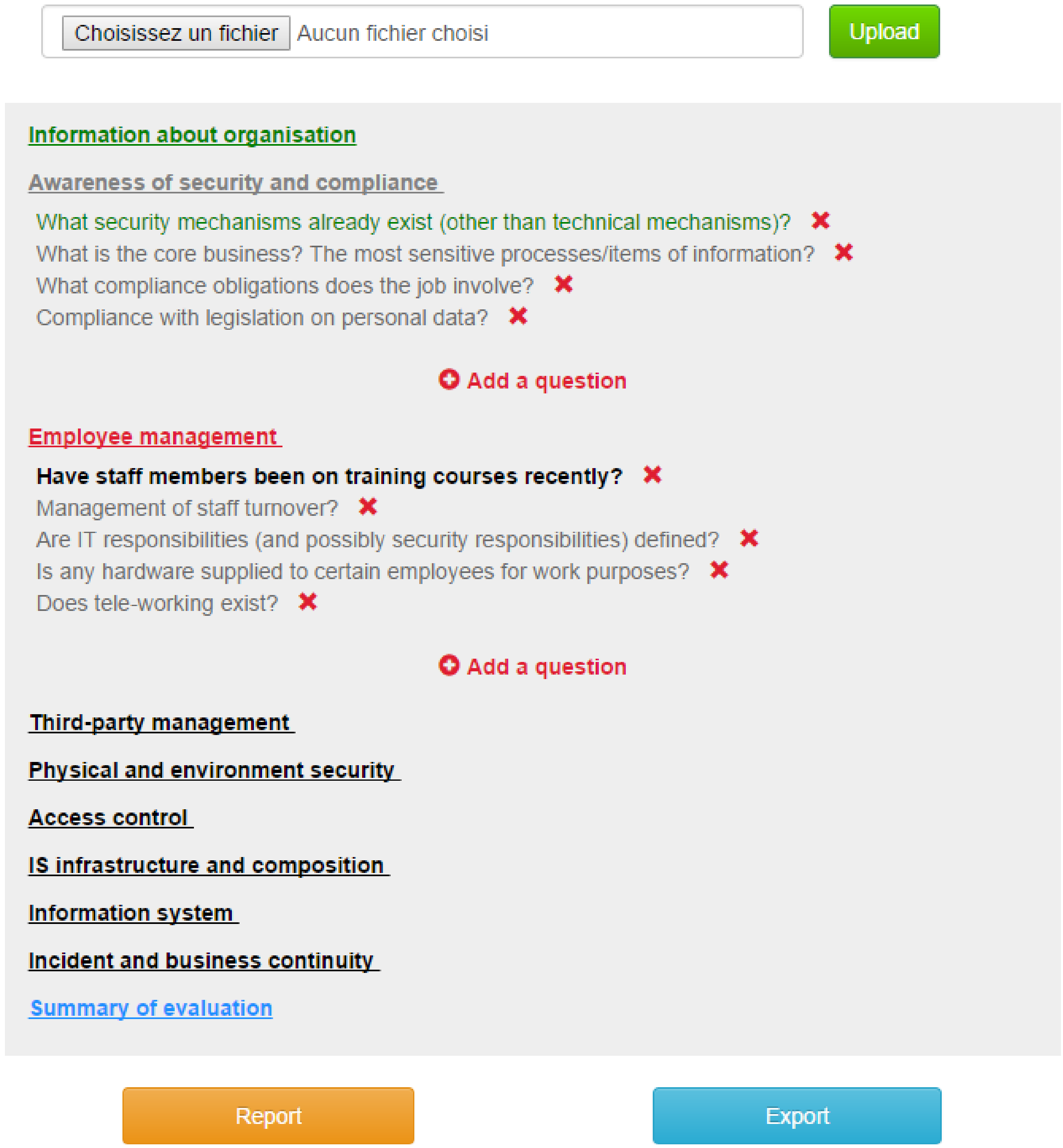
Those are the only free text fields which are present.

After saving the first information, you will be redirected to the first question.

As you can see in the navigation panel, there are eight big themes, which can contain some questions. The red color is mainly used on the theme where you currently are. The question which is black and bold is the current one. The green one is saved and contains text. By clicking on the main theme, question about it will appear, and then you can go on the questions by clicking on them.

The red cross near the question is for delete the question for this diagnostic.

WARNING	If you make a new one, the question will appeared again. If you want to make it disappear for all diagnostic that you make, you should just go in the administration panel to delete it.



You can also add questions by clicking the red **Add a question** button.

WARNING	Be careful, when you do add a question this way, it will be only last during this diagnostic. If you want to add a question for all yours diagnostic, you should add it in the administration part.

You will have the question field to add the question as it will appear into the report. The info field is for details which are displayed only for the question creator. It's useful to add details to the question, or have a reminder of the main points to talk about.

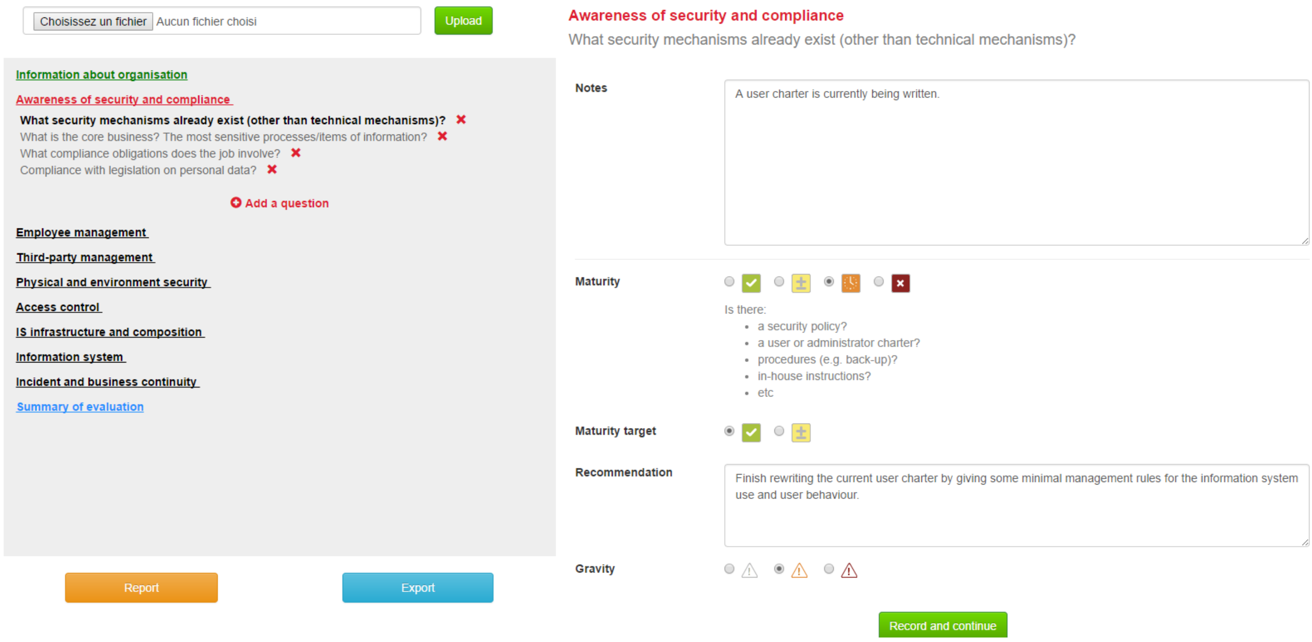
The threshold is a little more difficult to use. To put it simply, this is the weight in the category of the question.

Let's take an example:

Imagine you need a specific question on the BYOD, and you think this should be really important. You have, in the same category, a question less important.

If the threshold are respectively 60 and 40, then the maturity on a level is calculated this way: *((60/3 x maturity) + (40/3 x maturity))* where the maturity could be 0 if not managed, 1 if scheduled, 2 if more or less managed and 3 if managed. So if a policy is scheduled about BYOD and the other question is managed, the category will be *((60/3 x 1) + (40/3 x 3)) = 20 + 40 = 60* out of 100 (The maximal possible) of maturity for this category.

Finally, just hit the green 'Add' button to add your new question and get back on the main page.



On the right side, you have a text field 'Note' where you can put what you have seen, what has been said during the interview, precision about what you want…

The maturity panel is where you can set the current maturity on a scale of four levels (managed, more or less managed, scheduled, not managed). You will also have bullet points to think when you ask the question, what you should have in mind when you asking it, and what kind of answer you should have.

The maturity target panel is the maturity level that the company should have. It's not necessarily managed, so the information security could be adapted from a company to another.

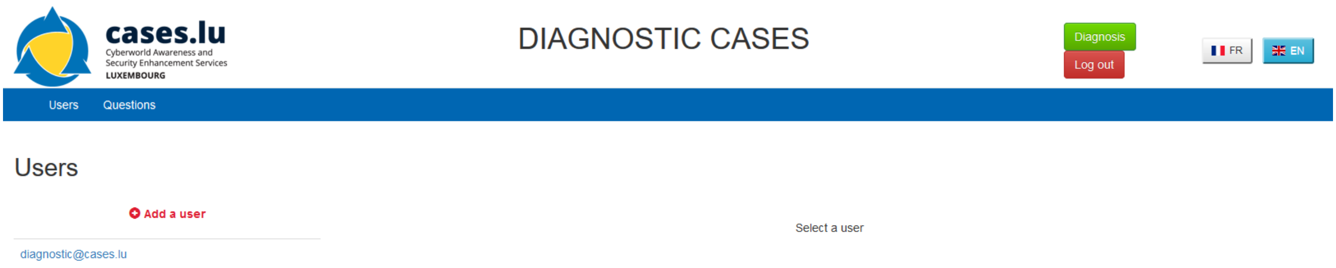
The recommendation panel is the place where you could just put what the company should do to have a better information security.

Finally, the gravity panel is to determine how much the recommendation should be quickly implemented. For saving, as before, just hit 'Record and continue'.

Administration Panel

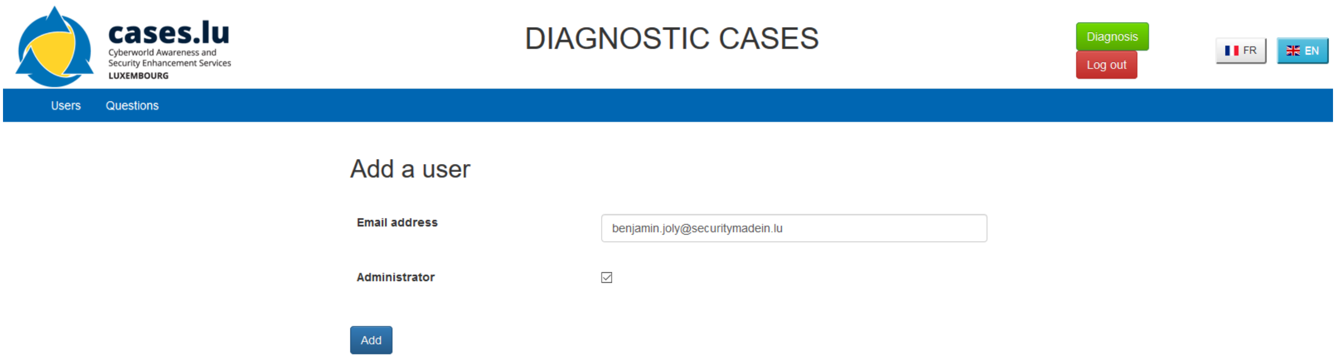
User Tab

You have two tabs (On the blue header), the first one is for Users, and the second one is about the Questions.



You can see all the mail addresses which are authorised to connect to the diagnostic. You can click on the 

button, so you can add a user.



You can put a mail address, choose if this account has access to this interface, and just add it by clicking the blue button 'Add'.

On the page where you can see all mail which is allowed to connect to the Diagnostic, if you click on them, you should be able to modify the address or choose whether it is admin or not.

TIP	The only way to modify a password is to get a password Forgotten link, or the script which is with the Virtual Machine.

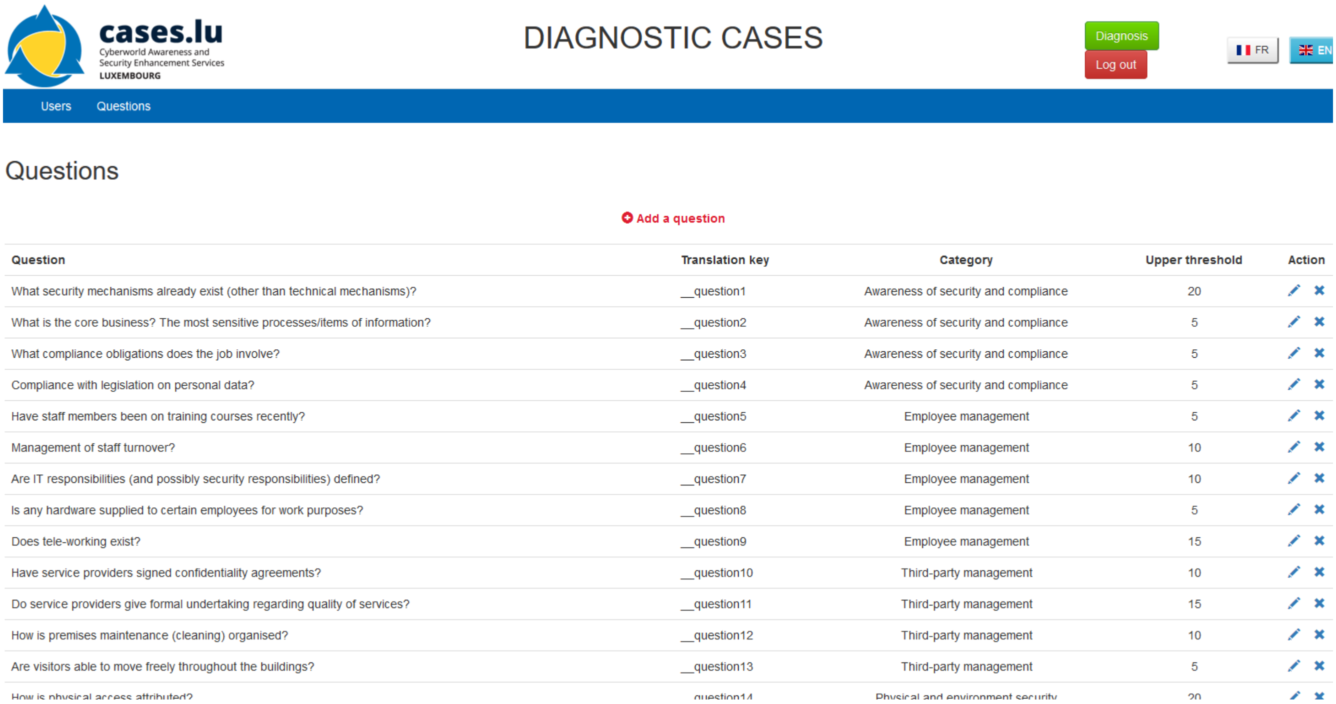
You can also delete an user by clicking on the right side, the red button where "Delete" is written.

WARNING	Be extremely careful, there is no confirmation message when you delete a user here.

Questions Tab

Question Screen

The second tab list all the default questions that will appear when you open a new Diagnostic.

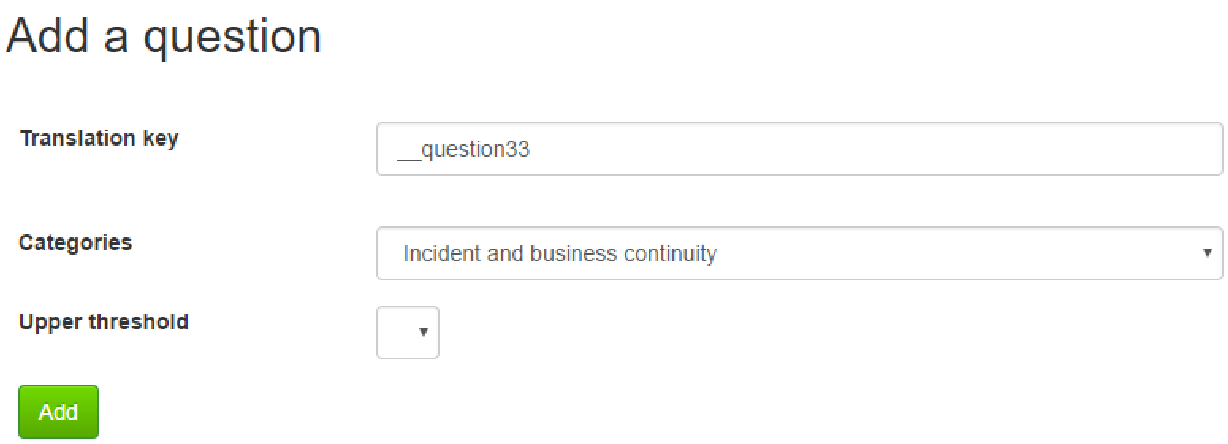


Question	Translation key	Category	Upper threshold	Action
What security mechanisms already exist (other than technical mechanisms)?	__question1	Awareness of security and compliance	20	
What is the core business? The most sensitive processes/items of information?	__question2	Awareness of security and compliance	5	
What compliance obligations does the job involve?	__question3	Awareness of security and compliance	5	
Compliance with legislation on personal data?	__question4	Awareness of security and compliance	5	
Have staff members been on training courses recently?	__question5	Employee management	5	
Management of staff turnover?	__question6	Employee management	10	
Are IT responsibilities (and possibly security responsibilities) defined?	__question7	Employee management	10	
Is any hardware supplied to certain employees for work purposes?	__question8	Employee management	5	
Does tele-working exist?	__question9	Employee management	15	
Have service providers signed confidentiality agreements?	__question10	Third-party management	10	
Do service providers give formal undertaking regarding quality of services?	__question11	Third-party management	15	
How is premises maintenance (cleaning) organised?	__question12	Third-party management	10	
Are visitors able to move freely throughout the buildings?	__question13	Third-party management	5	
How is physical access attributed?	__question14	Physical and environment security	20	

In the 'Question' column, you have all the questions that will appear. The translation key is mainly used to link questions through all languages. The category is, of course, the main theme linked, and the threshold could be assimilated to the maturity that will bring a managed control. To finish, the 'action' column represents the possibility to edit the question (by clicking the pen ( )) or delete it (by clicking the cross ( )).

Add a Question

You can also add questions by clicking the red **Add a question** button.



The first field is for the translation key used by the PO file. The built-in question is done by giving two underscores, the tag "question" and the number of the questions (For example, "__question33").

TIP	If the question is not found in the PO file, then the translation key will be displayed. So if you don't intend to used these files, you can just put your question directly in the translation key.

There are no obligations about it.

You can also choose the category of the question, and its upper threshold as if you were adding a question which is not definitive.

The diagnostic uses the PO files for translations. On the language folder ([*Path_to_Diagnostic*]/languages), you will find the .po files (uncompressed) and the .mo files (compiled).

You can modify manually .po files to add an entry with a text editor, or a PO file editor (Like POEdit).

```
#:
msgid "__question32"
msgstr "Is there a recovery plan?"

#:
msgid "__question32help"
msgstr "Outline or comprehensive?"

#:
msgid "__question33"
msgstr "Is there some protection to natural disaster ?"

#:
msgid "__question33help"
msgstr "Are there common in this area ?<br>What about the fire risks ?<br>Same for flooding, earthquakes, tornadoes ?"
```

If you want to add the translation in another language, you need to modify the other file (In this example, the language is fr_FR).

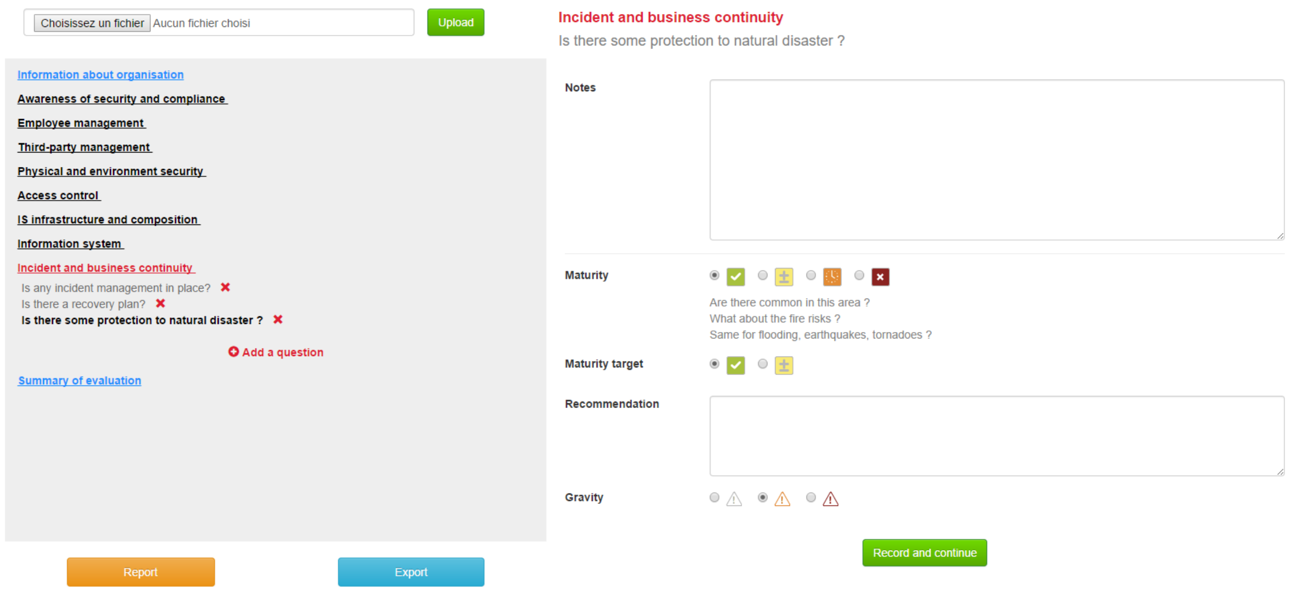
```
#:
msgid "__question32"
msgstr "Existe-t-il un plan de reprise ?"

#:
msgid "__question32help"
msgstr "Ébauche ou complet ?"

#:
msgid "__question33"
msgstr "Y a-t-il une présence de dispositif de lutte contre les catastrophes naturelles ?"

#:
msgid "__question33help"
msgstr "Quelle est la probabilité de telles catastrophes ?<br>Protections contre le feu ?<br>Concernant les inondations, les tornades, les tremblements de terre ?"
```

Then, you will find the question in every diagnostic you will do.



Change a Question

By editing, you will get on a similar interface as if you were adding a question. You can change details on the same ways, as you will also need to change .po and .mo files.

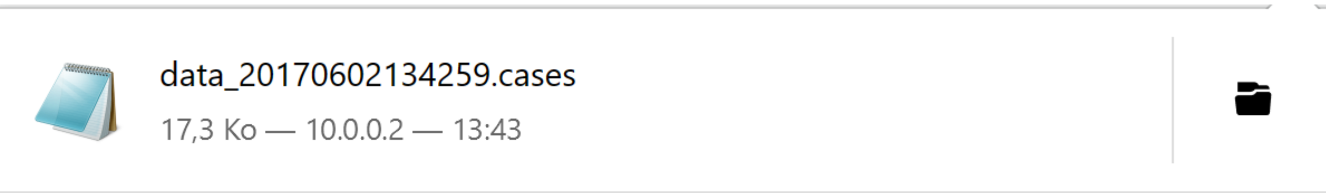
Delete a Question

Just click on the blue cross () to definitly delete the question.

WARNING	Be extremely careful, there is no confirmation message when you delete a question here.

Resume or finish a Diagnostic

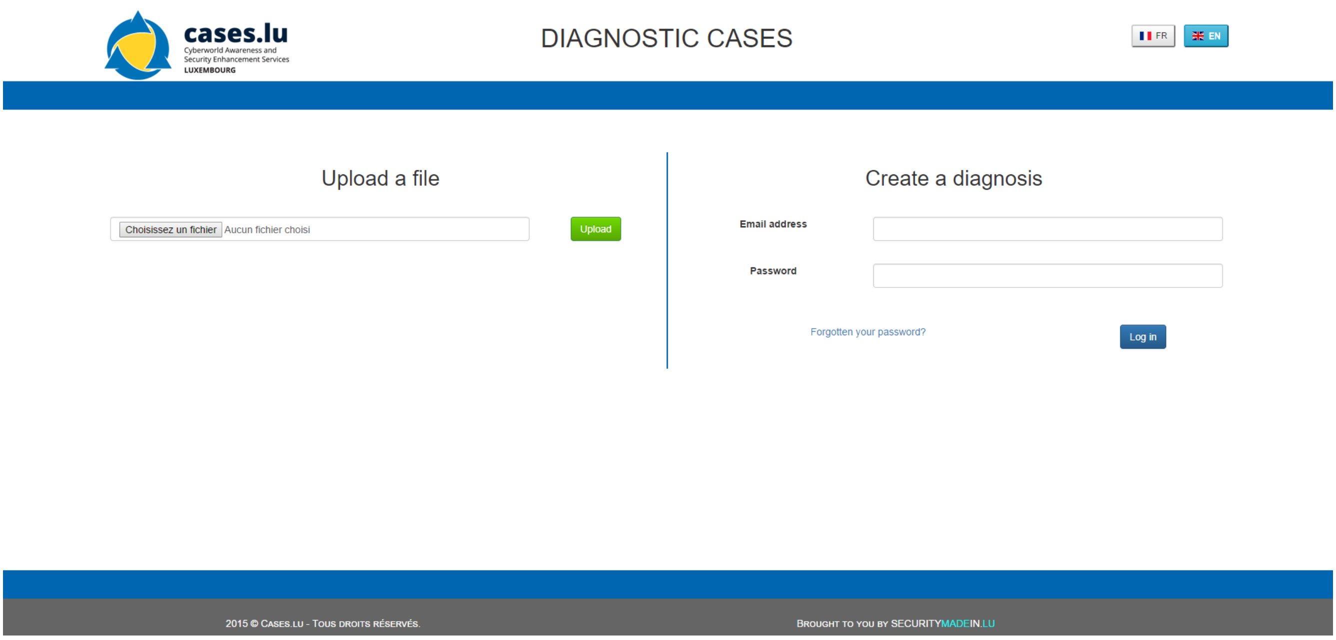
Before your session ends for security reason, or if you want to resume your diagnostic later, it is recommended to export often your work, by hitting the yellow button below the navigation panel.



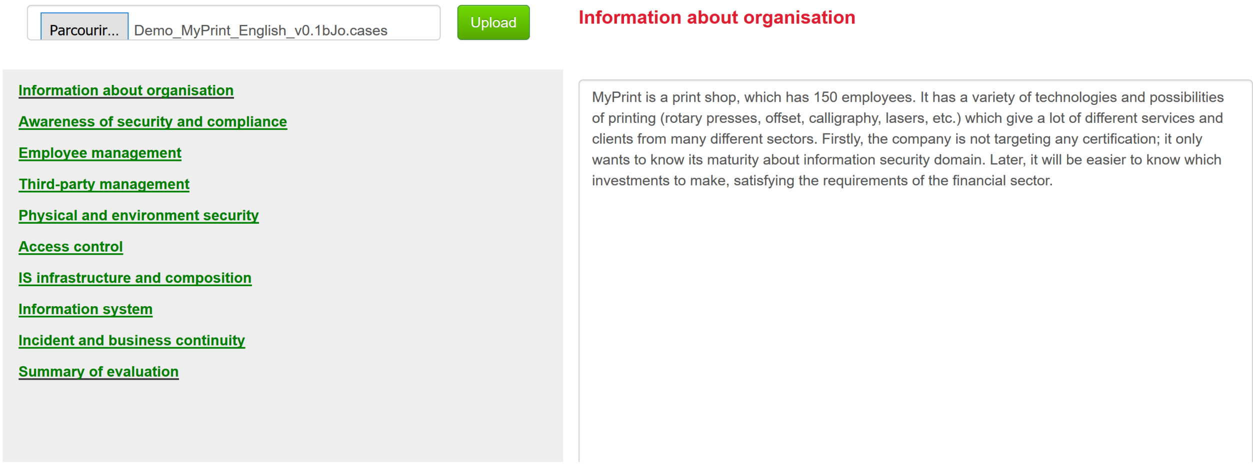
Files are renamed by the following name: data_yyyymmddhhnnss.cases where

- y = year
- m = month
- d = day
- h = hour
- n = minutes
- s = second.

There are two ways to load this diagnostic. The first one, at the connexion screen, doesn't need to have an account to go on it.



By doing this, you will have only access to the report this way. It is mostly used to have another quick way to show an overview of the report. The other way is on the main page that you access just after getting connected.



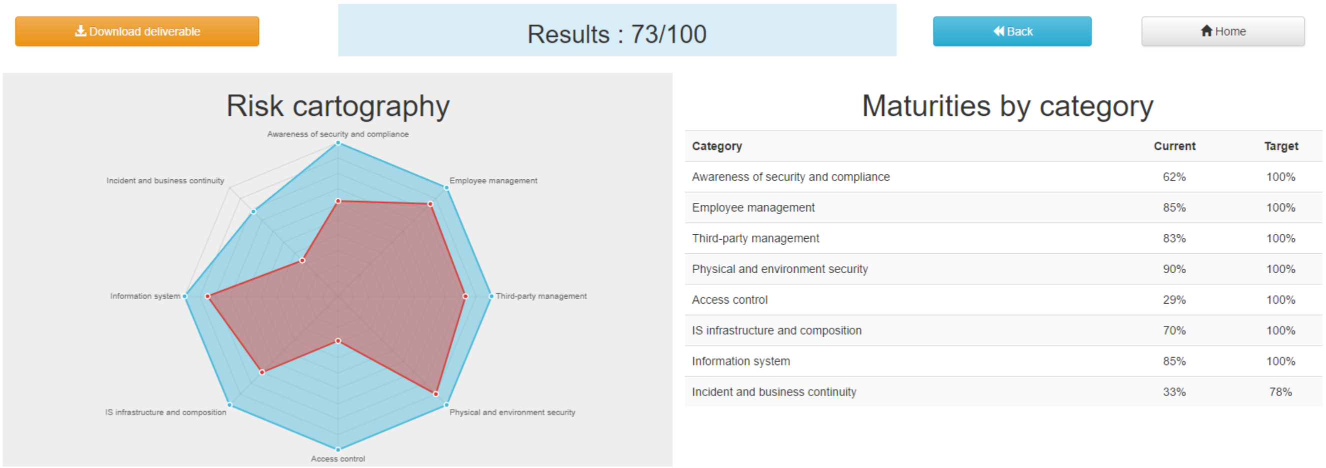
Just on the top of the navigation panel, you can load the file that you have downloaded, or that someone gives to you to resume or modify the Diagnostic.

Report

Online Report

You can access to the screen report by just clicking on the yellow button 

. You can also get this screen without being connected, but you will not be able to download the report as a '.docx'.



Category	Current	Target
Awareness of security and compliance	62%	100%
Employee management	85%	100%
Third-party management	83%	100%
Physical and environment security	90%	100%
Access control	29%	100%
IS infrastructure and composition	70%	100%
Information system	85%	100%
Incident and business continuity	33%	78%

The first graph that you can see is the maturity by domains with the risk cartography and more precisely with the tab on the right. You will also find the recommendation tab which briefly summarises the recommendations, their gravity and their current and target maturity.

Recommendations

Recommendation	Category	Gravity	Goal
Establish a policy of updating the server.	Information system		→
Establish a policy of automated updates on the workstations.	Information system		→
Use the user charter to set the password rules. Use the active directory to apply them.	Access control		→
Outsource a data set periodically. Inform management of the solution and the risks.	Information system		→
Wright broadly some scenario for a crisis or recovery.	Incident and business continuity		→
Raise awareness of the users to make them have a strong password.	IS infrastructure and composition		→
As there is no alarm, the restricted area should be well protected.	Physical and environment security		→
Formalize the hardware inventory by formalizing the coming in and out of the employees.	Employee management		→
Finish rewriting the current user charter by giving some minimal management rules for the information system use and user behaviour.	Awareness of security and compliance		→
Give an awareness campaign to the information security team.	Employee management		→
Sign SLAs with all providers.	Third-party management		→
Visitors must be registered at the reception.	Third-party management		→

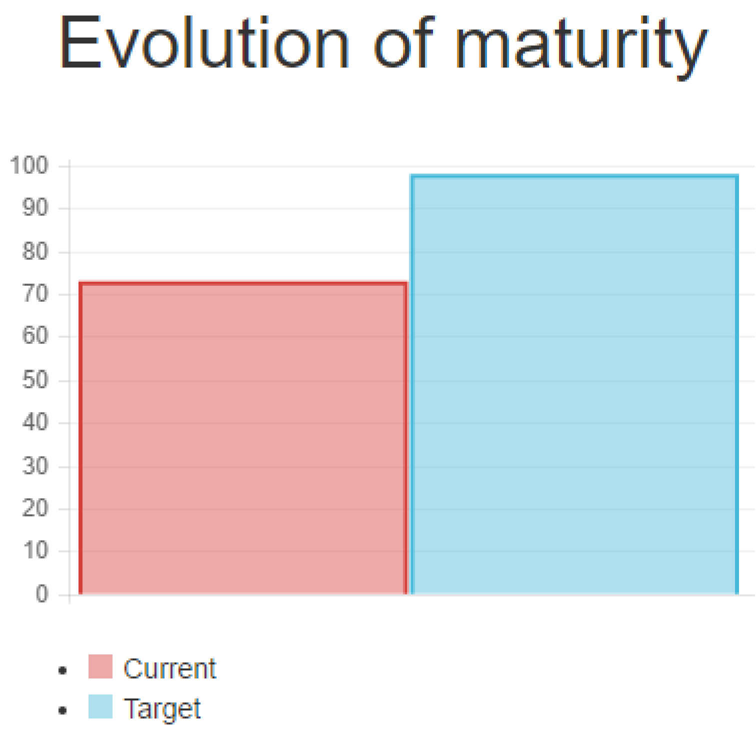
Maturity levels

Not managed | Scheduled | +/- manage | Managed

Gravity levels

Low | Medium | Strong

Just below the first tab, you will find the current maturity level and the target level.



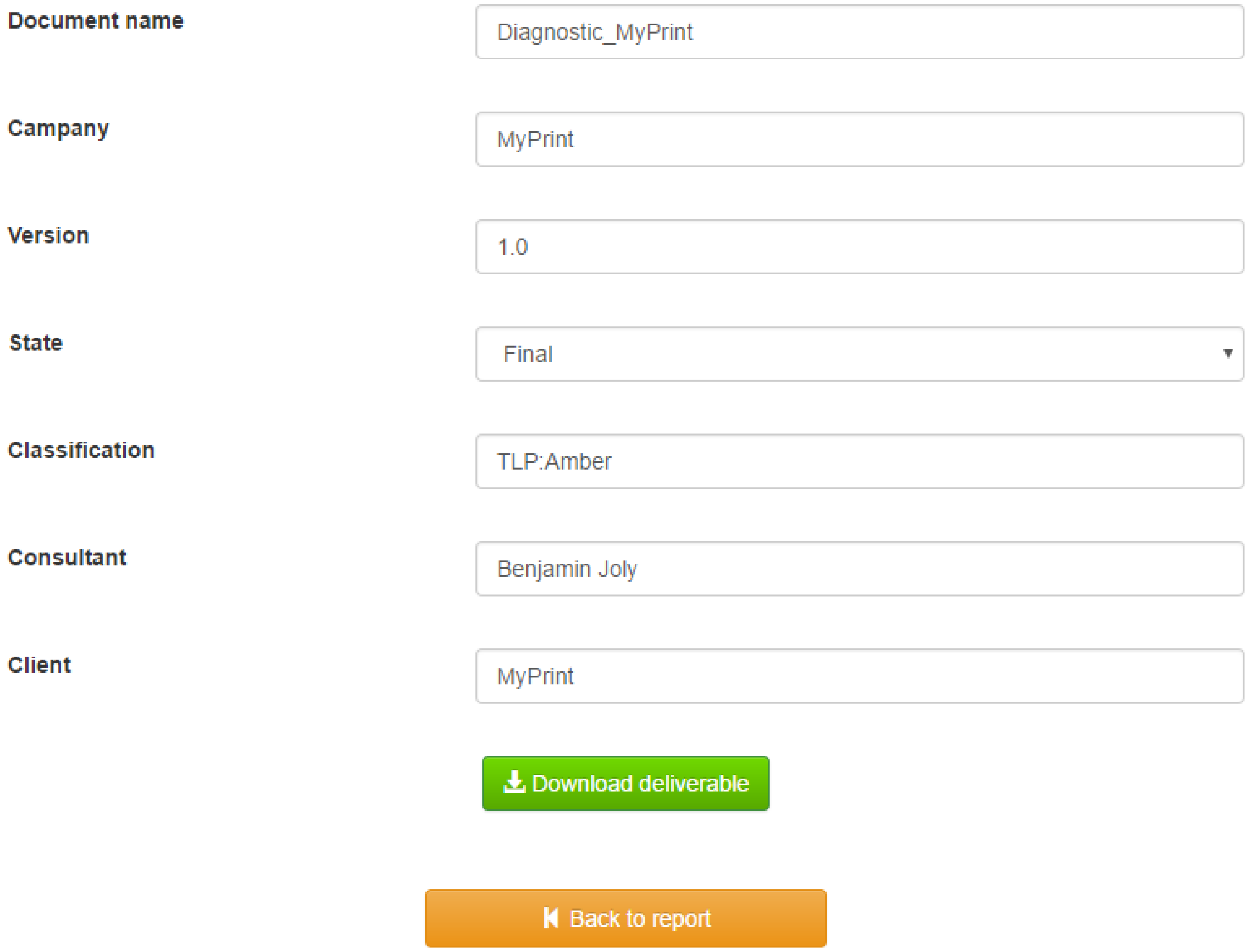
And you will also find the proportion of the category on the whole Diagnostic.

Weighting by category

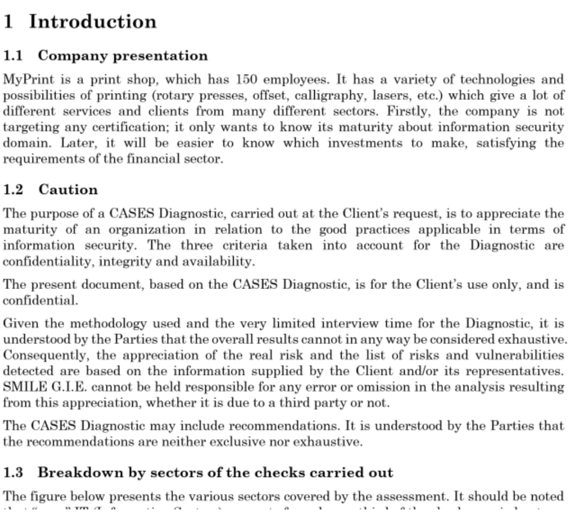
- Awareness of security and compliance
- Employee management
- Third-party management
- Physical and environment security
- Access control
- IS infrastructure and composition
- Information system
- Incident and business continuity

Offline Report

If everything seems okay, you just need to get it on a .docx, and for that, click on the yellow button 'Download deliverable.'



You will need to put a Document Name, the company which concerned by the Diagnostic, the version of the document (If there are multiple Diagnostics, or if you want to correct it…), a choice if it's a draft or a final version of the Diagnostic, the classification of the document (who can read it or have it, it's a free text, so it can be chosen with TLP, or a classification on your own), and finally the name of the consultant and the name of the client. Most of that data will be found on the document. The document will be named [*Document Name*]_Date.docx.



1 Introduction

1.1 Company presentation

MyPrint is a print shop, which has 150 employees. It has a variety of technologies and possibilities of printing (rotary presses, offset, calligraphy, lasers, etc.) which give a lot of different services and clients from many different sectors. Firstly, the company is not targeting any certification; it only wants to know its maturity about information security domain. Later, it will be easier to know which investments to make, satisfying the requirements of the financial sector.

1.2 Caution

The purpose of a CASES Diagnostic, carried out at the Client's request, is to appreciate the maturity of an organization in relation to the good practices applicable in terms of information security. The three criteria taken into account for the Diagnostic are confidentiality, integrity and availability.

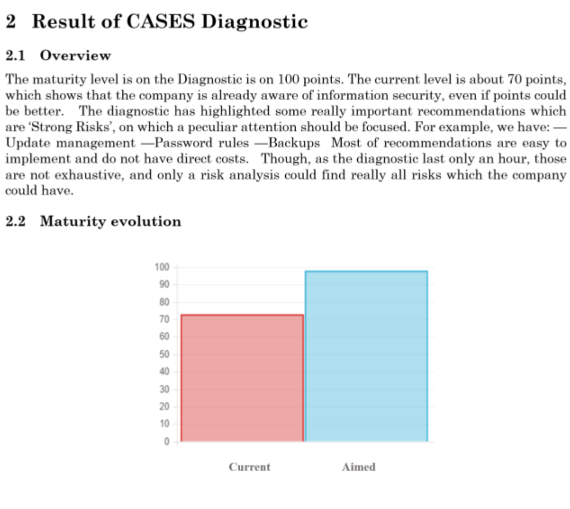
The present document, based on the CASES Diagnostic, is for the Client's use only, and is confidential.

Given the methodology used and the very limited interview time for the Diagnostic, it is understood by the Parties that the overall results cannot in any way be considered exhaustive. Consequently, the appreciation of the real risk and the list of risks and vulnerabilities detected are based on the information supplied by the Client and/or its representatives. SMILE G.I.E. cannot be held responsible for any error or omission in the analysis resulting from this appreciation, whether it is due to a third party or not.

The CASES Diagnostic may include recommendations. It is understood by the Parties that the recommendations are neither exclusive nor exhaustive.

1.3 Breakdown by sectors of the checks carried out

The figure below presents the various sectors covered by the assessment. It should be noted



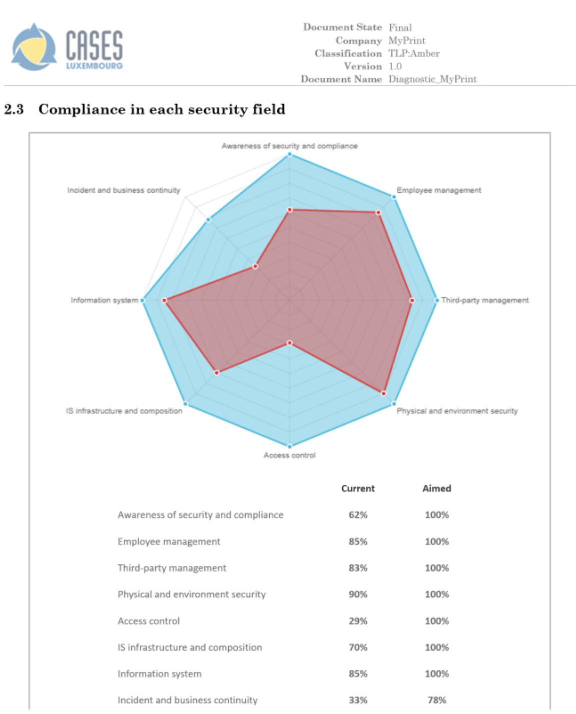
2 Result of CASES Diagnostic

2.1 Overview

The maturity level is on the Diagnostic is on 100 points. The current level is about 70 points, which shows that the company is already aware of information security, even if points could be better. The diagnostic has highlighted some really important recommendations which are 'Strong Risks', on which a peculiar attention should be focused. For example, we have: — Update management —Password rules —Backups Most of recommendations are easy to implement and do not have direct costs. Though, as the diagnostic last only an hour, those are not exhaustive, and only a risk analysis could find really all risks which the company could have.

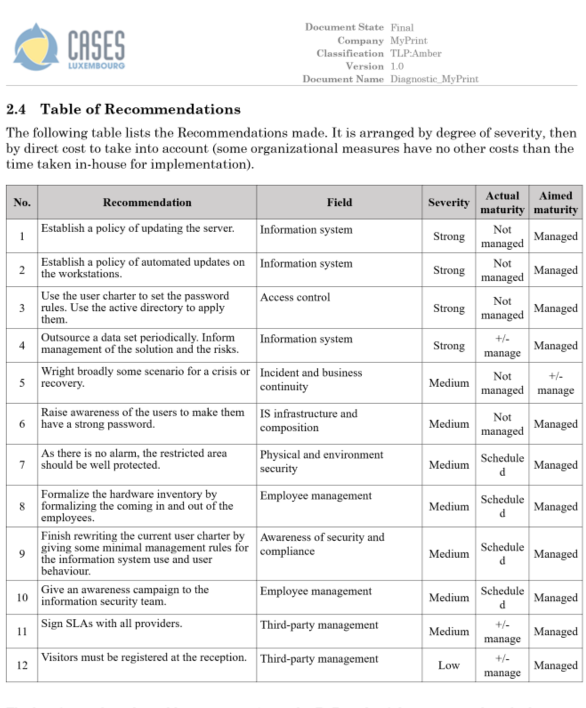
2.2 Maturity evolution

In the document, you can find on the Part 1.1 the free text in 'Information about organisation' and on 2.1 the free text in 'Summary of evaluation'.



2.3 Compliance in each security field

	Current	Aimed
Awareness of security and compliance	62%	100%
Employee management	85%	100%
Third-party management	83%	100%
Physical and environment security	90%	100%
Access control	29%	100%
IS infrastructure and composition	70%	100%
Information system	85%	100%
Incident and business continuity	33%	78%



2.4 Table of Recommendations

The following table lists the Recommendations made. It is arranged by degree of severity, then by direct cost to take into account (some organizational measures have no other costs than the time taken in-house for implementation).

No.	Recommendation	Field	Severity	Actual maturity	Aimed maturity
1	Establish a policy of updating the server.	Information system	Strong	Not managed	Managed
2	Establish a policy of automated updates on the workstations.	Information system	Strong	Not managed	Managed
3	Use the user charter to set the password rules. Use the active directory to apply them.	Access control	Strong	Not managed	Managed
4	Outsource a data set periodically. Inform management of the solution and the risks.	Information system	Strong	+/- manage	Managed
5	Wright broadly some scenario for a crisis or recovery.	Incident and business continuity	Medium	Not managed	+/- manage
6	Raise awareness of the users to make them have a strong password.	IS infrastructure and composition	Medium	Not managed	Managed
7	As there is no alarm, the restricted area should be well protected.	Physical and environment security	Medium	Schedule d	Managed
8	Formalize the hardware inventory by formalizing the coming in and out of the employees.	Employee management	Medium	Schedule d	Managed
9	Finish rewriting the current user charter by giving some minimal management rules for the information system use and user behaviour.	Awareness of security and compliance	Medium	Schedule d	Managed
10	Give an awareness campaign to the information security team.	Employee management	Medium	Schedule d	Managed
11	Sign SLAs with all providers.	Third-party management	Medium	+/- manage	Managed
12	Visitors must be registered at the reception.	Third-party management	Low	+/- manage	Managed

Graphics and tabs which were on the report screen could mostly be found on in the document. a .do

APPENDIX A : Notes Taken

Information to collect	Collected information	Current maturity				Recommendation	Aimed maturity	
		☑	±	◔	☒		☑	±
Awareness of security and compliance								
What security mechanisms already exist (other than technical mechanisms)?	A user charter is currently being written.			X		Finish rewriting the current user charter by giving some minimal management rules for the information system use and user behaviour.	X	
What is the core business? The most sensitive processes/items of information?	There is no department which availability criteria is crucial, even though some really confidential data are handled.	X					X	
What compliance obligations does the job involve?	There is no specific obligations.	X					X	
Compliance with legislation on personal data?	Some notification has been made to the CNPD. An update is planned for the GDPR.	X					X	
Employee management								
Is any hardware supplied to certain employees for work purposes?	Some hardware is supplied, like some computers for the meeting room. There are a lot of BYOD tablets which are blocked right now, but this will probably change. No inventory is kept, but there is a goal to have one sooner or later.			X		Formalize the hardware inventory by formalizing the coming in and out of the employees.	X	
Have staff members been on training courses recently?	INAP training is considered. A communication training is also planned.			X		Give an awareness campaign to the information security team.	X	
Does tele-working exist?	Only few people are tele-working, and	X					X	

SECURITY MADEIN.LU

7/11

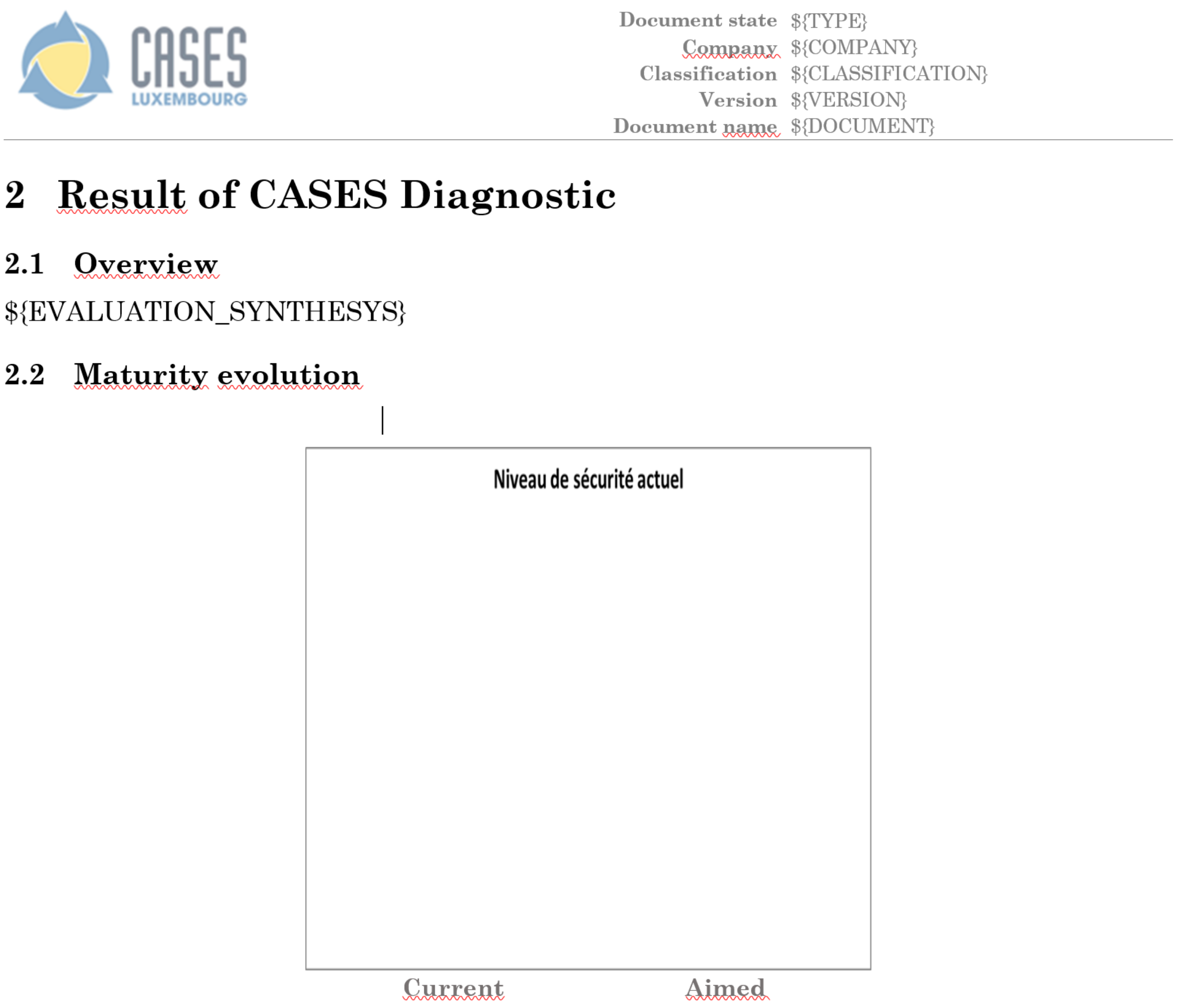
There is also a tab which contains the questions, the note taken, the recommendation and the current and target maturity.

Modify the template report

The template report is quite simple to understand. It can be found in : [*PATH_TO_DIAGNOSTIC*]/data/resources. There are some tags which corresponding to some fields in the diagnostic. You can find a complete list just below. Concerning the charts, some dummy pictures are in the document. Their name are "*image9.png*", "*image5.png*" and "*image10.png*".

```
//image
$container = new Container('diagnostic');
$this->setImageValue('image9.png', $container->bar);
$this->setImageValue('image5.png', $container->pie);
$this->setImageValue('image10.png', $container->radar);
```

And here is the dummy for the pie chart :


CASES LUXEMBOURG

Document state ${TYPE}
Company ${COMPANY}
Classification ${CLASSIFICATION}
Version ${VERSION}
Document name ${DOCUMENT}

2 Result of CASES Diagnostic

2.1 Overview

${EVALUATION_SYNTHESYS}

2.2 Maturity evolution

Niveau de sécurité actuel

Current Aimed

As you can also see, tags which can be modified in their order, or that could be just delete are under the form "*${TAGS}*". A complete list of the different existing tags can be found just below.

- **${CATEG_PERCENT_X}** *(Where X is a number under 1 to 8)* : The current percentage get in the category number X (Get automatically)
- **${CATEG_PERCENT_TARGET_X}** *(Where X is a number under 1 to 8)* : The aimed percentage get in the category number X (Get automatically)

- **${CLASSIFICATION}** : Indication to know where and how the document could be spread (Field get just before download the report)
- **${CLIENT}** : Name of the person who represents the company which has been the subject of the diagnostic (Field get just before download the report)
- **${COMPANY}** : Name of the company which has been the subject of the diagnostic (Field get just before download the report)
- **${CONSULTANT}** : Name of the security consultant or the company which has done the Diagnostic (Field get just before download the report)
- **${DATE}** : The date when is generated the report (Done automatically, depending on the server date)
- **${DOCUMENT}** : Name of the document (Field get just before download the report)Get automatically
- **${EVALUATION_SYNTHESYS}** : Some important conclusions of the diagnostic, or important information to underline (Field get on the last free-text field, "*Summary of evaluation*")
- **${ORGANIZATION_INFORMATION}** : Some information that is general on the company (Field get on the first free-text field, "*Information about organisation*")
- **${PRISE_NOTE_*Y_X*}** *(Where X is a number under 1 to 8 and Y is a number under 1 to 4)* : Contain a cross in the maturity Y for the current question in the category X (table of text)
- **${PRISE_NOTE_*Y_X*}** *(Where X is a number under 1 to 8 and Y is a number under 1 to 2)* : Contain a cross in the aimed maturity Y for the current question in the category X (table of text)
- **${PRISE_NOTE_CATEG_*X*}** *(Where X is a number under 1 to 8)* : The name of the category/security domain field number X (Get automatically)
- **${PRISE_NOTE_COLLECT_*X*}** *(Where X is a number under 1 to 8)* : The list of remarks corresponding to the question in the category number X (Recommendation field in a question, table of text)
- **${PRISE_NOTE_RECOMM_*X*}** *(Where X is a number under 1 to 8)* : The list of recommendation corresponding to the question in the category number X (Remarks field in a question, table of text)
- **${PRISE_NOTE_TO_COLLECT_*X*}** *(Where X is a number under 1 to 8)* : The list of questions in the category number X (Get automatically, table of text)
- **${RECOMM_CURR_MAT}** : The current maturity set before the recommendations is implemented (Field get when you choose actual maturity of any question, table of text)
- **${RECOMM_DOM}** : The category that concerns the recommendation (Get automatically, table of text, depending of where recommendations are found)
- **${RECOMM_GRAV}** : The gravity that concerns the recommendation (Field get when you choose the gravity, table of text)
- **${RECOMM_NUM}** : The position numbers of all the recommendations set (Get automatically, table of numbers, depending of the number of recommendations)
- **${RECOMM_TARG_MAT}** : The targeted maturity, set after the recommendation is implemented (Field get when you choose aimed maturity of any question, table of text)

- **${RECOMM_TEXT}** : The text all recommendations set (Field get when you put a recommendation to a question, table of text)
- **${STATE}** : State of the document, to know if it’s still a draft, or a final version (Field get just before download the report)
- **${VERSION}** : Versioning of the document (Field get just before download the report)