

User guide for CASES Diagnosis

Benjamin Joly

Version 1.0, 2017-09-19

First connection and Password change



DIAGNOSTIC CASES



Upload a file

Choisissez un fichier | Aucun fichier choisi

Upload

Create a diagnosis

Email address

Password

[Forgotten your password?](#)

Log in

2015 © CASES.LU - TOUS DROITS RÉSERVÉS.

BROUGHT TO YOU BY SECURITYMADEIN.LU

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.

Forgotten your password?

Email address

Receive e-mail

An e-mail will be sent to you at this address explaining how to change your password.

Note that the e-mail is only valid for 24 hours.

Then mail will be sent to you.

You have forgotten your password for the **CASES diagnosis**

To create a new password, please click on the button below:

[NEW PASSWORD](#)

If this e-mail does not concern you, please ignore this message

Cases

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.

New password

New password

.....

Confirm new password

.....

Change password

Then, you just need to create your first own diagnosis. For that, just log in to the main connection 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 won't 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 `[Path_to_Diagnostic]/scripts/changePassword.sh`

TIP

This script should be used only in a closed environment which does not have a network connection. This script needs to have the username of the user that wants to change his password. (Ex: `./changePassword.sh "diagnostic@cases.lu"`). The password needs to have at least a lower case, an upper case, a digit and a special char, and at least 8 characters.

Begin a diagnosis as a User

The screenshot shows the 'DIAGNOSTIC CASES' application interface. At the top left is the 'cases.lu' logo with the text 'Cyberworld Awareness and Security Enhancement Services LUXEMBOURG'. The title 'DIAGNOSTIC CASES' is centered at the top. On the top right, a red box labeled '1.' contains buttons for 'Administration', 'Log out', and language selection (FR and EN). Below the header, on the left, a red box labeled '2.' contains a file upload area with the text 'Choisissez un fichier | Aucun fichier choisi' and an 'Upload' button. Below this is a navigation panel labeled '3.' containing links: 'Information about organisation', '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', and 'Summary of evaluation'. At the bottom left, a red box labeled '4.' contains 'Report' and 'Export' buttons. On the right, a large text area labeled '5. Information about organisation' is shown. At the bottom right, a green 'Record and continue' button is visible.

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 diagnosis (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 Diagnosis (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 diagnosis, 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 Diagnosis, 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 to delete the question for this diagnosis.

WARNING

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

Choisissez un fichier Aucun fichier choisi

Upload

Information about organisation

Awareness of security and compliance

What security mechanisms already exist (other than technical mechanisms)? ✖

What is the core business? The most sensitive processes/items of information? ✖

What compliance obligations does the job involve? ✖

Compliance with legislation on personal data? ✖

➕ Add a question

Employee management

Have staff members been on training courses recently? ✖

Management of staff turnover? ✖

Are IT responsibilities (and possibly security responsibilities) defined? ✖

Is any hardware supplied to certain employees for work purposes? ✖

Does tele-working exist? ✖

➕ Add a question

Third-party management

Physical and environment security

Access control

IS infrastructure and composition

Information system

Incident and business continuity

Summary of evaluation

Report

Export

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 diagnosis. If you want to add a question for all your diagnoses, you should add it in the administration part.

Add a question

Question

Help

Upper threshold

▼

0

5

10

15

20

25

30

Add

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 10 and 5, then the maturity on a level is calculated this way: $((10/3 \times \text{maturity}) + (5/3 \times \text{maturity}))$ where the maturity could be 0 if not managed, 1 if more or less managed and 2 if managed. So if a policy is more or less managed about BYOD and the other question is managed, the category will be $((15/3 \times 1) + (10/3 \times 2)) = 5 + 6 = 11$ out of 16 (The maximal possible) of maturity for this category.

TIP

The maturity can also be not applicable, i.e. the question is not appropriate for the enterprise. Thereby, the question is not calculated in the final result.

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

Choisir un fichier

Aucun fichier choisi

Upload

Information about organisation

Awareness of security and compliance

What security mechanisms already exist (other than technical mechanisms) ✖

What is the core business? The most sensitive processes/items of information? ✖

What compliance obligations does the job involve? ✖

Compliance with legislation on personal data? ✖

Add a question

Employee management

Third-party management

Physical and environment security

Access control

IS infrastructure and composition

Information system

Incident and business continuity

Summary of evaluation

Report

Export

Awareness of security and compliance

What security mechanisms already exist (other than technical mechanisms)

Notes

A user charter is currently being written.

Maturity

Is there:

- a security policy?
- a user or administrator charter?
- procedures (e.g. back-up)?
- in-house instructions?
- etc

Maturity target

Recommendation

Finish rewriting the current user charter by giving some minimal management rules for the information system use and user behavior.

Importance

Record and continue

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, not managed and not applicable). You will also have some reminders 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.

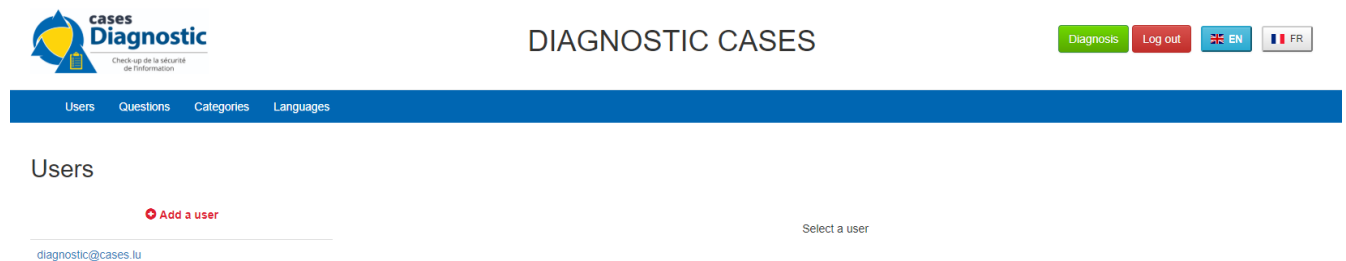
The recommendation panel is the place where you could just put what the company should do to have a better information security.

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

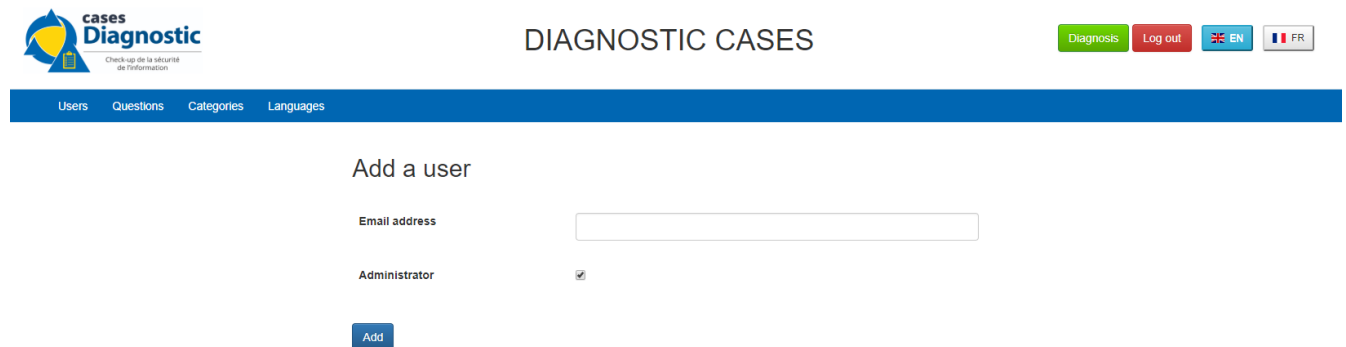
Administration Panel

Users Tab

You have six tabs (On the blue header), the first one is for Users, and then the other are Questions, Categories, Languages, Reports and Settings.

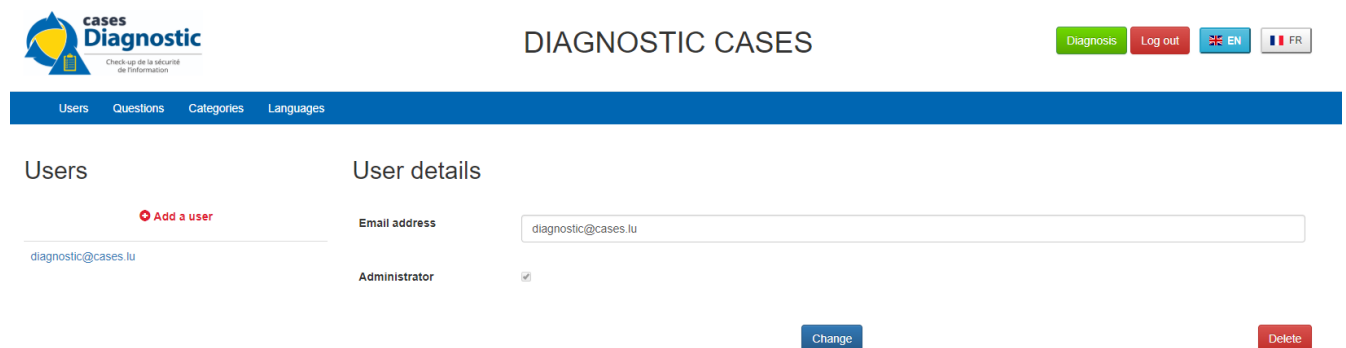


You can see all the mail addresses which are authorized to connect to the diagnosis. You can click on the **+ Add a user** button, so you can add a user.



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 Diagnosis, 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

Questions Screen

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



DIAGNOSTIC CASES

DiagnosisLog outENFR

UsersQuestionsCategoriesLanguages

Questions

[+ Add a question](#)

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.

Add a question

Translation key	<input type="text" value="__question33"/>
Translation 	<input type="text" value="Name of the question"/>
Help 	<input type="text" value="Main points to talk about"/>
Translation 	<input type="text" value="Nom de la question"/>
Help 	<input type="text" value="Points principaux à discuter"/>
Categories	<input type="text" value="Incident and business continuity"/>
Upper threshold	<div><div>▼</div><div><div>5</div><div>10</div><div>15</div><div>20</div><div>25</div><div>30</div></div></div>
<div>Add</div>	

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").

Then you have some fields in which you can translate your question and its help.

TIP

If you do not put translations, the name of the question will be the key you wrote above. You can choose to translate in one language and not in the others. Writing some help is optional, it depends on your needs.

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

Then, when you add your question, you will find it in every diagnosis you will do.

Incident and business continuity

Name of the question

Notes

Maturity

Maturity target

Recommendation

Importance

[Information about organisation](#)

[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](#)

Is any incident management in place? ☒

Is there a recovery plan ? ☒

Name of the question ☒

[Summary of evaluation](#)


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.


Change question

Translation key


__question1

Translation 


What security mechanisms already exist (other than technical mechanisms)

Help 

Is there:
a security policy?a user or administrator charter?

Translation 

Quels sont les mécanismes de sécurité existants (autres que techniques) ?

Help 

Existe-t-il ?
Une politique de sécuritéUne charte utilisateur ou

Categories

Awareness of security and compliance

Upper threshold

▼

5

10

15


20

25

30

Change

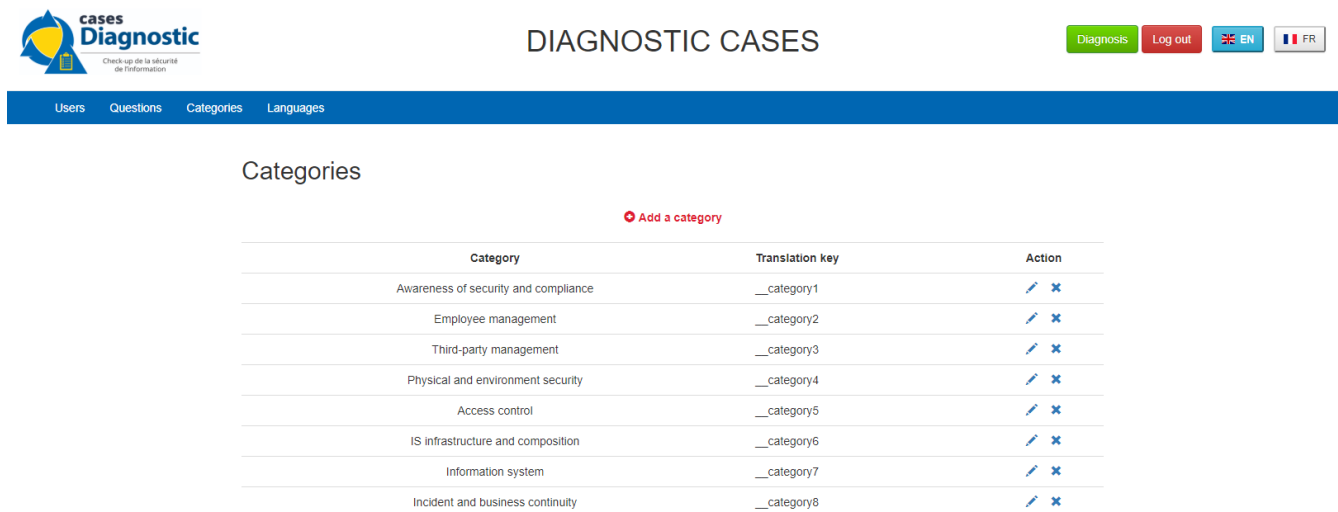
Delete a Question

















Just click on the blue cross () to definitely delete the question, with a confirmation message.



Categories Tab

Categories Screen

The third tab list all the default categories that will appear when you open a new Diagnosis.



Category	Translation key	Action
Awareness of security and compliance	__category1	 
Employee management	__category2	 
Third-party management	__category3	 
Physical and environment security	__category4	 
Access control	__category5	 
IS infrastructure and composition	__category6	 
Information system	__category7	 
Incident and business continuity	__category8	 

In the 'Category' column, you have all the categories that will appear. The translation key is mainly used to link categories through all languages. To finish, the 'action' column represents the possibility to edit the category (by clicking the pen ()) or delete it (by clicking the cross ()).

Add a Category

You can also add categories by clicking the red  **Add a category** button.

Add a category

Translation key

Translation 

Translation 

Add

The first field is for the translation key used by the PO file. The built-in category is done by giving two underscores, the tag "category" and the number of the category (For example, "__category9").

Then you have some fields in which you can translate your category.

TIP

If you do not put translations, the name of the category will be the key you wrote above. You can choose to translate in one language and not in the others.

Then, when you add your category, you will find it in every diagnosis you will do, as long as it contains at least one question.

Choisir un fichier | Aucun fichier choisi | Upload

Name of the category
Name of the question

Notes

Maturity

Maturity target

Recommendation

Importance

Record and continue

Report | Export

Change a Category

By editing, you will get on a similar interface as if you were adding a category. You can change details on the same ways.

Change category

Translation key

Translation

Translation

Change


Delete a Category

Just click on the blue cross () to definitely delete the category, with a confirmation message.

Languages Tab

Languages Screen

The fourth tab list all the default translations that exist when you open a new Diagnosis.

 **DIAGNOSIS CASES** Diagnosis Log out EN FR

Users Questions Categories Languages

Languages Add a language ad Add Delete

Translation key	Translation	Reference translation en OK	Action
__diagnostic	<input type="text" value="Diagnosis"/>	Diagnosis	Change Delete
__welcome	<input type="text" value="Welcome to CASES Diagnostic"/>	Welcome to CASES Diagnostic	Change Delete
__welcome_upload	<input type="text" value="Upload a file"/>	Upload a file	Change Delete
__welcome_login	<input type="text" value="Create a diagnosis"/>	Create a diagnosis	Change Delete
__file_to_upload	<input type="text" value="File to upload"/>	File to upload	Change Delete
__upload	<input type="text" value="Upload"/>	Upload	Change Delete
__login	<input type="text" value="Log-in"/>	Log-in	Change Delete
__password	<input type="text" value="Password"/>	Password	Change Delete
__log_in	<input type="text" value="Log in"/>	Log in	Change Delete
__email	<input type="text" value="Email address"/>	Email address	Change Delete
__logout	<input type="text" value="Log out"/>	Log out	Change Delete
__password_forgotten	<input type="text" value="Forootten your oassword?"/>	Forgotten your password?	Change Delete

In the ‘Translation’ column, there is the name of the translation keys, translated in the current language. You can modify it directly by changing its text and then click the green button ‘Change’ on the same line. You can also delete a translation by clicking the green button ‘Delete’.

The third column is the Reference translation and will be useful when you translate another language.

Add a Language

Indeed, at the top right of the page, you can add another language by selecting its code country and clicking the green button ‘Add’. You can also delete a language selected by clicking the button ‘Delete’.

Add a language de Add Delete

When the new language is added, a new button is created at the top right corner of the page, with the flag of the language chosen. You can click on the button.

__languages

__add_a_language ad __add __delete

__translation_key	__translation	__translation_ref	en fr de	OK	__action
__diagnostic		Diagno			__modify __delete
__welcome		Welcome to CASES Diagnostic			__modify __delete
__welcome_upload		Upload a file			__modify __delete
__welcome_login		Create a diagnosis			__modify __delete
__file_to_upload		File to upload			__modify __delete
__upload		Upload			__modify __delete
__login		Log-in			__modify __delete
__password		Password			__modify __delete
__log_in		Log in			__modify __delete
__email		Email address			__modify __delete
__logout		Log out			__modify __delete
__password_forgotten		Forgotten your password?			__modify __delete

As you can see, the translation column is empty, and you can then fill in translations as you want to. The Reference translation may help you filling translations, as you can choose a language to support you.

At the end of the page, you have two buttons which are 'Add a translation' and 'Change all translations'.

The two given tokens do not match The two given tokens do not match The two given tokens do not match

Change Delete

Add a translation Change all translations

'Change all translations' allows you to change multiple translations so that you do not have to change one by one all the translations. 'Add a translation' is for adding a translation.

TIP

Normally you won't use this last feature, unless you want to change the code of the application and you need another translation.

Add a Translation

Ajouter une traduction

Clef de traduction

__newKey

Traduction 

Name of the translation

Traduction 

Nom de la traduction

Ajouter

The first field is for the translation key used by the PO file. You can put the key you need to translate.


Then you have some fields in which you can translate your translation.

TIP If you do not put translations, the name of the translation will be empty.

Templates Tab

Templates Screen

The fifth tab list all the default report templates that exist when you open a new Diagnosis.

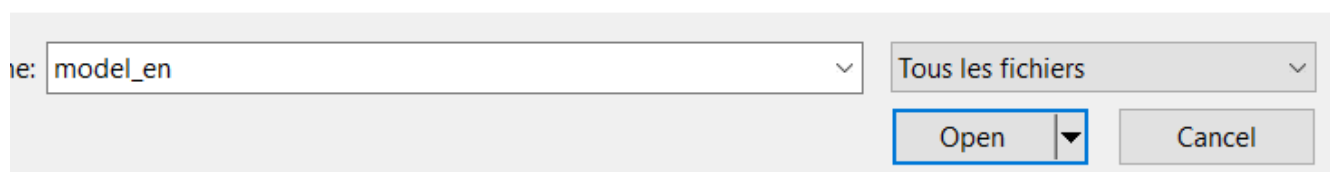
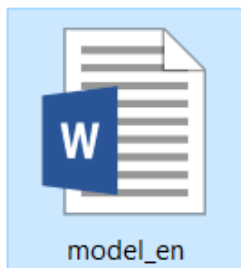


Template	Last modification	Action
model_en	June 15 2018 08:52:26 by diagnostic@cases.lu	Download
model_fr	June 15 2018 08:52:23 by diagnostic@cases.lu	Download

[Choisir un fichier](#) | Aucun fichier choisi [Upload](#)

In this tab you can download all the actual templates in order to modify them.

After modifying them, it is possible to upload them if you want to apply changes in the diagnosis.



File name: ▼ Files of type: ▼

[Open](#) ▼ [Cancel](#)

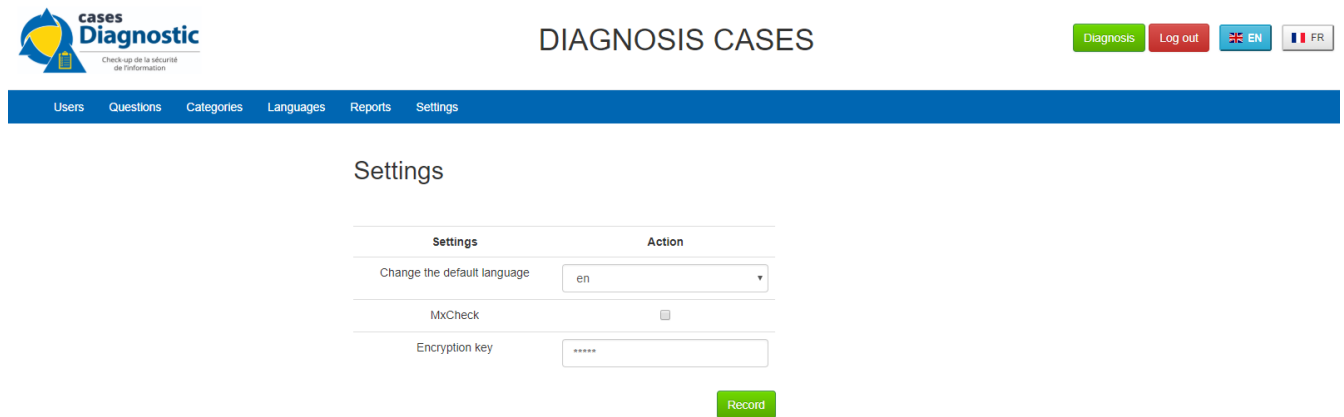
WARNING

The uploaded template must have the same name that in the diagnosis.

Settings Tab

Settings Screen

The sixth tab list all the settings you can modify in the diagnosis.



Settings	Action
Change the default language	en
MxCheck	<input checked="" type="checkbox"/>
Encryption key	*****

Record


In this tab you can modify the default language (The one which is used when you open a diagnosis), the MxCheck (When this option is activated, it forces you to verify your mail address to enter a diagnosis) and the encryption key (Its strength).

TIP

After getting again in the settings tab, all the settings will be set by default but all the modifications will be updated.

Resume or finish a Diagnosis

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




data_20170602134259.cases
17,3 Ko — 10.0.0.2 — 13:43





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 diagnosis. The first one, at the connection screen, you doesn't need to have an account to go on it.



DIAGNOSTIC CASES

Upload a file

Choisissez un fichier

Aucun fichier choisi

Upload

Create a diagnosis

Email address

Password

Forgotten your password?

Log in

2015 © CASES.LU - TOUS DROITS RÉSERVÉS.

BROUGHT TO YOU BY SECURITYMADEIN.LU

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.

Parcourir...

Demo_MyPrint_English_v0.1bJo.cases

Upload

Information about organisation

- [Information about organisation](#)
- [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](#)
- [Summary of evaluation](#)

Information about organisation

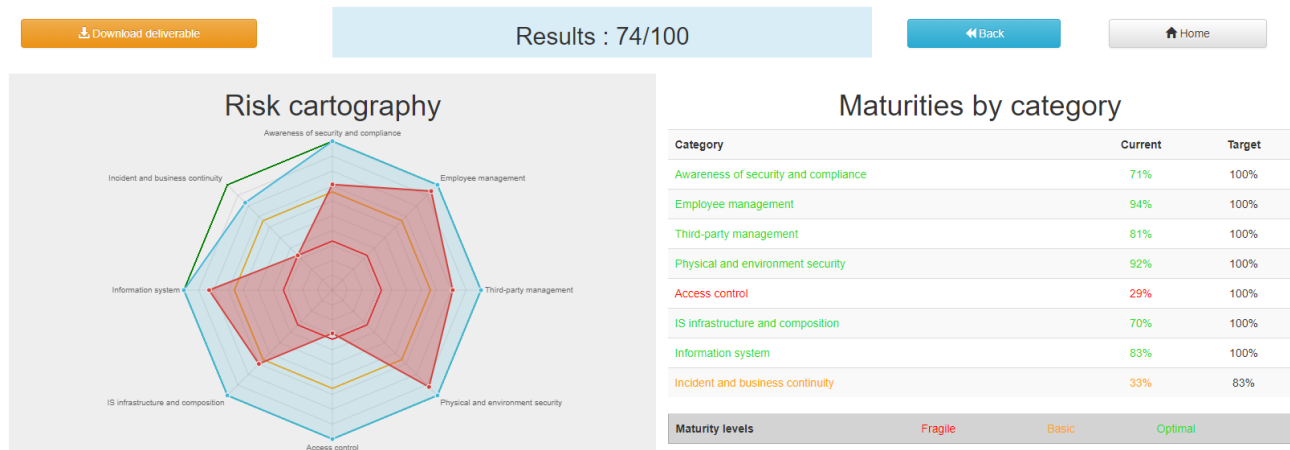
MyPrint is a print shop, which has 150 employees. It has a variety of technologies and possibilities of printing (rotary presses, offset, calligraphy, lasers, etc.) which give a lot of different services and clients from many different sectors. Firstly, the company is not targeting any certification; 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.

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 Diagnosis.

Report

Online Report

You can access to the screen report by just clicking on the yellow button [Report](#). You can also get this screen without being connected, but you will not be able to download the report as a '.docx'.



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. The colors determine the level of maturity of each category (red when maturity is under 33%, orange between 33% and 66% and green over 66%). You will also find the recommendation tab which briefly summarizes the recommendations, their gravity and their current and target maturity.

Recommendations

Recommendation	Category	Importance	Goal
Use the user charter to set the password rules. Use the active directory to apply them.	Access control	● ● ●	✗ → ✓
Establish a policy of automated updates on the workstations.	Information system	● ● ●	✗ → ✓
Establish a policy of updating the server.	Information system	● ● ●	✗ → ✓
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	● ●	± → ✓
Sign SLAs with all providers.	Third-party 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	● ●	± → ✓
Formalize the hardware inventory by formalizing the coming in and out of the employees.	Employee management	● ●	± → ✓
Give an awareness campaign to the information security team.	Employee management	● ●	± → ✓
Visitors must be registered at the reception.	Third-party management	●	± → ✓

Maturity levels

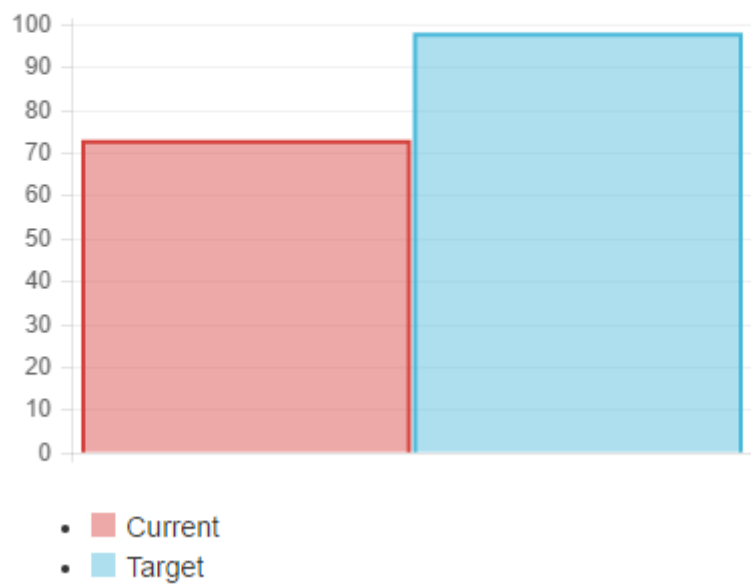
✗	Fragile	±	Basic	✓	Optimal
---	---------	---	-------	---	---------

Importance levels

●	Low	● ●	Medium	● ● ●	Strong
---	-----	-----	--------	-------	--------

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

Evolution of maturity



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

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.'

Document name

Diagnostic_MyPrint

Company

MyPrint

Version

1.0

State

Final ▼

Classification

TLP:Amber

Consultant

Benjamin Joly

Client

MyPrint

⬇ Download deliverable

⬅ Back to report

You will need to put a Document Name, the company which is concerned by the Diagnosis, the version of the document (If there are multiple Diagnoses, or if you want to correct it...), a choice if it's a draft or a final version of the Diagnosis, 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

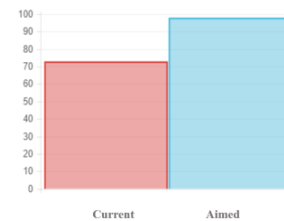
The figure below presents the various sectors covered by the assessment. It should be noted

2 Result of CASES Diagnostic

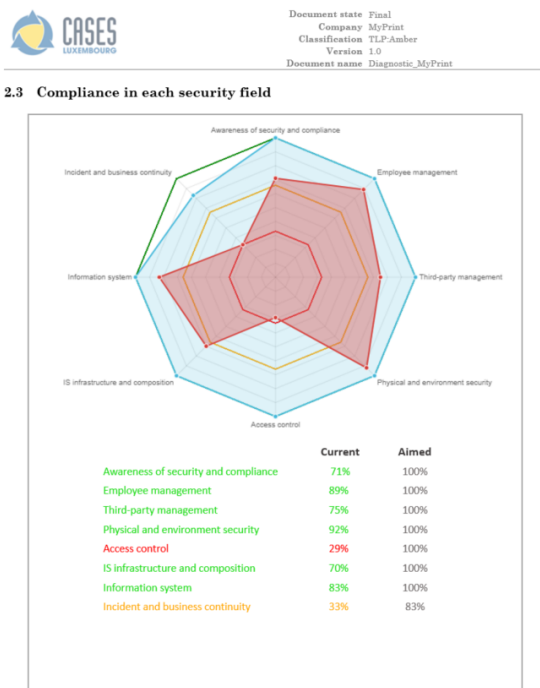
2.1 Overview


The maturity level 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 organization' and on 2.1 the free text in 'Summary of evaluation'.





Document state: Final

Company: MyPrint

Classification: TLP-Amber

Version: 1.0

Document name: Diagnostic_MyPrint

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).

Details of the scores used as the basis for the recommendations are given in appendix A.























Legend of the table of recommendations

Each recommendation has their importance level:

- : Really important risk which needs an emergency care.
- : Important risk which need some care sooner or later.
- : Minor risk or advice that could make a better level of security.

Nr	Recommendation	Domain	Importance	Current maturity	Maturity target
1	Use the user charter to set the password rules. Use the active directory to apply them.	Access control	●●●	Fragile	Optimal
2	Establish a policy of automated updates on the workstations.	Information system	●●●	Fragile	Optimal
3	Establish a policy of updating the server.	Information system	●●●	Fragile	Optimal
4	Outsource a data set periodically. Inform management of the solution and the risks.	Information system	●●●	Basic	Optimal
5	Wright broadly some scenario for a crisis or recovery.	Incident and business continuity	●●	Fragile	Optimal
6	Raise awareness of the users to make them have a strong password.	IS infrastructure and composition	●●	Fragile	Optimal
7	As there is no alarm, the restricted area should be well protected.	Physical and environment security	●●	Basic	Optimal
8	Sign SLAs with all providers.	Third-party management	●●	Basic	Optimal
9	Finish rewriting the current user charter by giving some minimal management rules for	Awareness of security and	●●	Basic	Optimal

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

Information to collect	Collected information	Current maturity				Recommendation	Maturity target	
								
Awareness of security and compliance								
What security mechanisms already exist (other than technical mechanisms)	A user charter is currently being written.					Finish rewriting the current user charter by giving some minimal management rules for the information system use and user behaviour.		
What compliance obligations does the job involve?	There is no specific obligations.							
Compliance with legislation on personal data?	Some notification has been made to the CNPD. An update is planned for the GDPR.							
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.							
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.					Formalize the hardware inventory by formalizing the coming in and out of the employees.		
Have staff members been on training courses recently?	INAP training is considered. A communication training is also planned.					Give an awareness campaign to the information security team.		
Management of staff turnover?	There is almost no staff turnover.							
Are IT responsibilities (and possibly security responsibilities) defined?	There is a specific post for IT responsibilities.							

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

Contents in the template report

There are some tags which corresponding to some fields in the diagnosis. 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 :



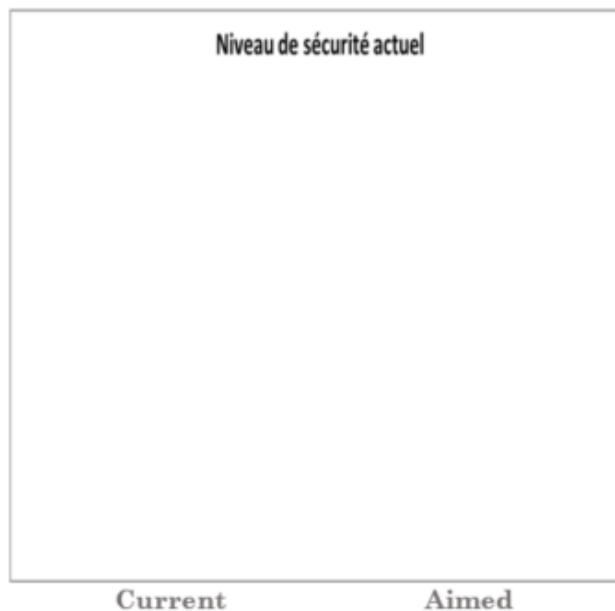
Document state \${TYPE}
Company \${COMPANY}
Classification \${CLASSIFICATION}
Version \${VERSION}
Document name \${DOCUMENT}

2 Result of CASES Diagnostic

2.1 Overview

\${EVALUATION_SYNTHESES}|

2.2 Maturity evolution



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

- **\${CATEG_PERCENT}** : The current percentage got in the categories (Got automatically)
- **\${CATEG_PERCENT_TARG}** : The aimed percentage got in the categories (Got automatically)

- **`\${CLASSIFICATION}`** : Indication to know where and how the document could be spread (Field got just before download the report)
- **`\${CLIENT}`** : Name of the person who represents the company which has been the subject of the diagnosis (Field got just before download the report)
- **`\${COMPANY}`** : Name of the company which has been the subject of the diagnosis (Field got just before download the report)
- **`\${CONSULTANT}`** : Name of the security consultant or the company which has done the Diagnosis (Field got just before download the report)
- **`\${DATE}`** : The date when is generated the report (Done automatically, depending of the server date)
- **`\${DOCUMENT}`** : Name of the document (Field got just before download the report)
- **`\${EVALUATION_SYNTHESES}`** : Some important conclusions of the diagnosis, or important information to underline (Field got on the last free-text field, "*Summary of evaluation*")
- **`\${LEGEND_PIE}`** : The legend of the pie chart which contains all the categories (Got automatically)
- **`\${NOTES_TABLE}`** : The table which contains all the notes, maturity, recommendation of each questions (Got automatically)
- **`\${ORGANIZATION_INFORMATION}`** : Some information that are general on the company (Field got on the first free-text field, "*Information about organization*")
- **`\${PRISE_NOTE_CATEG}`** : The name of the categories/securities domain field (Got automatically)
- **`\${RECOMMENDATION_TABLE}`** : The recommendation table (Got automatically)
- **`\${STATE}`** : State of the document, to know if it's still a draft, or a final version (Field got just before download the report)
- **`\${TYPE}`** : State of the document, to know if it's still a draft, or a final version (Field got just before download the report, other font text)
- **`\${VERSION}`** : Versioning of the document (Field got just before download the report)