EBIOS Risk Manager report

EBIOS case study using the EBIOS Risk Manager guide

Thomas Gregoire
Bastien Levasseur
Théophane Paradis
Marc Sanchez

Lecture and lab given by Rémi KOUBY & Florent AUTRÉAU

Contents

I Introduction

The goal of this workshop is to create an EBIOS Risk Manager and risk analysis report for a given case study.

The context is during the COVID-19 pandemic, the French government required all pharmacies that were conducting tests to report their results and the identities of the individuals tested to the Assurance Maladie. The company *TestAntiCovid-France* developed a solution to automate the submit process. It was adopted by all pharmacies.

It was revealed that TestAntiCovidFrance stored all their results in an insecure manner, using Google Drive and hard-coding credentials into the software.

In response to this incident, the French Ministry of Health and Access to Care established a new protocol to transmit test results. To avoid repeating the same mistakes, we must assess the security of the new protocol using the EBIOS Risk Manager method.

The new protocol is as follows :

Pharmacies make COVID tests and have their own server to store their results.A TestAntiCovidFrance module is installed on all servers, it sends test results to a TestAntiCovidFrance server over the Internet. TestAntiCovidFrance's server is hosted by AWS. The INEXUM corporation is in charge of the exploitation.

Finally, the TestAntiCovidFrance servers send the data to the Assurance Maladie server hosted by themselves.

Access between servers is done with usernames and passwords. No password policy has been defined. TestAntiCovid-France's server is running on Debian 8.

For this workshop, our reference will be the lecture slides and the *EBIOS Risk Manager* guide[1].

[1] EBIOS Risk Manager guide : `https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide`

II Workshop 1 : Define case study and feared events

II.A Define the case study

Our main goal is to ensure the availability of the test results, to allow politicians to make decisions according to the figures. The confidentiality of the results and the health data of the people is also important, as we don't want to repeat the same mistakes as last time. The integrity of the data is also important but we can have some false data as long as the overwhelming majority is correct.

To protect the data we must protect each stakeholder that handles it, and also protect the communication between stakeholders since we use the Internet, an insecure channel.

II.B Business and technical perimeter

We start by defining the business values, that is everything that holds value, whenever it is informational property or the main functionalities of the protocol.
We define the following business values :

Business values			
Name :	**Type of business value :**	**Description :**	**Responsible entity :**
Results of tests	Information	The results from the tests and the identity of the person	Pharmacies are responsible to ensure the test integrity
Possibility to add results	Processus	Add test results to the TestAntiCovidFrance server	TestAntiCovidFrance are responsible for their server
Possibility to send results	Processus	Send the results to the Assurance Maladie server	TestAntiCovidFrance are responsible for their server
Possibility to consult results	Processus	See the test results from the Assurance Maladie server	Assurance Maladie are responsible for their server

Our business values are the tests themselves and the actions on them, mainly, adding tests, sending them and consult them.

Then we define the supporting assets, which are the tangible assets that holds our business values, machines, network or software.
We define the following supporting assets :

Supporting assets		
Name :	**Description :**	**Responsible entity :**
TestAntiCovidFrance Database	Handle test results from all the pharmacies	Database is handled by INEXUM and hosted by AWS
Assurance Maladie's FTP server	Handle test results from all the pharmacies	Assurance Maladie are responsible for their server
TestAntiCovidFrance AWS servers	Hosts the TestAntiCovidFrance server	AWS are responsible for their hosting
TestAntiCovidFrance Module	Automatically sends the data to the TestAntiCovidFrance server	TestAntiCovidFrance are responsible for their module
Internet	Enable sharing the results through the network	ISPs

The supporting assets are all the hardware software in the protocol, plus the Internet used to transfer data.

II.C Feared events

Then we define the feared events, which are events that can negatively impact the CIA attributes (Confidentiality, Integrity, Availability) of the business values.
We use the following scale to rate the gravity for each feared event, it comes from the official *Méthode EBIOS Risk Manager* guide, page 26 :

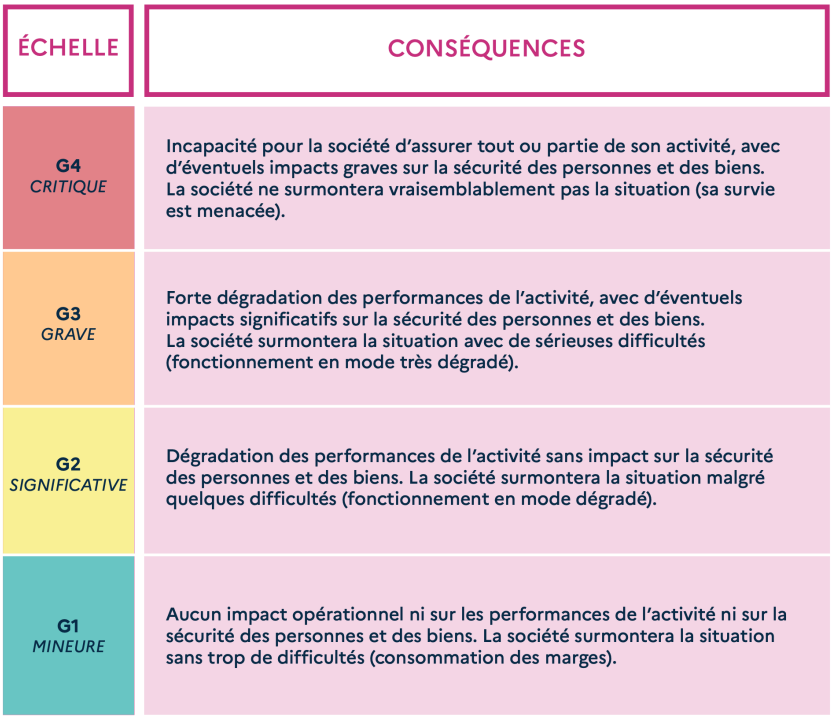

Figure 1: The gravity scale used to measure our feared events

We define the following feared events :

Feared events			
Business value	**Feared Event**	**Impact**	**Gravity**
Add test results	Unable to add results *Harms Availability*	Update of results impossible Loss of trust Financial loss	4
	Someone else than a pharmacy adds new results *Harms Integrity*	False results added may lead to bad decisions Fraud from the pharmacies	2/3
Consult test results	All test results are leaked *Harms Confidentiality*	Loss of citizen trust in the application Loss of state reputation Financial loss	4
	Some test results are leaked *Harms Confidentiality*	Small loss of citizen trust in the application Small financial loss	1
	Some test results are false *Harms Integrity*	As long as the false test results remain a insignificant part, it should be manageable, but false test results leads to wrong decisions	1
	A large part of test results are false *Harms Integrity*	A significant part of the test results are false, it will lead to wrong decisions Loss of trust if its revealed Financial loss	4

There is no Confidentiality issue for the functionality of adding new results, because it does not make sense by definition. There is also no Availability issue for consulting test results.
The feared events compromising availability have the highest gravity. All events that affect a large part of the results are also considered critical.

We make a distinction between a *small* and *large* part of false test results. A very small portion of false test shouldn't impact the decisions taken, but a large proportion of false tests will inevitably lead to wrong decisions. A statistically

significant portion of tests can be considered to be around 1%.
According to the French ministry, there were around 168 millions of tests in 2021[2], so less than 1.5 millions of false tests can be considered insignificant.

II.D Determine the security base

In this section we want to define the security base, that is a list of measures taken to ensure a baseline for the security of the protocol. It can be security protocols, encryption standards, standards...

Security base	
Category	**Proposed measures**
Standards	GDPR, ISO 27001, ISO 27002, HDS
Authentication	At least single authentication factor to access the test results. Preferably MFA
Communication protocols	TLS (preferably 1.3, at least 1.2)
Backups	Each party should have a backup of their data

To handle health data in France, we must obtain the HDS (Hébergeurs de Données de Santé) certification. As we are operating in Europe, we must comply with the GDPR (General Data Protection Regulation). Finally, we also comply with the ISO 27001 & ISO 27002, two standards widely used to manage information security within organizations.
Each party in the protocol should backup their data, especially the Assurance Maladie were all tests are sent. They should use the 3-2-1 backup strategy, 3 copies of the data, on 2 different medias, with 1 backup offsite.

To go further, it would be advisable to cipher the data handled by each party, it will prevent the leakage of the medical data in plain text. Still, the info were stolen, but no one should be able to read them, a big improvement over the usual database leaks that occurs on a regular basis.

[2]Bilan 2022 du dépistage Covid-19 : `https://drees.solidarites-sante.gouv.fr/delais-covid19-2023-02-02`

III Workshop 2 : Define risk sources and targeted objectives

III.A Identify risk sources and targeted objectives

The risk sources are the entities that can do potential damage. They have a targeted objective, something that they benefit by harming us.

We define the following risk sources and their targeted objectives :

Risk sources	
Risk source	**Targeted objectives**
Hacktivists	Sabotage, show their dissatisfaction with the state. Or pure boredom from the pandemic.
Competing company	Strategic move, show that it would be better to give them the contract instead.
State threat	Ruin the reputation of the country or the government in place.
Ordinary citizen	Take advantage of the system, just to go somewhere despite being infected.

Our risk sources are ranging from simple citizens to states. We will see that, obviously, citizens are less threatening than states or corporations.

III.B Evaluate the couples Security risk/Targeted objectives

To evaluate the couples we use this scale, it comes from the EBIOS lecture slides, page 59 :

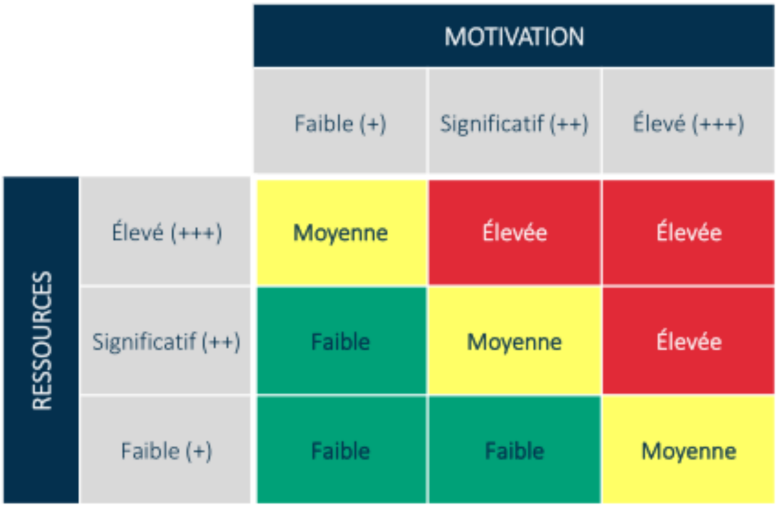

Figure 2: The scale used to correlate motivation and resources

We evaluate the couples :

Risk sources and their motivation					
Sources of risk :	**Objectives targeted :**	**Motivation :**	**Resources :**	**Relevance :**	**Retained couple :**
Hacktivists	Show their discontent by disrupting the information system	++	++	Middle	Yes
Competing Company	Destroy the current informatic system to show that it would be better to give them the contract instead (Financial loss)	+	++	Low	No
State Threat	Ruin the reputation of the country or the government in place	+	+++	Middle	Yes
Ordinary Citizen	Take advantage of the system	+++	+	Middle	Yes

We note that ordinary citizens are highly motivated to take advantage of the system. Some of them really want to go out despite the pandemic. Fortunately they have very little resources.
We do not keep the competing company. We suppose the competing companies do not care about the contract. The hacktivists be as harmful as the competing companies, with increased motivation.

IV Workshop 3 : Identify stakeholders

IV.A Identity stakeholders of the ecosystem

We define the stakeholders of the ecosystem, the entities that have an interest in the whole project, either because they are participating or they have an investment.
We define the following stakeholders :

Stakeholders :
Pharmacies
Assurance Maladie
TestAntiCovidFrance
INEXUM Technical Administrators
AWS (Amazon Web Service)
French government

The French government are a stakeholder, they commissioned the project.

To assess these stakeholders, we will base ourselves on 4 criteria :

- **Dependence:** Is the relationship with this stakeholder vital to the project?
- **Penetration:** To what extent does the stakeholder access the internal resources?
- **Cyber maturity:** What are the stakeholder's capabilities in terms of cybersecurity?
- **Trust:** Can the stakeholder's intentions or interests be contrary to me?

Each of these criterion will be assessed from 1 (weak) to 4 (strong) using this table it comes from the EBIOS lecture slides, page 102:

Dépendance	Pénétration	Maturité cyber	Confiance
1 : Relation non nécessaire aux fonctions stratégiques	1 : Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, etc.).	1 : Des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	1 : Les intentions de la partie prenante ne peuvent être évaluées.
2 : Relation utile aux fonctions stratégiques	2 : Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	2 : Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	2 : Les intentions de la partie prenante sont considérées comme neutres.
3 : Relation indispensable mais non exclusive	3 : Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	3 : Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	3 : Les intentions de la partie prenante sont connues et probablement positives.
4 : Relation indispensable et unique (pas de substitution possible à court terme)	4 : Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	4 : La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.	4 : Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

Figure 3: The scale used to measure the different criteria

The threat level is calculated with the following formula : $\frac{Dependency * Penetration}{CyberMaturity * Trust}$.

Stakeholders criteria					
Stakeholder :	**Dependency :**	**Penetration :**	**Cyber maturity :**	**Trust :**	**Threat level :**
Pharmacies	2	2	1	3	1.333
Assurance Maladie	4	4	3	4	1.333
TestAntiCovidFrance	4	4	2	3	2.666
Indexum Technical administrators	3	4	3	3	1.333
AWS (Amazon Web Services)	4	1	4	4	0.250
French government	4	4	4	4	1

We'll take an example with pharmacies :

- **Dependency :** The application does relies on pharmacies, but some of them can fail impacting the protocol → 2
- **Penetration :** Pharmacies still have access to their information, but not the information of other pharmacies. → 2
- **Cyber maturity :** The interview made it clear that pharmacies have some very rudimentary cybersecurity measures → 1
- **Trust :** Pharmacies can be trusted, but sometimes they may produce fake results → 3
- **Threat Level :** $\frac{(2*2)}{(1*3)} \approx 1.333$

A few notes on some critera :

- Pharmacies have a mid dependency, if all pharmacies of the country cease to operate, the whole system crumbles, but it shouldn't happen. If some pharmacies fails, it's acceptable.
- TestAntiCovidFrance have a mid cyber maturity due to their previous scandals.
- We are hosting our data on AWS but we give them a penetration of 1, according to their Data Privacy FAQ[3], *"We do not access or use your customer content for any purpose without your agreement"*. We can trust fully trust AWS, it's the largest leader in cloud services after all.
- We decided to put the penetration of the government at 4. They do have access to the data but it's the Assurance Maladie job to access it. It affects negatively their threat level.
- The threat level of the French government should be lower than AWS. We can argue that the cyber maturity and trust level could be higher than 4, lowering the trust level to nearly zero.

[3]AWS Data privacy FAQ : `https://aws.amazon.com/compliance/data-privacy-faq/?nc1=h_ls`

IV.B Develop strategic scenarios

We are interested in the following risk sources / targeted objectives pairs :

- Hacktivists that want to sabotage the information system to show their dissatisfaction.
- A state that wants to ruin the reputation of a government to discredit it.
- A citizen that wants to take advantage of the system by modifying his test results.

We define the following strategic scenarios :

Scenario 1 : An ordinary citizen attacks the pharmacies :
Pays the pharmacist to falsify the results of their test.

Scenario 2 : An hacktivist attacks the Assurance Maladie :
Performs a Denial of Service on the TestAntiCovidFrance or the Assurance Maladie server.

Scenario 3 : An hacktivist attacks the Assurance Maladie :
Create a new pharmacy with only the installer, send a lot of false results to have an impact on the national average.

Scenario 4 : A state directly attacks TestAntiCovidFrance :
Gains access to the database, steals or modifies the results.

There are many more scenarios but we stick to a few simple ones that are reasonable. The french government and AWS are not a targeted stakeholder because there are weaker targets (TestAntiCovidFrance or the Assurance Maladie).

IV.C Defining security measures on the ecosystem

To protect ourselves against these attack paths, we establish some basic security measures. We will go further in section VI.C.
We define the following security measures and threat level for each attack path :

Security measures and threat level				
Targeted stakeholder :	**Attack path :**	**Security measure :**	**Initial threat level :**	**Residual threat level :**
Pharmacies	Falsification of test results	Awareness campaign	1.333	1.333
Assurance Maladie	Denial of service	Anti-DoS protection	1.333	1
TestAntiCovidFrance	Creation of fake pharmacies	More information to establish a pharmacy, than just the installer	2.666	2
TestAntiCovidFrance	Direct attack on servers	Database encryption	2.666	2

V Workshop 4 : Operational scenarios

V.A Defining operational scenarios

Operational scenarios are a detailed sequence of all the actions made by an risk source to accomplish their attack path. We define the following operational scenarios for each attack path :

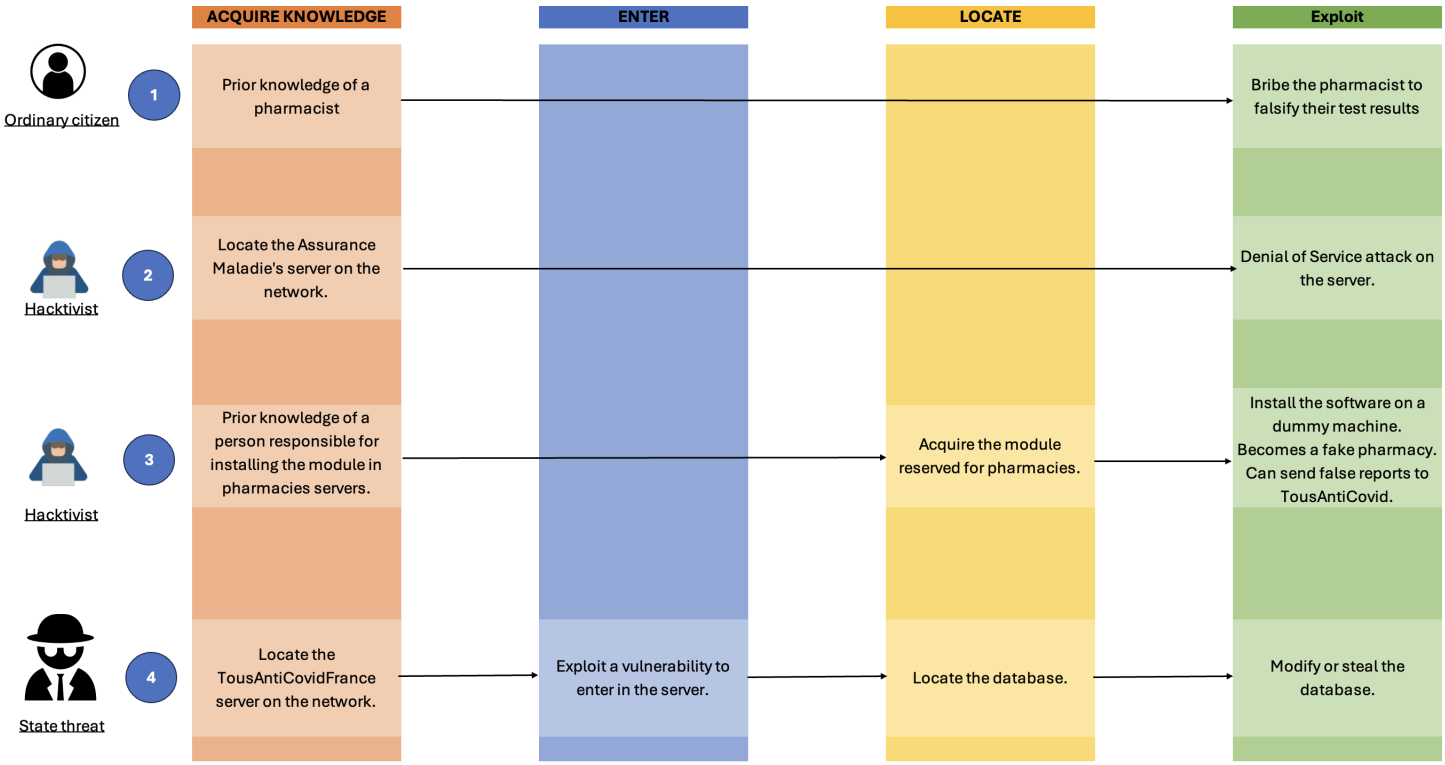

Figure 4: The operational scenarios for each attack path
Note: The numbers represent the the scenario number defined in section IV.B.

We note that the operational scenarios for the ordinary citizen and the hacktivist are very simple. It doesn't take much to bribe its pharmacist (even if the success rate can be questionable). Conduction a Denial of Service attack is very simple, the hacktivist just have to learn the address of the servers, which are visible on the network. Gathering the network resources to conduct the attack is also trivial.

Getting access to the servers is much harder, but states have plenty of resources.

V.B Defining likelihood scale

For each attack path, we asses a likelihood, how well the attack path can actually happen.
We use the following scale, it comes from the official *Méthode EBIOS Risk Manager* guide, page 66 :

ÉCHELLE	DESCRIPTION
V4 *quasi certain*	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 *Très vraisemblable*	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 *Vraisemblable*	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 *Peu vraisemblable*	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

Figure 5: The likelihood scale used to measure each attack path

We define the following likelihood for each attack path:

- **Scenario 1 :** Bribing the pharmacist → Level 4
- **Scenario 2 :** Denial of service → Level 3
- **Scenario 3 :** Create a false pharmacy → Level 2
- **Scenario 4 :** Steal or modify the database → Level 2

The likelihood of bribing a pharmacist is 4. With the 168 millions test conducted, statistically someone managed to bribe their pharmacist. Still, it should be taken with precaution, the success rate is very low, this explains the threat level at 1 defined in section IV.C.

Denial of Service will manage to hurt the entities with certainty. But the likelihood is not very high. So we keep the likelihood at 3.

Creating a false pharmacy is somewhat easy if one can get access to the installation software. But it shouldn't happen often enough to be statically significant.

Steal or modify the database will definitely hurt the entities, but the likelihood is not that significant.

VI Workshop 5 : Handle risk

VI.A Synthesis of risk scenarios

We make a synthesis of the different risk scenarios, their gravity and their likelihood.

Synthesis of risk scenarios					
Risk source :	**Targeted objectives :**	**Attack path :**	**Gravity :**	**Operating modes :**	**Likelihood :**
Ordinary citizen	Personal gain	Prior knowledge of a pharmacist. Bribe them.	1	Bribe the pharmacist to falsify the results	4
Hacktivist	DoS TousAntiCovid server.	Denial of service	3	Locate the server, make a DoS attack.	3
	Sabotage the system.	Acquire the installation software, make a fake pharmacy	2	Fetching the installer. Putting it on a machine. Sending fake results.	2
State threat	Ruin the reputation of the country	Steal the database	4	Locate and enter into the server by exploiting vulnerabilities, steal or modify the database.	2

VI.B Handle risk

We use the following risk levels to define if we should take actions or not for each risk scenarios, it comes from the official *Méthode EBIOS Risk Manager* guide, page 74 :

NIVEAU DE RISQUE	ACCEPTABILITÉ DU RISQUE	INTITULÉ DES DÉCISIONS ET DES ACTIONS
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme
Élevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé

Figure 6: Risks levels to be used for each risk scenarios

We define the following risk level for each risk scenario :

- **Scenario 1 :** Bribing the pharmacist → Low : Acceptable, the impact is so low. At the very worst, make prevention campaign.
- **Scenario 2 :** Denial of service → High : Unacceptable, we cannot afford to lose the availability of the test results for a long period of time (∼1 day). Entities should prepare for disruptions, and have a well-tested recovery process.
- **Scenario 3 :** Create a false pharmacy → Mid : Tolerable under control, acceptable if we have very few fake pharmacies. The system should check the pharmacies before accepting their results. If we send too many fake results (enough to modify the overall results) we should be able to detect it.
- **Scenario 4 :** Steal or modify the database → High : Unacceptable, we cannot afford to lose this business value.

We put the level risk of the scenario 1 at Low, as we said before, even with a high likelihood, we don't except a high success rate, so it should remain statistically insignificant.
Risk scenarios that affects the Availability of the database are deemed unacceptable.

We plot our risk scenarios on a heat map:

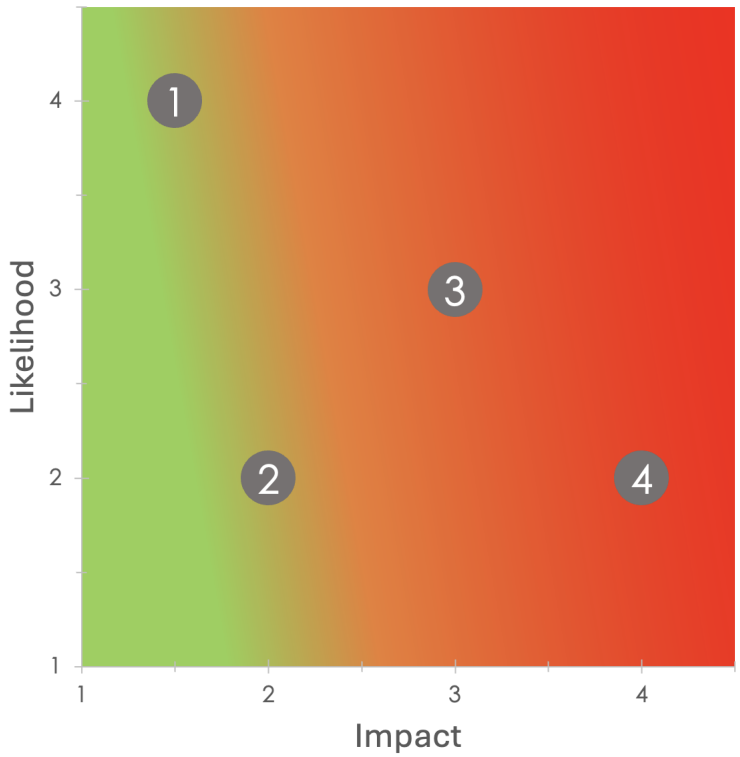

Figure 7: A heatmap of the risk scenarios
Note: The colors are not perfectly matched with our precedent definition.
We still consider the risks levels that we defined above.

VI.C Security measures

We go further into the security measures taken for each risk scenarios.

- **Scenario 1 :** Bribing the pharmacist → Accepted, no security measure should be taken. One should try to evaluate the bribery, if it's too high there should be a awareness campaign. They doesn't cost too much and should be effective enough to lower the likelihood to an acceptable level. It should be least prioritized measure taken.
- **Scenario 2 :** Denial of service → Tolerable under control. One should invest in a better host, capable of handling DoS attacks. Also a good restoration strategy minimize the MTTR (Mean Time To Recovery) is advisable to limit the financial loss and loss of productivity. Even then the risk still exists, but the likelihood of a strong impact should be reduced, DoS attacks will still happen at the same frequency, but we should be more resilient about them. It should be the first priority when taking security measures.
- **Scenario 3 :** Steal or modify the database → Tolerable under control but we highly advise to take actions, implement further checks to accept data from a pharmacy. Certificates should be simple enough to implement and won't cost much. The risk will be greatly reduced, but not non-existent (if one manages to bypass the checks, which is less likely). It should be the second last in terms of priority when taking security measures.
- **Scenario 4 :** Create a false pharmacy → Unacceptable, we have to take actions. Restrict access to the DB to only the people that work on the data. It's basic protection and should not cost much. Update the server, Debian 8 is deprecated since 2018! It induces some downtime but is greatly offset by the reduced risk. We still advise to encrypt the data, takes some setup time but it's a good practice.
  Even then, the risk is still present, but reduced, it's still our most feared event due to the impact, especially the long term impact, whereas a DoS attack is over in one day at worst. It should be the second in terms of priority when taking security measures.

Note: About the module developed by TestAntiCovidFrance, subjects says "*The application is developed in J2EE*", it is unclear if the version of Java used is Java 2 Entreprise Edition or not. If it is, it's very advisable to upgrade to *Jakarta EE* the successor of J2EE that supports the latest versions of Java which are safer than Java 2 that was deprecated in 2008.

VI.D Evaluation and reporting of residual risks

Synthesis of risk scenarios					
Risk source :	**Targeted objectives :**	**Attack path :**	**Gravity :**	**Operating modes :**	**Residual likelihood :**
Ordinary citizen	Personal gain	Prior knowledge of a pharmacist. Bribe them.	1	Bribe the pharmacist to falsify the results	4
Hacktivist	DoS TousAntiCovid server.	Denial of service	3	Locate the server, make a DoS attack.	2.5
	Sabotage the system.	Acquire the installation software, make a fake pharmacy	2	Fetching the installer. Putting it on a machine. Sending fake results.	1.5
State threat	Ruin the reputation of the country	Steal the database	4	Locate and enter into the server by exploiting vulnerabilities, steal or modify the database.	1

With our security measures, we reduced the likelihood of all the attack paths (except for the first where no security measure have to be taken immediately). The likelihood is still high for the denial of service attack due to it's nature.
The creation of fake pharmacies should be reduced to a minimum, if some basic measures are taken to ensure the pharmacies are indeed, real pharmacies.
The theft of the database is still a concern, but by applying the given measures the risk of a leak should be greatly reduced.

We make a heat map with the residual risks:

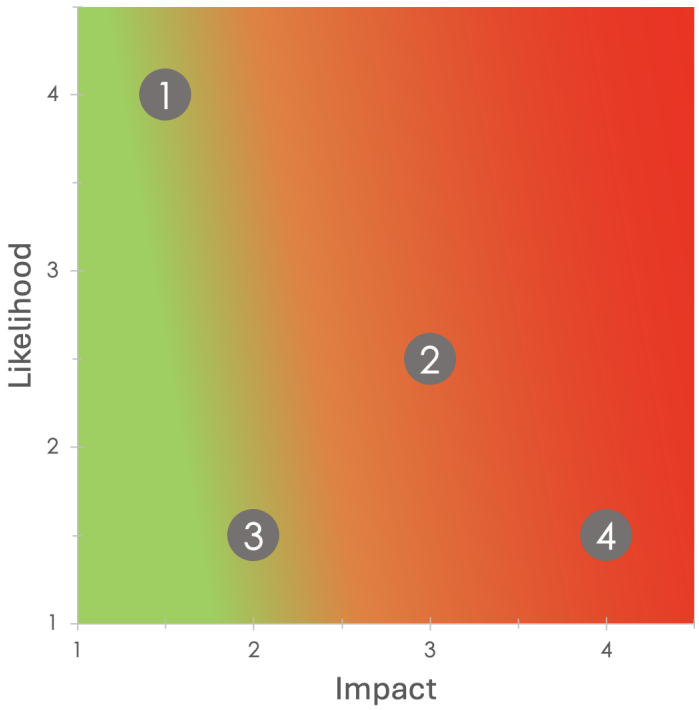

Figure 8: A heatmap of the residual risks
Note: The colors are still not perfectly matched with our precedent definition.
We still consider the residual risks levels that we defined above.

We see that the scenario 4 is still in a Red area, it should be Orange like the scenario 2. The gradient in our heat map is not ideal.

VII Conclusion

Using the EBIOS Risk Manager guide, we first defined the business values and the supporting assets of the project.
Then, we defined the risk sources and targeted objectives to identify the potential damage.
We moved to defining the stakeholders, the potential targets of an attack. We explored some operational scenarios to visualize the possible actions of a risk source to accomplish their goal. Finally we proposed some security measures that should mitigate the impact of the potential attacks.

Even after the security measures, we still a non-negligible likelihood of some attacks, particularly denial of service attacks and direct attacks on the database, these attacks are considered the worst kind of possible attacks. We have no choice but to expose the servers to the network to be able to receive the test results from all the pharmacies, this inevitably comes with risks that we tried to reduce to a minimum, while maintaining cost.

Taking some basic security measures like updating the server to a supported Debian distribution should already improve the security. Upgrading the version of Java used is also advisable, it shouldn't induce much difficulties if the software don't have a dependency hell.