MASTER IN COMPUTER SCIENCE

Risk management & Threat Modeling
a comparative approach

Bourdoud, Faris

Award date:
2019

Awarding institution:
University of Namur

UNIVERSITÉ DE NAMUR

FACULTÉ D'INFORMATIQUE

Risk management and Threat Modelling a comparative approach

Bourdoud Faris

RUE GRANDGAGNAGE, 21 ● B-5000 NAMUR(BELGIUM)

Acknowledgment

This thesis comes as a conclusion of a two-year adventure. I would like to thank all the people I met during this master degree. I am not going to mention all of them but thank you all for all the moments we shared. I would also like to thank my Professor Jean-Noël Colin for his availability, support and his precious advices during the development of this thesis.

I would like to make a special acknowledgement to my family who has always supported me and given me courage. To my two daughters Jalyn, Jennai, thank you for all your smiles that gave me the strength when I needed it. To my half, Evelyne, without you none of this would have been possible!

Abstract

The information systems, the technologies, the laws on data privacy and data protection are continuously evolving. It becomes more and more complex to analyse and describe a system, and its relationship with others. Because of that, preventing all attacks and detecting the risks is becoming a very difficult task. Hopefully the methodologies to help in this field evolve too, new approaches are created every year. Unfortunately, this constant evolution makes it difficult to choose the correct tool, methodology, framework to ensure the risk management on a project or on an organisation level. This thesis intends to offer to the reader a first step and guidance in his choice regarding the context.

Keywords

Risk management, risk assessment, threat modelling, threat, security, data breach, data flow.

Table of contents

Chapter 1: Introduction

Goal

Today the risk management became a very sensitive subject for the industry. More and more information systems are the target of cyber-attacks with huge financial and human consequences. According to an IBM security study published in 2018, the average cost of a data breach is $3.86 million. But the cost of "mega breaches," where 1 million to 50 million records are lost, can cost from $40 million up to $350 million. To these amounts we must add all the hidden cost such as bad reputation, the implementation of the recovery plan etc.

Hopefully we have a lot of different methodologies to help us assess and manage the risks and threats. One could even say that there are too many methodologies existing for someone who starts in this domain and would like to inform himself. It is very difficult to choose the right one when you do not know about the others. Worse than that, if the choice is not appropriate for the project, the risks could be ignored or not detected. Therefore, the choice must be made at the beginning of the project after having taken into consideration all the aspects of the project. Also, another crucial argument saying that the risk management should be performed from the beginning, is that according to Microsoft, the cost of implementing the security in a deployed solution is up to 30 times more than if it was done at the start phase of the project.

The goal of this thesis is to help people understand what risk management is and have an idea of the existing tools and approaches that are at their disposition to manage the risks in their project and help them choose the right tool according to their context. The risk management tools will be compared to another approach, threat modelling, to determine what really the differences are and see if they are complementary or redundant.

Due to the huge number of existing methodologies, this thesis will not analyse all of them but select a sample of the most representative solutions. Once the approach is selected, the user will have to continue investigating if other tools exist which have not been developed here.

Research questions

The main research question of this thesis is what are the differences between risk management and threat modelling? One sub question tends to discover if the two approaches are redundant or complementary. To answer to these questions, the first thing we need before starting is to clearly define what risk management and threat modelling are, what are the different implementations that exist to use them.

Then we will analyse the different sorts of risk management methodologies that can be used for a project or organisation. Therefore, we will analyse four risk management methodologies that are used in the industry. For each of them, we will describe them and try to see what their strengths and their weaknesses are.

Afterwards we will analyse five of the existing tools to do threat modelling. Like for the risk management methodology, we will define them, try to find their strengths and their weaknesses.

Another part of this thesis will be to experiment one risk management methodology and one threat modelling methodology for the same use case in order to confirm what we discovered with the analysis of the different tools.

To compare those tools, we will define search criteria. They will allow us to do a first comparison between the risk management methodology and threat modelling and try to see if their results are complementary or redundant.

Roadmap of this thesis

This thesis contains seven chapters. First, we have the introduction to the subject. Then we have the second chapter which will define the study concepts, the description and the analysis of the concept we will use. Later in chapter three, different risk management methodologies will be selected, analysed and evaluated with predefined criteria. In chapter four, we will do the same but with threat modelling methodologies. In chapter five, an experimentation of one risk management methodology and one threat modelling technique will be done on the same use case. In chapter six we will compare the risk management and the threat modelling approaches with all the criteria and points we analysed in chapter three, four and the experimentation in chapter five. Finally, we will finish this thesis by the conclusions in chapter seven.

Chapter 2: Risk, risk management and threat modelling

In this chapter the terms used will be defined and a first analysis of risk management and threat modelling method in general will be done by explaining the different approaches for each of them, why they are important and what they offer.

Risk

The first thing we must understand and agree on when we speak about risk management is of course what is the definition of a risk? And by risk we are talking about project risks. According to the project management institute a "project risk is an uncertain event or condition that, if it occurs, has an effect on at least one project objective". In a project there is an infinite number of risks, all with different level of severity, probability. To control a project, it is important to be aware of those risk and if necessary, mitigate them or on the contrary exploit them. Therefore, we have different methodology to help us to do risk management.

Risk management

The risk management is a process which will allow to minimise the risks and take advantage of the opportunities. It is important that this process is applied during the entire life-cycle of the project. For certain part like data protection it is even a legal obligation if you want to respect the new regulation (GDPR). In any case this process is essential if a company wants to have a good governance.

Risk management approach

One of the most important part in the process of risk management is the risk assessment. It is an activity where the risks will be identified and assessed. Contrary to the risk management the risk assessment is not continuous, it is only done when required. This activity will allow to produce a document with security requirements to mitigate the identified risks. This document will be used in the context of the project but could also be used to help management to make strategic decisions, to modify the company privacy policy etc. The goal of the risk management in general is not to have a plan to avoid all the negative risks but to have a risk plan that allows to have an acceptable level of security. In figure 1 we can see the different activities that compose the risk management process.

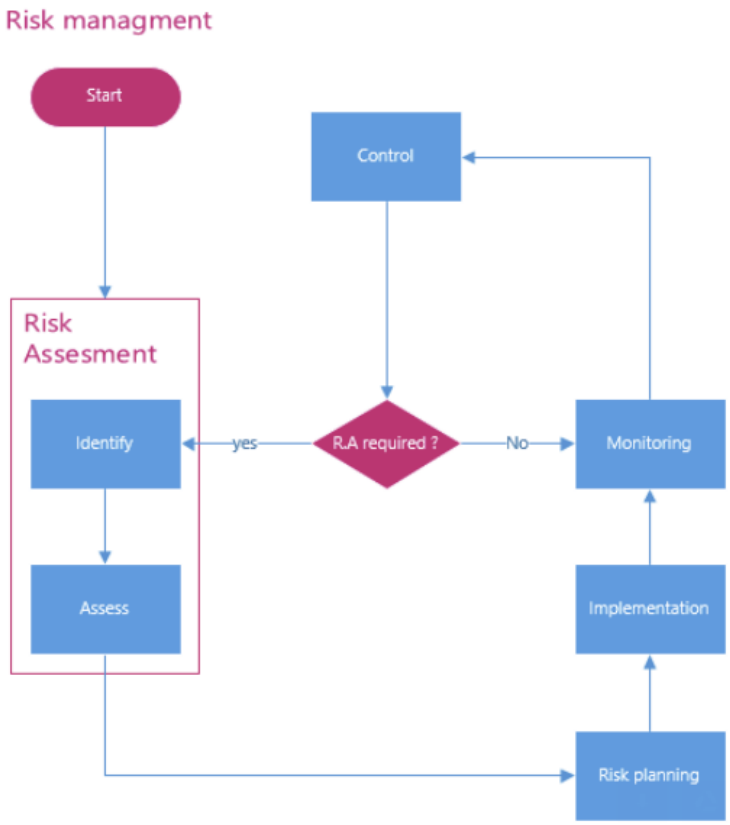


Figure 1: Risk management activities

1. Identify: this is the most important step of the risk assessment. During this step the vulnerabilities and their origin are identified.
2. Assess: this step will allow to assess the probability and the impact if the event occurs. Based on this assessment the risk will be sorted by cost for example and then prioritised. This step helps to decide which risk needs to have a mitigation plan.
3. Risk planning: it is in this step that the mitigation plans for the risks will be decided.
4. Implementation: the strategies are implemented.
5. Monitoring: follow the project if a change can raise new risks.
6. Control: if a change is made, a control is performed to see whether a risk assessment is necessary or not.

Approaches for security risk assessment

As we can see in figure 1 the risk assessment is a crucial part of the risk management. In this step the risks are identified and analysed to assess their probability and the lost they can cause. It will help the project manager and the board if necessary, to take actions about the threats. To assess those risks is not always easy and for that it exists many methodologies and approaches.

Qualitative approach

The qualitative approach consists in a series of interviews and meetings. It will result in a list of descriptions and recommendations for each risk. The advantages of this approach are:

1. Much easier to implement.
2. Faster.
3. Does not need a lot of input to be conducted.

On the other side, the disadvantages are:

1. The results are approximate.
2. We do not have concrete numbers.

This approach is perfect for projects or organisations with limited resources or with tight schedule.[18]

Quantitative approach

The quantitative approach will be much more accurate by associating numbers to the probability and to the damages/benefit results. The disadvantages of this approach are:

1. In order to have an accurate value we need a lot of inputs from the project and the context.
2. To implement this approach, it is expensive and time consuming.
3. Specialists are most of the time needed

Strategies for the threat

The threat are the events that will result if they happened into a negative effect.

Avoid

This strategy consists into taking the necessary measures to completely avoid the risk. For example, the menace is: it is impossible to prove that a sub-contractor is GDPR compliant. The response could be breaking the contract with the contractor and implement an in-house solution.

Transfer

This strategy consists into giving the responsibility and accountability to a third party. For example, by taking an insurance.

Diminish

This strategy consists into acting to diminish the probability or the consequences of the event. For example, by creating first a mock-up to show the client and to confirm that the requirements were correctly understood.

Strategies for the opportunities

The opportunities are the events that will result if they happened into a positive effect.

Exploit

This strategy will try to reduce the factors that could avoid these events to happen. For example, another client could need a similar solution. So, the solution could be more generic to satisfy several clients.

Share

For example, to share a performant process with another unit within the company.

Enhance

Try to raise the probability that this event happens.

Strategies for both

- Accept the risks and do nothing to mitigate them.
- Conditional response

Threat modelling

When we read the literature about risk management there is another method which is very popular, the threat modelling. If we take the definition from the Open Web Application Security Project "Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value". The threat modelling will help to assess the applications and identify the threats. Again, it is recommended to do this from the beginning of the project.

Security threat

We can define a security threat as a vulnerability that an attacker could use to cause harm to an application. When this happens, it is called an attack. And to avoid these attacks it will be necessary to implement counter measures. In a system it is not enough to implement a counter measure only for a very specific part of the system, it is important to consider the context, the dependencies, the purpose of the module etc. There is no point in implementing huge login security on your application web interface if your database is accessible from outside and with a simple password. In the end, the security of your entire application will be as strong as the weakest point. Threat modelling allows to take the appropriate counter measures. It is very important to include this process in the software development life cycle (SDLC)[12]. This will help to:

- define the security requirements
- have a secure design
- prioritize the threat
- have a secure release

Threat modelling approaches

According to the literature as in [9], there are three different approaches for threat modelling.

Software-centric

One of the most important part in a software is of course the source code. When you develop an application for a client, there is not always information about the deployment environment,

sometime for security reason. With the software-centric approach it is possible to focus on the software itself, his different components and detect where the software itself can be attacked. To be able to do that it is very important to have a deep understanding of the application model. And since we are in the development phase, every stakeholders of the project need to understand it. So, a good communication plan is critical. Once everyone is up to date in the understanding of the model, we will have a security improvement in the different components of the software. The software-centric approach of threat modelling will allow the developers to participate to the threat modelling and to have a better business understanding which will make them more efficient. Also, the detected threat will be known and shared to everyone.[9][10]

Asset-centric

With this approach the focus and the main interest are on the infrastructure of the application or what the company owns. Like in the risk management we call that asset. So, this approach will be used when a good needs to be protected, for example data subject personal data that have been collected with a legal purpose. As opposed to the software-centric approach here there is a need to know the context in which the software will be deployed. If there are processes that allow to access the asset, they must be communicated and understood.[9]

Today we have a lot of tools that allow to increase the security on the assets. For example, the Open Web Application Security Project (OWASP) provides a list of existing attacks and the action plan that could be put in place to mitigate them for the web application. They defined this as an awareness document that regroups the most critical security risks. To create this document, they took advantage of the experience from security experts who shared their expertise.

Attacker-centric

Another way to see the system vulnerabilities is of course from an attacker point of view. For that, all the access points of the application need to be identified. When we looked at attacker-centric models we can see that they list all the threats and present them as attack trees. Each tree represents an attack on system. We have the goals as roots, and the leaves represent the ways to achieve that goal, this is recursive, each root sub node is a sub goal etc. We can also have OR nodes to represent the different possibilities or AND nodes if all the steps are required to reach the goal. You can see the example of one tree representation in figure 2.[9][10]

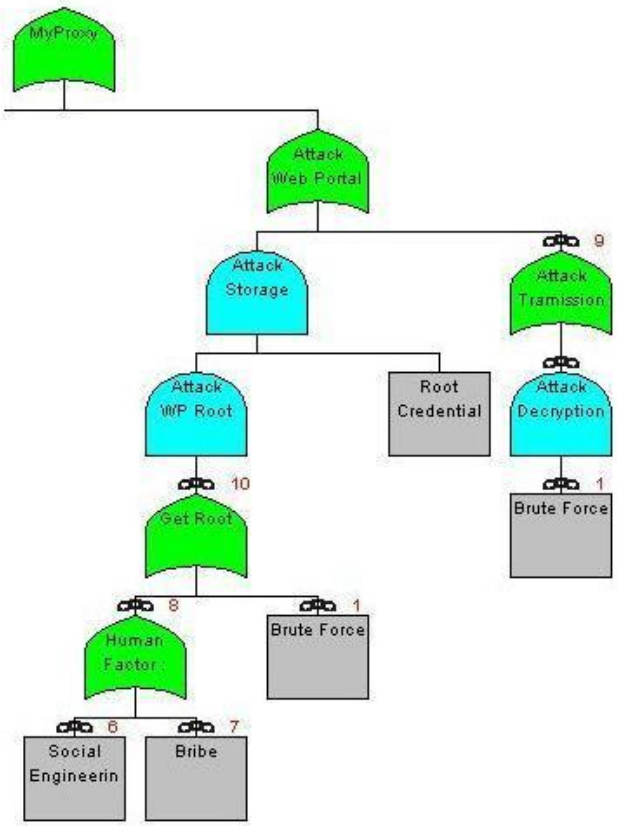


Figure 2: Example of an attack tree. Reproduced from ThreadModel-AttackTree[14]

When the tree is built, we can associate attributes to each node and give a value for each of them. These values will allow us to evaluate the security of the goal. The figure 3 shows an example of the attributes and their values.[14]

TABLE 1: COST OF ATTACK AND DAMAGE

Attacks/leaf	Cost of Attack	Damage Cost
Social Engineering	100	2500
Brute Force	15000	10000
Steal user Credential	1500	2500
Bribe	1000	2500
Steal Renewer Credential	2500	7500
Steal Retriever Credential	2500	7500
Steal MyProxy Credential	7500	17500
Attack Requester Credential	2500	10000
Attack Root	6000	15000

Figure 3 example of node attributes. Reproduced from ThreadModel-AttackTree[14]

This example of evaluation shows us how threat could be prioritized and what we could sort them by (damage cost – cost of attack), if the attacks cost more than the profit, it will probably not occur, otherwise these vulnerabilities need to be secured. These attributes help to associate risks with an attack. Of course, we could add many different attributes, knowledge or time required, cost of development… [14]

Threat modelling point of view

There are two points of view we can use to do threat modelling:

1. Defender point of view
   This one requires less technical knowledge and is easier to implement. One needs to know the infrastructure on this, one detects the vulnerabilities.
2. Attacker point of view
   This one is a little bit trickier. The attacker does not necessarily know the architecture, he will modelize the system as a succession of layers and for each of these layers list the attacks he could use to access the system.

Chapter 3: Analysis of risk management methodologies

Like it was said in the introduction, today there are plenty of solutions or methodologies to implement the risk management. In this chapter we are going to select the most relevant ones for our subject. For that we will use several criteria:

- The method can be used on new and existing information systems
- There is enough online documentation
- The method is known and used by the community and already has convincing results
- The output allows to create a risk plan like described in fig.1
- It focuses on projects rather than organisations

First a list of methodology has been created by browsing the literature like [14][15]. Here is an exhaustive list table with all the methodologies founded.

Name	Selected
Austrian IT Security Handbook	No
Cramm	-
Cobit	No
Ducth A&K Analysis	No
Ebios	Yes
Fair	Yes
Frap	Yes
Isam	No
ISF Method	No
ISO/IEC 13335-2	No
ISO/IEC 17799	No
ISO/IEC 27001	No
IR-Grundschutz	-
Magerit	-
Marion	No
Mehari	-
Migra	-
Octave	Yes
Rfm	-
RiskSafe	-
SP800-30	-
Tara	-

Excluded methodologies

- Austrian IT Security Handbook: The available documentation for the Austrian IT Security Handbook is very limited.
- Cobit: Is not focused enough on project but is more on IT governance.
- Ducth A&K Analysis: Very poor online documentation.
- Isam: Very poor online documentation.
- ISF Method: Very poor online documentation.
- ISO/IEC 13335-2: This is a standard to comply.
- ISO/IEC 17799: This is a standard to comply.
- ISO/IEC 27001: This is a standard to comply.
- Marion: Very poor online documentation.
- Migra: Very poor online documentation.

Selected methodologies

The purpose of this thesis is to give information on tools available to do risk management and to compare them to the threat modelling approaches. The analysis of all methodologies is out of scope. Three methodologies will be selected by using the selection criteria defined above.

Here is the list of the selected methodologies:

- EBIOS: This methodology is wildly used and partly used in other tailored methodologies for data privacy impact assessment for example.
- FAIR: Simpler and quantitative approach.
- OCTAVE: Octave is one of the most named methodology in the literature.
- FRAP: A more visual risk assessment methodology.

The goal of this selection is to have the most different risk assessment approaches as possible. Of course, the criteria popularity is also important here since the goal is to inform. For the analysis of the selected methodologies the following structure will be used

- Origins: explain where, how, the methodology has been created
- Purpose: the goal of the methodology.
- Process: all the process defined in the methodology.
- Reflexion: A first analysis of the methodology, the advantages and disadvantages.

The methodologies with a ‘-‘ could have been chosen but It was not possible to study them all so choice had to be made.

Comparison criteria

To compare these methodologies, we will use the following criteria:

comparison criteria	**Definitions**
Time for implementation	By reading the documentation, an appreciation is given on the time needed to implement the solution. This is deduced by the number of steps required by the methodology and their level of details.
Necessary skills (complexity)	By analysing the methodology, an appreciation is given on the complexity of this one. If the complexity is high, a more experienced profile will be needed to use the methodology.
Results readability	This criterion will determine if the produced result is easily understandable and usable.
Scope	This criterion will assess if all the risks are considered for the studied solution.

Time for implementation scale

The following scale will be used in order to express the appreciation of the time needed

Level of scale	**Scale description**
Fast	Not many steps, straight to the point.
Normal	Requires organisation.
Long	Long process that requires a lot of analysis and implementation time

Necessary skills (complexity)

The following scale will be used in order to express the experience needed to implement the methodology due to its complexity

Level of scale	**Scale description**
None	Anyone can do it
Normal	A previous experience in risk assessment or project management is needed
Advanced	A strong experience in risk management is needed

Result readability scale

The following scale will be used in order to assess the result of the implementation, if it easily usable or not.

Profile	**Profile description**
Easy	Results are user friendly and understandable by all.
comprehensible	The results require attentive reading to be understand
complex	The data are there but not easy to understand.

Scope scale

The following scale will be used in order to assess the scope covered by the methodology.

Profile	**Profile description**
Low	Many risks or threats are not covered.
Complete	The results are correct
Detailed	The results are extensive and consider all the aspects.

EBIOS

Origins

The EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) methodology was created in 1995 by the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). EBIOS is an experienced methodology that has more than 20 years of experience.[17]

Purpose

EBIOS allows to assess the risks and to identify the counter measures to mitigate them. This method also allows to validate the level of acceptable risks and to improve the security of the information system on the long term. This methodology will bring a better communication and will allow the management to make decisions with the arguments provided by the methodology.

This methodology can be used for several purposes:

1. To put in place an entire risk management process within an organisation.
2. To assess and manage the risks.
3. To define for each good the level of security that needs to be reached by considering the context and the scope of the study.

According to EBIOS, this methodology is fit for all organisations, small, big, private sector or public sector. The methodology could be used on a green field project or an existing one.[19]

Process

The EBIOS methodology has a top down approach. First, it will do a high-level analysis and then it will focus more and more on the business elements by studying the possible attack on them. The goal is to create a list of scenarios for possible attacks on business elements. In order to realise that, the methodology is articulated around 5 modules.

- Context and scope
- Sources
- Strategic scenario
- Operational scenario
- Mitigation plan

These modules are executed in cycles. There are two kinds of cycles. (See figure 4)

1. Strategic cycle
   - This cycle will reassess the entire study, especially the strategic scenarios.
2. Operational cycle
   - This cycle will focus on the operational scenarios when a new security breach occurs, or new vulnerabilities are detected. [19]

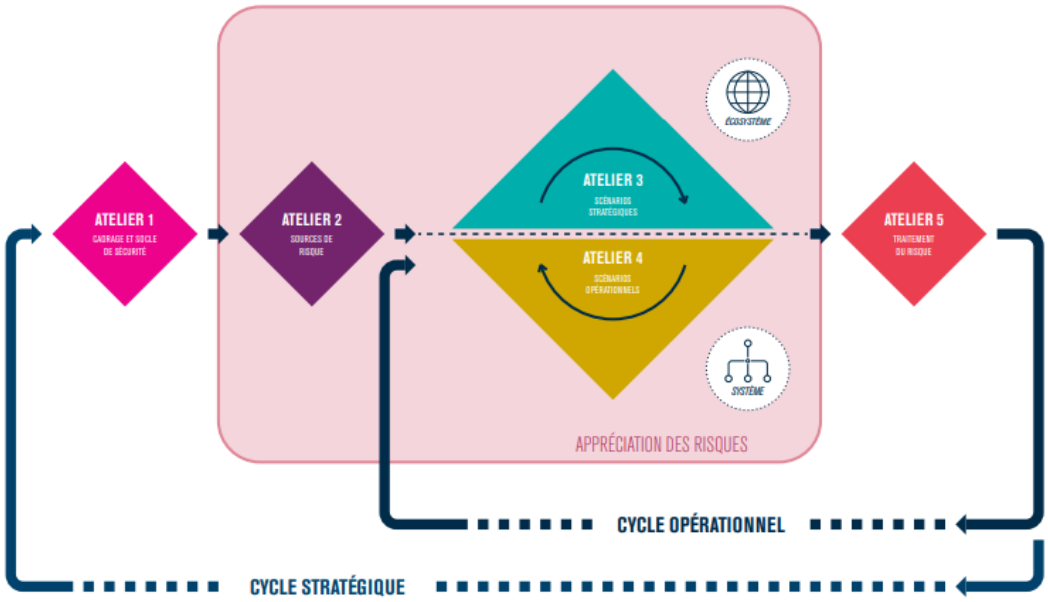


Figure 4: EBIOS steps source [guide-methode-ebios-risk-manager]

The five modules

Like we said before the methodology consists of five modules. For each of them, we will:

- Detail the objectives
- Identify the contributors
- Define the steps and how to proceed
- Define the produced outputs

Context and scope

The objectives

This first step is there to analyse and define the context of the project, the scope which must be covered by the study, the stakeholders, the time table. An analysis on the goods will be done to list them and determine the dreaded events and their impacts. During this step the required security level will be defined.

The contributors

This step is done in the strategic cycle which means that the management must be involved since decisions over the risk strategy must be made. The recommended profiles required for this step are:

- Direction
- Operational manager: the different profiles responsible for the concerned business
- The CISO, Chief Information Security Officer who will provide or approve strategic security decisions.
- The information system director: his input is necessary since it could concern several and sometimes all the information systems of the organisation.

The steps and how to proceed

The methodology requires 4 steps to be done during workshops or analysis:

1. **To define the case study**
   In order to do so, the methodology offers to first explain the subject and the requirements of the meeting. It is very important that everyone understands, agrees on the requirements and the subject of the study. Once they are set, it is not always easy to change them since it would require a new strategic cycle. An example of study could be the management of the privacy management of the process on the personal data. This subject will determine the level of details required by the study.
   During this module, the required people and skills will be identified and associated to the different workshops.
   The recurrence of the cycle must be defined. To be defined, they must take into account the context, the goal of the study…
   And of course, the planning that is required by the project manager will be drafted.

2. **To define the scope of the study**
   To do that the methodology offers to analyse the object of the study. What are the processed used, why, what are the related goods or process that the object needs to be able to work… the documentation provides a nice table as example that could be used (see figure 5). The goal here is not to be exhaustive but only to have a list. It allows to easily change the table if necessary.

3. **To identify the dread events and assess them**
   In this step, the dread event needs to be identified and assessed. With EBIOS each dread event needs to be linked to the affected good. It allows the stakeholders to be aware of the security issues and their consequences. In order to do that, the table filled in the previous step can be used and for each element we will list the threats.

4. **To put in place the required security level**
   To put that in place you need to refer to a model. It could be ISO specification, special regulation, internal guidelines… For the study object, we need to do an assessment of the compliance regarding these references.

To define the produced outputs

This first module will produce the following outputs

- A case study
- The necessary stakeholders for the different steps
- The list of different processes and goods of the study
- The references with the flexibility

MISSIONS	MISSION 1	MISSION…		
DÉNOMINATION DE LA VALEUR MÉTIER	Valeur métier 1	Valeur métier 2		Valeur métier…
NATURE DE LA VALEUR MÉTIER (PROCESSES OU INFORMATION)				
DESCRIPTION				
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE / EXTERNE)				
DÉNOMINATION DU / DES BIEN(S) SUPPORT(S) ASSOCIÉ(S)	Bien support 1	Bien support 2	Bien sup-port 3	Bien support…
DESCRIPTION				
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE / EXTERNE)				

Figure 5 source [guide-methode-ebios-risk-manager fiche 1]

Sources

The objectives

The goal of this module is to identify the sources of the risks and their target. Once they are identified they will be analysed and assess. Only the selected risks will be used to create the scenario in the next modules.

The contributors

This module is still in the strategic cycle, so the management still needs to be involved. The recommended profiles required for this step are:

- The direction: for strategic decisions
- The Operational manager: to confirm the sources and the damages. It can also raise their awareness
- The CISO: he brings his expertise for sources of risk
- A security expert can be required if the skills of the team are not sufficient.

The steps and how to proceed

This module is relatively short, but to be able to correctly identify the steps, it requires a certain knowledge like whom could the menace come from, why would they attack, how.... This module requires several steps:

1. **To identify the sources of the risks and their target**
   A list of all the sources risks and their goals must be done. For that the methodology provides a table with all the existing threat sources.
2. **To analyse and assess**
   Once the first step is done, an assessment must be conducted. In order to do that, matrix must be used in order to prioritize the risks.

3. **To select the relevant one**
   Here the decisions are made to select the risks that are considered as non-acceptable.

The produced outputs

This module will produce the following outputs:

- list of coupled sources/goals
- table of assessment

Strategic scenarios

The objectives

This step will allow to have a better vision of the information system and all its threats. This will allow to create high level scenarios called “strategic scenarios”. They represent the path that a threat can take to attack the system. When this step is done a security measure of the information system is already possible.

The contributors

With this module we are not in the strategic cycle anymore, so the decision management is not required anymore. The recommended profiles required for this step are:

- Operational manager
- Functional architect
- CISO
- A security expert if the knowledge of the team is not enough.

The steps and how to proceed

This module requires to:

1. Select the critical stakeholders and list the linked threat that are in the context of the studied object.
2. Produce strategical scenarios.
3. Define security measures for the strategical scenarios that could happen

The produced outputs

This module will produce the following outputs:

- List of threats in the context of the studied object.
- List of strategical scenarios
- Relevant security measures

Operational scenarios

The objectives

In this step, more detailed scenarios are built. These scenarios will define the exact way the threat source can use to realise the strategic scenarios. This Step is organised in the same way as the previous one but will focus on the support goods.

The contributors

The recommended profiles required for this step are:

- The CISO
- The information system director
- A security expert if the knowledge of the team is not enough.

The steps and how to proceed

In order to create the operational scenario, you need to use the strategic scenarios defined in the previous module and try to identify the support goods that could be used to implement those strategic scenarios. To help you with this task you could use models that list the existing attacks on specific goods. Once this is done you can represent your scenario as an attack three for example.

The produced outputs

This module will produce the following output:

- A list of the operational scenarios

Mitigation plan

The objectives

In this last step, a recap of all the analysed risks will be done to allow the creation of a risk plan. In this document, we will describe the necessary security measures and a proper way to monitor them.

The contributors

The recommended profiles required for this step are:

- The management: to acknowledge on the result of the cycle.
- The CISO

The steps and how to proceed

This final module will use the 4 previous modules to create a synthesis. In order to complete this module, you need to:

1. **Represent the identified risks**
   In order to represent the identified risks, you could use a graph which represents the likelihood and the severity and dispose the risk on it. This way, the management will clearly identify the most dangerous ones.
2. **Decide the strategy for the identified risks**
   Mitigate, control, accept.
3. **Assess and document the residual risks**
4. **Define a plan to follow the risks**

The produced outputs

- This final module produces the following necessary documents for the management
- the mitigation plan
- the residual risks
- the plan to enhance the overall security
- the plan to follow the risks

Synthesis

What we conclude with this methodology:

- This methodology could be used for all kinds of environments, small or big organizations.
- The granularity of the study can be customized.
- The methodology provides a lot of tools to help during the implementation.
- The methodology is modular and has an agile approach.
- The documentation can be sometimes confusing, it is not always easy to see the link between the steps.
- The full implementation is quite fastidious.
- An expert is required if the security knowledge is not enough in the organization.

The overall impression of this methodology is that only big companies will think or have the need to implement it, even if the documentation says that it is fit for small organisation as well. Moreover, the number of contributors is high and going through all the hierarchy can be quite difficult sometimes. We also clearly see in the following tables that the produced outputs are most of the time for the management which means that the knowledge remains at their level and they need to have a communication plan to raise the awareness with the rest of the stakeholders.

Steps	Output	Contributors	Target users	Complementary methodology, technique
Context and scope	-case study -stakeholders necessary for the different steps. -list of different process and good of the study -The references with the flexibility	-management -expert	management	Data flow diagram
Sources	-list of coupled sources/goal -table of assessment	-management -expert	management	
Strategic scenario	-list of threat in the context of the studied object. -list of strategical scenarios -relevant security measures	-Operational manager -Functional architect -CISO	-Architect -CISO	Elevation of privileged
Operational scenario	-list of the operational scenarios	-The CISO -The information system director -A security expert	-Architect -CISO	T-MAP
Mitigation plan	-the mitigation plan -the residual risks -the plan to enhance the overall security -the plan to follow the risks	-management -CISO -operational manager	management	

Criteria

Time to implement: Long

Justifications

- It requires the involvement of the hierarchy
- The methodology is not always easy to understand
- There are a lot of documents to produce
- The execution of all modules is fastidious

Level of skill: Advanced

Justifications

- It requires having a good organisation and management experience.
- The methodology is not always easy to understand.
- The target user is most of the time the management.

Readability: comprehensible (The produced documents can be long)

Justifications

- If the representation is chosen correctly, the management will not have difficulties to understand. E.g. use a matrix to represent the risks.
- The number of created tables can be confusing and the link between them is not always clear

Scope: Detailed

Justifications

- This detailed appreciation requires that the methodology is correctly implemented, that the necessary skills and knowledge are available and the cooperation of all the stakeholders.

FAIR

Origins

FAIR (Factor Analysis for Information Risks) is a risk management framework developed by Jack A. Jones in 2001. It has been adopted by The Open Group as a standard. [21]

Purpose

The core of the FAIR framework is to quantify the risks in an organisation. For this methodology, if it is not possible to measure the risks, then it is not possible to make decisions. This framework will provide a way to effectively quantify the risks and then manage them.[33] The approach of this methodology is to have a quantitative evaluation of the risks. It will try to answer to these main questions:

- "How much risk do we have?
- How much risk is associated with…?
- How much less (or more) risk will we have if…?
- Which of our risk management options are likely to be most cost-effective?
- What benefit are we getting for our current risk management expenditures?"

(Measuring and Managing Information Risk (A Fair Approach), Jack Freund and Jack Jones, 2015 Introduction)

Process

The FAIR framework is composed of two main elements (figure 6):

1. Risk
   This first element is composed of a combination of threats controls assets impact that could lead to a loss. The controls are the means which are put in place in order to monitor the assets of the organisation (firewall, passwords complexity, backup for the integrity…)

2. Risk management
   In this element we can see 2 main roles groups:

   - The decisions: This is the role of the management. They will draft processes, choose technologies, define policies in order to define the risks goals.

   - The execution: To apply the guide lines drafted by the decision management, there is a need for an execution role. And of course, to execute correctly and make the good decisions that respect the guidelines established by the decision management, a good communication, support and enforcement must be provided as well. This is essential because without support, for example, a head of unit could be powerless. Of this depend the awareness (of the policies…), the capability to execute correctly and their motivation.

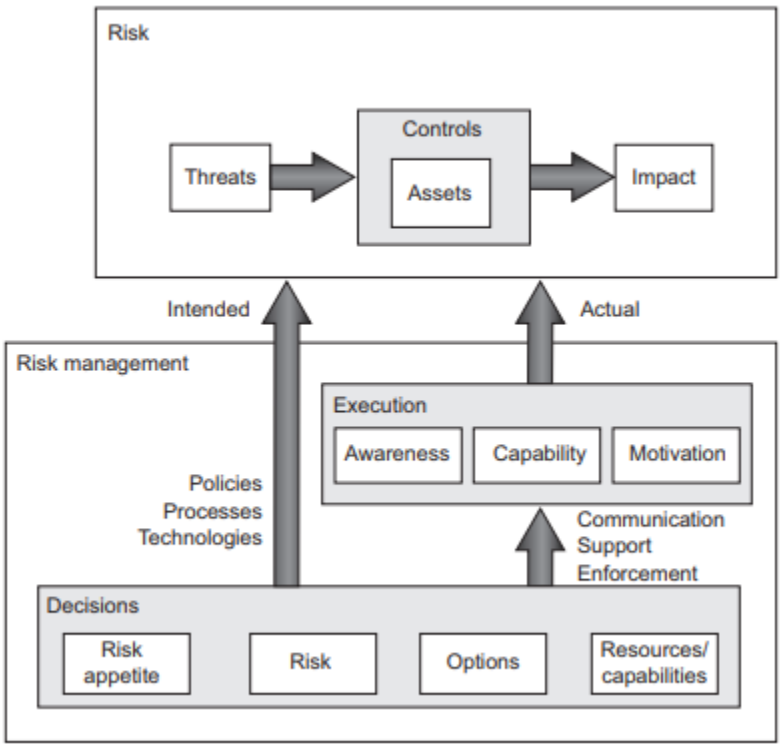


Figure 6: FAIR risk management system[21]

In order to have a proper risk management system, there is obviously a need for loop to repeat the cycle. (figure 7). The loop is represented by feedbacks coming from the different roles, capabilities and elements. Like we saw previously, the FAIR framework believes in a quantified approach, so it is necessary to add matrix to these feedbacks that will help the decision groups to correctly assess.

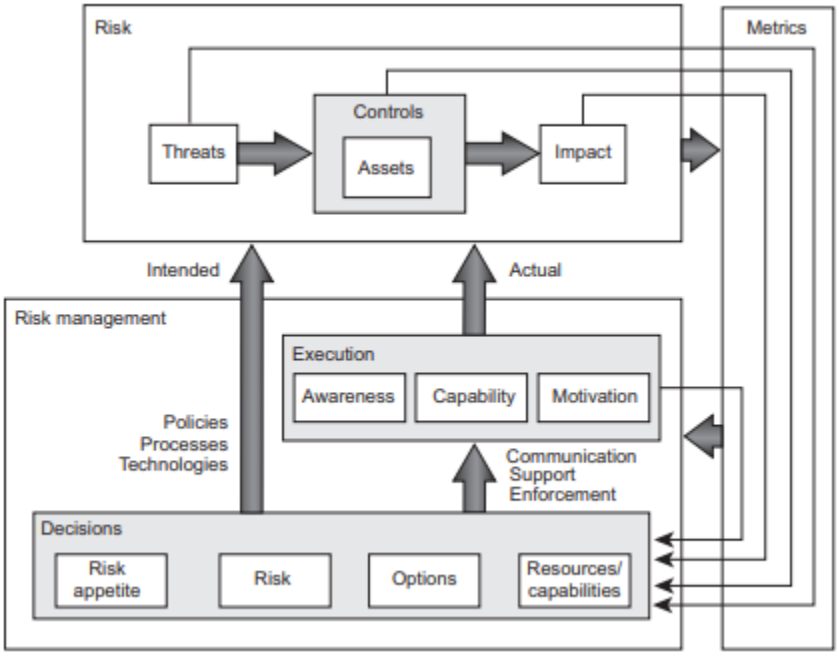


Figure 7: complete FAIR risk management system

Risk analysis

With the FAIR framework it happens sometimes that the same scenario is assessed several times, one for each point of view. This will allow to bring the most relevant scenario to the top. The process flow for the risk analysis is the following (fig 8)

Figure 8: risk analysis flow [31]

Scenario building

The objectives

In this step, the scenarios and their scope will be defined. The goal is to structure the thought of the participants.

The contributors

The contributors can be the execution roles, the operational roles, the developers, anyone who could have an idea, a question, or a suggestion on the organisation assets.

The steps and how to proceed

The methodology insists in compartmentalizing the scenarios in four factors:

- **Assets at risk**
  In most of the scenarios, multiple assets are involved, personal computers stolen, password displayed on stickers on the desk, a database.
- **Threat community**
  Here we are going to list who or what is the threat source.
- **Threat type**
  Here we will determine the nature of the threat. Is it a malicious human? Is it Mother Nature? Is it a human error? All these factors will have an influence on the impact.
- **Effect**
  Here we need to assess the effect on the asset itself. The framework advices to use the CIA framework.

The framework does not provide tools or template in order to that but tries to help by giving examples of questions that should be asked or by providing another framework that could be useful.

The produced outputs

- A table that contains, for each scenario, all the assets affected, by who or what, the threat type and the effect on the asset.

FAIR factors

The objectives

In this step, we will perform a further comprehension of the scenario by analysing the outputs of the previous step.

The contributors

The contributors can be the execution roles, the operational roles, the developers, anyone who could have an idea, a question, or a suggestion on the assets of the organisation.

The steps and how to proceed

In order to do this evaluation, we will use the documents from the scenario building

- The analysed asset and his environment will help to understand the control that are in place and why they are not sufficient. It will also help to analyse by whom or what it can be attacked.
- The threat community will also help to determine the capability of the threat and the frequency at which it can attack.
- The threat type will also help to assess the frequency and the loss. For example, unintentional events occur more than a malicious attack.
- The effect associated with the asset will also give information on the frequency.

The produced outputs

There are none. This step only brings knowledge and a better comprehension of the scenario and will help for the next steps.

Expert estimation and PERT

The objectives

In this step an estimation will be performed. To do so, the framework provides measurement techniques like calibrated PERT.

The contributors

- The contributors can be the execution roles, the operational roles, the developers, anyone who could have an idea, a question, or a suggestion on the assets of the organisation.
- experts

The steps and how to proceed

Like we said previously, techniques like PERT will be used. You can see in figure 10 an example of quantified threats. These data will be used in the next step as well as the data from the figure 9 that represents the quantification if the risk occurs.

Loss Forms	Confidentiality	Availability	Possession of $
Productivity	$5000–$75,000	$5000–$50,000	$15,000–$150,000
Response	$50,000–$250,000	$50,000–$100,000	$50,000–$500,000
Replacement	$0	$0	$50,000–$1.5 million
Fine and judgments	$500,000–$2 million	$50,000–$150,000	$1–$5 million
Secondary response	$100,000–$500,000	$50,000–$100,000	$1–$5 million
Competitive Advantage	$0	$0	$0
Reputation	$500,000–$1 million	$100,000–$1 million	$250,000–$2 million

Figure 9: Loss for the risks [21]

Asset	Threat Community	Threat Type	Effect	Threat Event Frequency	Threat Capability
Customer information	Cyber criminals	Malicious	Confidentiality	0.5–2	0.75–0.95
Customer information	Privileged insiders	Error	Confidentiality	2–6	0.98–0.99
Customer information	Privileged insiders	Malicious	Confidentiality	0.02–0.05	0.98–0.99
Customer information	Privileged insiders	Error	Availability	2–6	0.98–0.99
Customer information	Privileged insiders	Malicious	Availability	0.02–0.05	0.98–0.99
Customer funds	Privileged insiders	Error	$	0.5–2	0.98–0.99
Customer funds	Privileged insiders	Malicious	$	0.1–0.3	0.98–0.99
Customer funds	Customers	Malicious	$	6–12	0.75–0.95

Figure 10: quantified threats [21]

The produced outputs

- Estimation analysis
- Documentations on the scope and the reasoning for these results.

Monte Carlo engine

The objectives

Now that all the data have been created, we are going to use a tool provided by the framework in order to process them and provide a modelling view.

The contributors

- Monte Carlo engine

The steps and how to proceed

Give the previous inputs to the modelling tool.

The produced outputs

The report that the decision management will use. The interpretation of these results is not in the scope of this framework. There is an entire chapter dedicated to that in the documentation that explain each graph created.

Quasi quantitative analysis

The objectives

The framework also provides another possibility to analyse the risks. We are going to briefly describe it since it is not the primary way. Indeed, like we said before FAIR recommends to have a fully quantitative risk analysis.

The contributors

- Expert in FAIR concept and method
- Any member of the organisation

The steps and how to proceed

This basic FAIR analysis is composed of 11 steps within 4 stages

- **Stage 1 To identify scenario components**

    - 1) To identify the assets at risk: all the assets that are concerned are listed.
    - 2) To identify the threat community under consideration (Human, malware…): Here all the different threat community will be listed and documented.

Threat community: _____

Description	

Figure 11

- **Stage 2 To evaluate Loss Event Frequency (LEF)**

    - 3) To estimate the probable TEF: The threat event frequency is estimated.
    - 4) Estimate T-Cap: Here we estimate the threat capability to see if the threat can come from isolated individuals or on the contrary lambda people.

Rating	✔	Description
Very high (VH)		Top 2% when compared against the overall threat population
High (H)		Top 16% when compared against the overall threat population
Moderate (M)	X	Average skill and resources (between bottom 16% and top 16%)
Low (L)		Bottom 16% when compared against the overall threat population
Very low (VL)		Bottom 2% when compared against the overall threat population

Figure 12: Estimate TCAP

    - 5) Estimate difficulty: we do an estimation of the difficulty to accomplish the threat.
    - 6) Derive vulnerability: Here we will create a matrix difficulty/T-Cap that will allow us to visualise the vulnerability.
    - 7) Derive Secondary Loss Event Frequency (SLEF) : Now we will create a matrix threat event frequency/vulnerability, that will allow to visualise the loss event frequency.

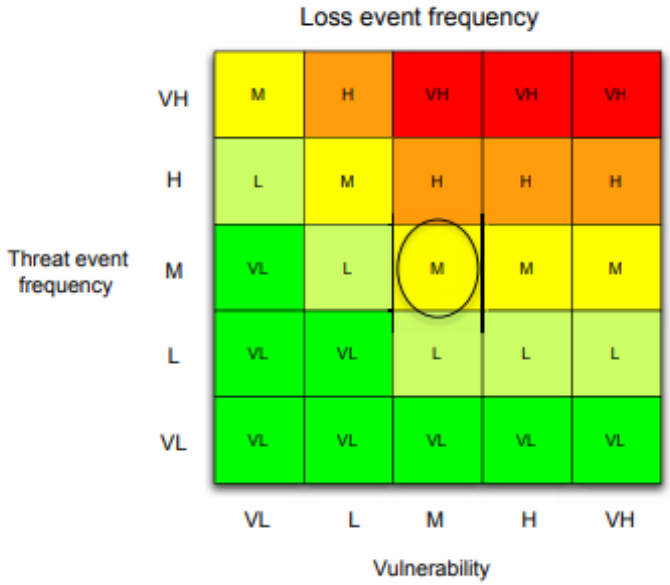


Figure 13

- **Stage 3 To evaluate LM**

  - 8) To estimate Probable Loss Magnitude (PLM): This will allow the management to determine whether or not the responses are sufficient to cover the losses.

Magnitude	Range Low End	Range High End
Very high (VH)	$1M	–
High (H)	$100K	$1M
Moderate (M)	$10K	$100K
Low (L)	$1K	$10K
Very low (VL)	$0	$1K

Productivity	Response	Replacement	Fines & Judgments	Competitive Advantage	Reputation
	Moderate	Low			

Figure 14

  - 9) To estimate SLM : this is the Secondary Lost of Magnitude, it is the same output than the previous point but for the secondary loss.

- **Stage 4 To derive and articulate risk**

  - 10) To derive and articulate primary and secondary risk: Here we create a matrix loss magnitude/loss event frequency that will give the risk.
  - 11) To derive and articulate overall risk reflexion: and finally, we create a risk/secondary risk matrix to have an overall risk view.

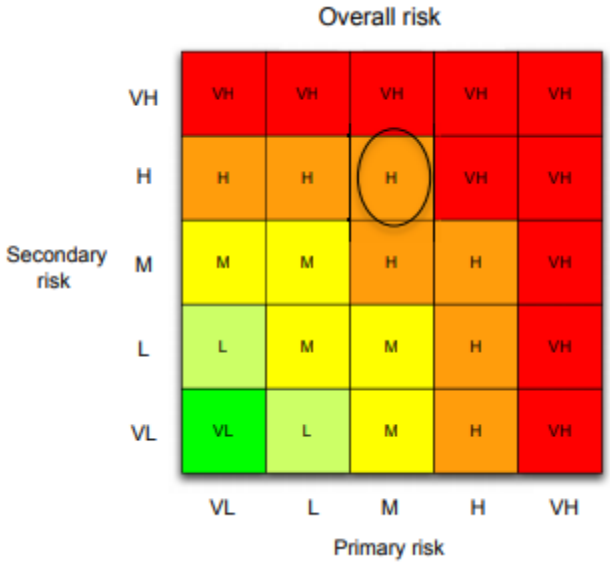


Figure 15 : overall risk

The produced outputs

- Modelling and tables that will allow the management to make decisions.

Synthesis

The interesting things about this methodology:

- It brings a quantitative approach. This is something more objective for the management. This can help them to make better decisions for the organisation.
- All the involved organisations, the execution, the application of the guidelines depend on the management support.
- The book of knowledge is heavy to read
- Not enough tool or template provided to help implement the methodology
- A certification is required to correctly implement this methodology.
- Like we can see in the following table it is possible to use other techniques to help us for some of the steps during the risk analysis.

Like EBIOS, this methodology seems oversized for smaller companies, especially when you see the complexity and the time it takes to understand and analyse it. Again, the risk management methodology is clearly done for the management, but we can see that there is an execution role that will ensure that the decisions are applied. I did not find this element in EBIOS for example. If the execution roles have the motivation and the tools, we could imagine workshop to raise the awareness of the developers on the data privacy for example. And if it is not working, the framework allows to send feedbacks to the decision management.

Block	Outputs	Contributors	Target users	Complementary methodology, technique
Decisions	-policy document -process definition -technology authorised	-management	-company	
Execution	-feedback on his capabilities	-execution roles	-management	
Risks	-feedback on the risks	-operational roles	-management	
Scenario building	- affected affected, by who or what, the threat type and the effect on the asset.	Any members of the organisation	-management	-use an attack tree -CIA framework
FAIR factors	None	Any members of the organisation	-management	-DFD -stride -LINDDUN (depends the on context of the scenario)
Expert estimation and PERT	-raw estimation and data	-Any members of the organisation -expert	-management	
Monte Carlo engine	-report with all the risk quantitative analysis	-compilation by a tool	-management	

Criteria

Time to implement: Long

Justifications

- The book of knowledge is long and not easy to read / understand
- The missing tools or template make the workshop long to implement
- All the hierarchy must be involved

Level of skill: Advance

Justifications

- The book of knowledge is long and not easy to read / understand
- A certification is required to be able to correctly implement it

Readability: comprehensible

Justifications

- The modelling produced by the tool help to have a nice overview
- The quantitative approach makes it more concrete

Scope: Detailed

Justifications

- This methodology allows to go deep in the details.
- Focus on the assets of the organisation
- Take into account the context

OCTAVE

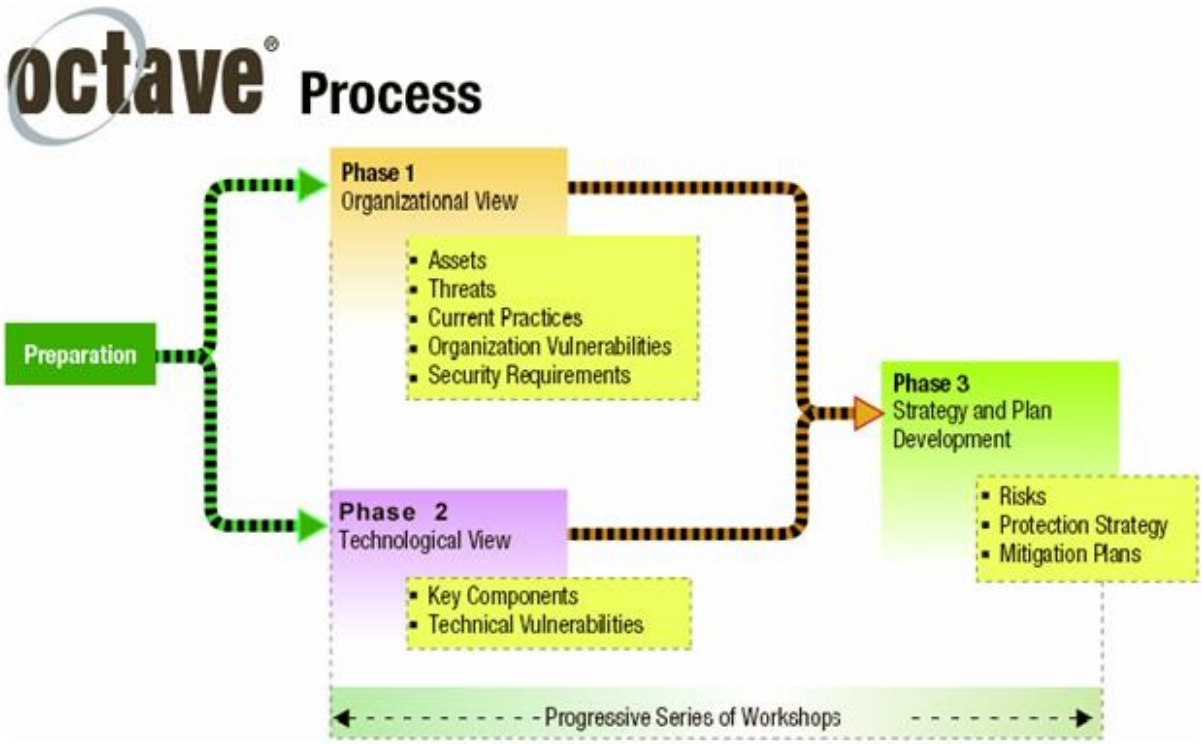
Origins

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was released in 1999 by the Software Engineering Institute. It has been requested by the department of defence. The last update was in 2007[23]

Purpose

Octave will allow a company to compare the cost of the vulnerabilities discovered with the cost of the implementation of mitigation plans. In order to do that it will use a catalogue of good practices, templates, workshops to gather a maximum information. With this methodology we can implement mitigation plan without waiting for the decision of the management by using existing guidelines of the organisation for example. This methodology is conducted by a dedicated team within the organisation to ensure that all the stakeholders in the organisation could be part of the process. This methodology strongly suggests that the assessment is done by internal stakeholders. Conducting an assessment by a third-party company could lead to misevaluate an asset and could lead to unnecessary mitigation plan.

Contrary to the two first analysed methodologies, OCTAVE is not a continuous process. It has a beginning and an end. So, it is important to set some markers on signals that will relaunch this assessment work (change in law, new data privacy regulation, etc.).



- *Figure 16: Octave source [CERT http://www.cert.org/octave/, 2008.]*

The outputs of this methodology are intended for the management that must deal with the risks. OCTAVE framework is optimized for medium and big companies (more than 100 people for OCTAVE-S). [24] OCTAVE has 3 declinations:

- OCTAVE: This is the original one. (last 2001)
- OCTAVE-S: This modified version is adapted to smaller organisations (2005)
- OCTAVE Allegro: This approach is straighter forward, and it will focus on information asset. (2007)

Process

In the context of this analysis, we will focus on OCTAVE Allegro. This methodology approach is more asset centric and is composed of 4 phases and 8 processes. The goal of this method is to provide a good risk assessment analysis without being an expert in risk assessment. It is very important to successfully implement the OCTAVE method to use and to understand the suggested worksheet of the methodology.

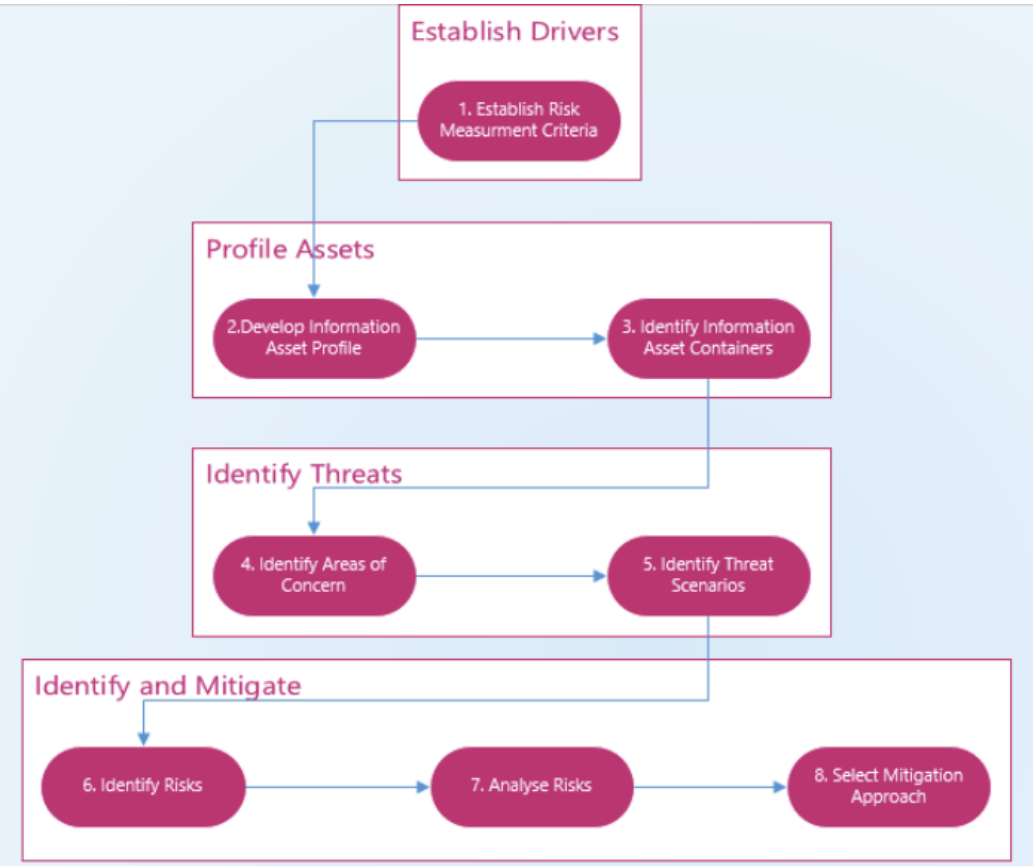


Figure 17: Octave Allegro processes

Establish Driver

The objectives

In this phase, we are going to decide what the risk criteria are and how to evaluate them. Of course, the result of this phase will be different for each organisation and assessment since the context is always different.

The contributors

The contributors will be the dedicated team which should be composed of internal stakeholders and possibly external experts. (It could be one person)

The steps and how to proceed

For this phase there is only one step which is:

- To establish risk measurement criteria

  In this step, the methodology requires all the sectors and assets where the organisation could be impacted to be listed. Once this is done, measurement criteria must be decided to evaluate the effect that a risk could have on it. In this methodology, the criteria will be qualitative, and they will reflect the organisation view.

  In addition, the processes or assets that are more critical than other if attacked, should also be identified. This will allow to set a prioritisation in the assets.

To help with this step, the methodology provides worksheet templates to create the criteria on the identified areas and prioritise them.

The produced outputs

- A list of defined criteria's for the different assets, areas and their prioritisation.

Asset profile

The objectives

Like we said before, the methodology is asset focused. In this step, we will focus on those assets and create a profile. A profile will be composed of:

- The features
- The qualities
- The characteristics
- The value

If the methodology is correctly followed, the assets will be correctly described, the scope of each asset will also be correctly defined as well as the security requirements.

The contributors

The contributors are the dedicated team that should be composed of internal stakeholders and possibly external experts. (It could be one person)

The steps and how to proceed

This phase is composed of 2 steps:

- To develop an information assets profile

  Information asset is very important in the OCTAVE methodology. It is a definition of all the organisation goods that have value. In this step, they will be listed and documented. Each asset will have its own sheet that will be used later for the threats identification.

- To identify information assets containers

All the information assets that have been listed in the previous step must be stocked somehow. In this step, information on the storage means it will be collected (hardware, databases, paper, etc.) In order to do that the team will map each asset with all the containers it depends on. Those containers englobe all the places where the assets are processed.

The produced outputs

- A list of all the containers where the data is processed.
- A mapping between the data and those containers.

Identity threats

The objectives

The goal of this phase is to detect the threats on the identified assets in their environment. Once these threats are detected, they are properly documented.

The contributors

The contributors are the dedicated team that should be composed of internal stakeholders and possibly external experts. (It could be one person)

The steps and how to proceed

- To identify areas of concern
  In this step, we will start with the proper risk identification. Scenarios that could lead to a data breach will be detected through brainstorming. The goal of this step is not to have a full list of threat scenarios for each asset but it is more about to quickly capture the first areas of concern that pops in the mind of the team.

- To identify threat scenarios
  Here, we are going to use the areas of concern from the previous step and create with them threat scenarios. They will bring more details to the threats. The problem is that if we only use the team knowledge to detect threat we risk missing some. In order to avoid that, in the second part of this step, we will use threat tree to identify remaining threats. This step will be also used to add the probability in the documentation of the threat. However, at this step, it is not easy to exactly quantify the probability. So the methodology requires to use the following assessment: low medium high.

The produced outputs

- A list of documented threats with their probability

To identify and mitigate

The objectives

During this phase, the identification of the risks and the mitigation plan will be put in place by using the identified threats.

The contributors

The contributors are the dedicated team that should be composed of internal stakeholders and possibly external experts. (It could be one person).

The steps and how to proceed

This phase is composed of 3 steps:

- To identify the risks

  Here, for each identified threat and their identified consequences, the impacts if the threat happens is analysed, all the impacted points in the organisation are assessed. This will result in a list of the corresponding consequences for each threat.

- To analyse the risks

  Here the impacts if the risks occurred will be quantitatively measured. Each of them will receive a value. To give this value the different impacted point, their consequences and the probability that it happens will be used. This is different for each organisation because they all have different assets importance (reputation, data, etc.). Now that we have that, the management should be able to make decisions on which risk to mitigate or to accept. OCTAVE provides a method to quantify the risks. If an organisation correctly prioritises the impact criteria's, it will allow the risks to be treated according to these priorities.

- To select a mitigation approach
  Finally the risk plan is defined. Most of the time, a grid is defined with different zones. The risks are displayed on that grid and depending on their zone, they are mitigated, deferred or accepted. [23]

The produced outputs

- A list of the corresponding consequences for each threat
- A list of the identified risks and their quantification
- A list of the mitigation plan

Synthesis

By analysing this 'famous' methodology we can see that:

- This assessment methodology is asset centric.
- By tailoring a little bit the assessment methodology, we can easily detect data privacy threats (by using LINDDUN for example).
- The steps of one iteration are fastidious but much clearer than EBIOS for example.
- The tool allows the tailoring and provides many worksheets to help with the implementation.
- Again, this risk management method has as target group the management. But the assessment team could be composed of all sort of internal stakeholders which could lead to a raise of the security awareness within the company.
- This method is mostly used by big companies.
- To be really efficient, it should rely on the business knowledge of the assessment team and the technical expertise of security.

The overall impression when we analyse this methodology is that you will need someone who is trained at OCTAVE, to know what to do during the workshops, which sheet to use, etc. It is clearly stated in their documentation that they recommend a training before implementing the

solution. Nowadays many IT companies that provide services count less than 100 employees and even OCTAVE-S that is intended for what they call ‘small companies’ would not quite fit.

phases	Outputs	Contributors	Target group	Complementary methodology, technique.
Establish Driver	- List of defined criteria for the different asset, area and their prioritisation.	-assessment team	-management	-elevation of privilege
Profile assets	-List of all the container where the data is processed. -Mapping between the data and those containers.	-assessment team	-management	-data flow diagram
Identity threats	- List of documented threat with heir probability	-assessment team	-management	-LINDDUN(to detect the data privacy threat)
Identify and mitigate	-list for each threat the corresponding consequences -List of the identify risks and their quantification -List of the mitigation plan	-assessment team	-management	

Criteria

Time to implement: Normal

Justifications

- The implementation of the eight different steps takes time but the phases are not complicated.
- Workshops need to be organised to produce the necessary lists (areas of concern, threat scenarios, risks evaluation…)
- The methodology provides many tools to help and can be completed by other tools to help.

Level of skill: Normal

Justifications

- The documentation is clear but extensive
- It requires experience to organise so many workshops and be sure to invite the correct people.
- According to the documentation, two days of training are sufficient to implement correctly the methodology

Readability: comprehensible

Justifications

- The produced matrix and the prioritisation is clear
- If needed additional arguments are available in the produced documents in the previous steps.

Scope: detailed

Justifications

- This methodology if correctly implemented provides a detailed list on the existing risks of an organisation.
- Again, business and technical knowledges are required to arrive to such appreciation

FRAP

Origins

For a long time, the risk assessment was delegated to external companies that had a lot of experience doing these tasks. The issue is that those analysis always take weeks and were expensive. Also, with this approach, the internal stakeholders were not taken into account and the expectations from the management were rarely met. Then of course the management was often reluctant to implement the recommendations and all the assessment was done for nothing. So, there was a need for a new methodology that considers the requirements of the management, the expertise of the internal stakeholders and that is much faster to deliver results. This FRAP (Facilitated Risk Analysis Process) methodology tends to all these new requirements. [30]

Purpose

FRAP will provide a method that will allow to conduct the risk assessment in-house and in addition it does not require an expert to conduct it. Good facilitation skills are on the opposite extremely important. The FRAP methodology is focused on the business needs and has an efficient and rigorous method to ensure that the business operations and the security risks are known and documented.

Process

Before and during the first month of use of the FRAP methodology in your organisation it is important to raise the awareness of the methodology to all the stakeholders. Like previous risk management methodologies that we analysed, if you do not have the necessary support from your management it will be difficult to correctly implement the methodology [30]. Usually the advantages that have been listed before such as the cost efficiency and the rapidity of results should convince the management. The methodology defines several roles:

- The facilitator: he could be seen as a scrum master.
- The FRAP team: which could be seen as the resources available for the project. (between 7-15 peoples)

The methodology suggests 3 workshops:

Workshop 1: The Pre-FRAP workshop

The objectives

This first workshop is very important. It is a short one (less than an hour). The goal will be to gather 5 key components that will be used for the rest of the assessment.

The contributors

- The business manager
- The team leader
- The facilitator

The steps and how to proceed

This meeting has no defined structure but it is required that the following points are defined:

1. Scope statement
   It is important that the business manager and the project lead express clearly the scope of the study.

2. Visual
   A visual modelling of the assessed process needs to be created. It will be used during the study to show to the other participants where the scope of the process is.
3. Nomination of the FRAP team
   The methodology says that a FRAP team should be composed of 7 to 15 peoples.
4. Meeting structures
   This meeting leader is the business manager, so he is responsible of the organisation.
5. Confirmation of the definitions
   It is very important to agree on the definition of the integrity, confidentiality, availability and all the criteria's that are taken into account for this study. Also you have to be sure that the notions used by the methodology (Risk, control, impact and vulnerability) are well defined and understood.

During this meeting the process of prioritisation of the threats needs to be defined. The methodology suggests two ways to achieve that:

1. The team reviews all the threats without considering the existing controls. The advantages are that it will define what the perfect controls are and we will be able to show the gap between what currently exists and what should be in place.
2. We consider the existing controls.

The produced outputs

- Clear organisation set documented
- Documented agreements on the scope and the key points of the methodology

Workshop 2: The FRAP workshop

The objectives

During this workshop the FRAP team will identify the risks, prioritise them and define a mitigation plan.

The contributors

- The owner
- The project lead
- The facilitator
- The scribe
- The team members

The steps and how to proceed

There are four phases for this workshop:

1. **The preliminary phase**
   In order to introduce the workshop, the scope of the study will be presented to the team. A technical profile will introduced, the visual produced during the pre-FRAP meeting and then a copy of all the definition agreed on during the pre-FRAP meeting will be distributed to everyone.
2. **The brainstorming process**

During this phase all the criteria's will be analysed (integrity, confidentiality, etc.) and for each team, the risk, the threat, the concerned will be identified. The methodology provides precise process in order to realise this phase.

3. **The risks prioritisation**
   In order to prioritise the risks, the team will use the definition that they received during the introduction. An example of definition could be:
   - High sensibility: …
   - Medium sensibility: …
   - Low sensibility:
4. **Mitigation plan for relevant risks**
   The methodology provides a list of mitigation plans that allow to control the risks. When the FRAP team received the invitation, they also received this list. It will be used as a starting point to create a mitigation plan.

The produced outputs

- A list of the identified risks
- The prioritisation of the risk
- The needed controls

Workshop 3: The post-FRAP workshop

The objectives

During this step, we finalise the reporting for the management by regrouping all the information received in the previous meetings.

The contributors

- the business manager
- the project lead
- the facilitator

The steps and how to proceed

During the meeting, the first document will be established by the facilitator. It is the cross-reference sheet. This is the document that requires most time to be produced. Each mitigation plan needs to be linked with the risk that it will be control. Once this is done, the cross reference sheet and the mitigation plan are sent to the business manager. After reading a first time the document the business manager, the project lead and the facilitator meet to review the documents and recommend the necessary mitigation plan.

The produced outputs

- The cross reference sheet
- The identification of existing mitigation plans
- The final report

Synthesis

According to the documentation, this methodology is one of the most used today. After analysing it we can say the following:

- The FRAP methodology is cost effective.

- It requires many people through the hierarchy.
- It is fast to implement.
- It provides very specific tools and method to use. Even the structure of the workshops is explained.
- The output is for the management which will decide what to implement.
- The methodology is easy to understand and does not require expertise, but the facilitator needs to have very good organisational and communication skills.
- Not possible to associate another tool to complete the methodology
- There is no real need to use other methodologies or tool to complete this one.

This methodology relies more on the human experience of the internal stakeholders rather than predefine classification given by a sheet. All the actors of the organisation take part into the process, which allows to cover all the points of view.

Workshop	Outputs	Contributors	Target	Complementary methodology, technique.
Pre-FRAP meeting	-Clear organisation set documented -Documented agreements on the scope and the key point of the methodology	-The business manager -The team leader -The facilitator	-facilitator -FRAP team	
FRAP meeting	-List of identified risks -Prioritisation of the risk -Controls needed	-The owner -The project lead -The facilitator -The scribe -The team members		
Post FRAP meeting	- The Cross Reference Sheet -Identification of existing controls -Final Report	-the business manager -project lead -facilitator	-management	

Criteria

Time to implement: Normal

Justifications

- This methodology according to the documentation could be done in 4 to 6 days.
- There is still the availability of every contributors that could cause issue for the workshops

Level of skills: Normal

Justifications

- Even if according to the documentation no expert skills are needed, the soft skills are extremely important.

Readability: comprehensible

- The produced documents meet the requirement of the management
- They are explained and reviewed during the post-meeting
- The manager is advised on the mitigation plan to adopt

Scope: Low

- The study is focused on one business need at the time
- It would require a lot of iteration to cover all the business requirements of a big company.

Discussions

After analysing those methodologies, we can already draw some points of attention that we could use for the comparison between risk management and assessment and the threat modelling approach.

- The risk management process is performed by someone dedicated to this task.
- It requires to acquire the knowledge of the organisation or project via documentation, interview, workshop…
- The risk management is an exercise that should start at the beginning of a project but could be executed later to assess the state of security of the project.
- It is always a cyclic event that should be executed by the detection of event (Architecture changes for example)
- In the documentation of these risk management methods, the concept of management or organisation is frequently used.

	EBIOS	FAIR	OCTAVE	FRAP
Quantitative approach	X	X	X	
Qualitative approach				X
Requires management	X	X	X	X
Small company <50		X		X
Big company >50	X	X	X	X

Chapter 4: Analysis of threat modelling method

Like for the risk management, the choice of the correct threat modelling method is essential if one wants to detect and assess correctly the threats in his project. In this chapter, five methods will be described and analysed. In order to select the five methods that I will analyse, I first did a quick survey of the existing tools and I selected 5 tools that I found very interesting for this study. I selected two that have a defender point of view and one with an attacker point of view, one that is more cooperative and a last one that is focused on the data privacy threats.

- DFD (Data Flow Diagram)
  The data flow diagram is one of the most important modelling. It does not actually represent a threat modelling technique, but this representation is very important to understand since many threat modelling techniques use this data flow diagram. That is the reason why we are going to explain it in detail.
- Microsoft STRIDE

  STRIDE is one of the most popular threat modelling method.

- Elevation of privilege

  It is a method based on a card game. This approach is very interesting and entertaining.

- T-MAP: a methodology that use an attacker point of view
- LINDDUN

  LINDDUN is a method that is based on a data flow diagram and can be realised on several levels. Like the OCTAVE Allegro methodology, this method focuses on data assets. This could be very interesting also for data privacy assessment, in order to detect possible data breach for example.

Comparison criteria

To be able to compare the threat modelling methods with the risk management/assessment methods that we previously analysed we will use the same criteria's to evaluate them.

- Time for implementation
- Necessary skills(complexity)
- Results readability
- Scope covered

See point comparison criteria's from analysis of risk management methodologies for the details.

The same structure used for the risk management analysis will be used here for the threat modelling analysis.

- Origins: explain where, how, the methodology has been created
- Purpose: the goal of the methodology.
- Process: all the process defined in the methodology.
- Reflexion: A first analysis of the methodology, the advantages and disadvantages.

DFD

Origins

DFP (Data Flow Diagrams) are used since 1970. They have been introduced by E. Yourdon and L. Constantine. It was a way of visualising software designs before the Uml diagrams arrive.

Purpose

This threat modelling tool is very easy to implement and is most of the time used to model the security relevant part of the system. One other advantage is that the diagram produced is easy to understand and extended. [29] The data flow diagram consists to modelized how the data are processed by an information system by looking at the input and the outputs. It will have a particular attention on the flow of information, where are they? Where are they going and how? Where are they stored?

Process

The notation

There are two types of notations for the data flow diagrams, each of them represents differently the four main objects used for these diagrams which are:

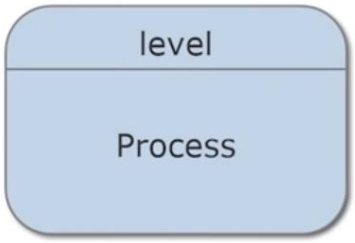
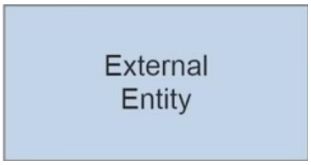
1. Data flows
2. Processes
3. Data stores
4. External entities

Like we said there is two different types of notations

1. The one from Yourdon
   This one is more used for the system analysis and design.
2. The from Gane & Sarson
   Their representation is more used to represent information systems.

Let us compare the two notations and define what they mean. (see the table below to see the representation)

1. **Data flows**
   The data flow represents the means of the information used to travel. The two notations are the same, if necessary, we add information about the data that is transferred.
2. **Processes**
   A process will change the data flow that is considered as input into another data flow that will be considered as output. A process could represent an update on the data, a reformatting, an encryption…
3. **Data stores**
   The data store represents the container that will keep the data. It could be a piece of paper, an external drive, a no-SQL database, etc.
4. **External entities**
   The external entities are the ones that do not belong to the information system. We can say that the data flow that are coming and going to these external entities represent the inputs and the outputs of the modelized system.

	Yourdon's notation.	Gane & Sarson's notation.
Process		
Data flows		
Data store		
External entities		

The layers

Data flow diagrams are composed of different layers. This will help visualizing different information system.

- The context diagram
  This is the top-level diagram, it can also be considered as level 0 diagram. It always contains only one process which is the process 0. The process 0 will represent the process of the entire information system and his interaction with the external entities. You can see in figure 34 an example of level 0 Diagram. We can see in the middle the process 0 that represent the process done by the entire system, and all the external entities on the outside that interact with the process 0 via data flows.

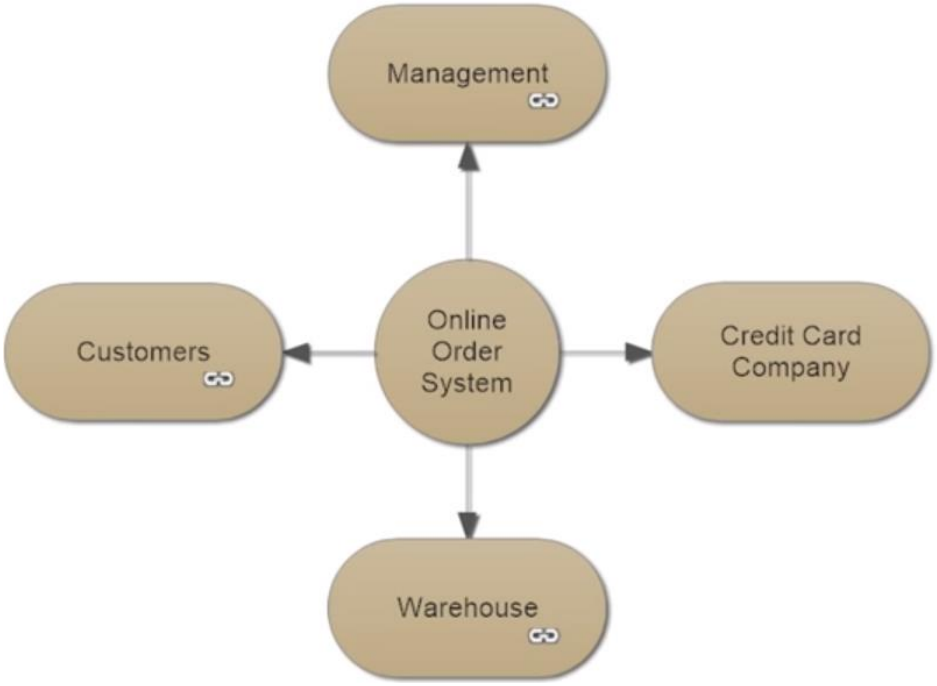


Figure 18: Context diagram source [34]

- The level 1 layer
  Each of the object that are in the context diagram could be define. Therefore, we have also a level 1 diagram that will define more in detail the data in the level 0 diagram. In the figure 19 we can see an example of the level 1 diagram that will detail the warehouse external entity that we had in the level 0 diagram. Note that the other notation could be used to represent object. For example, here a computer image was used to model the fact that the receipt are encoded into the app by a computer.

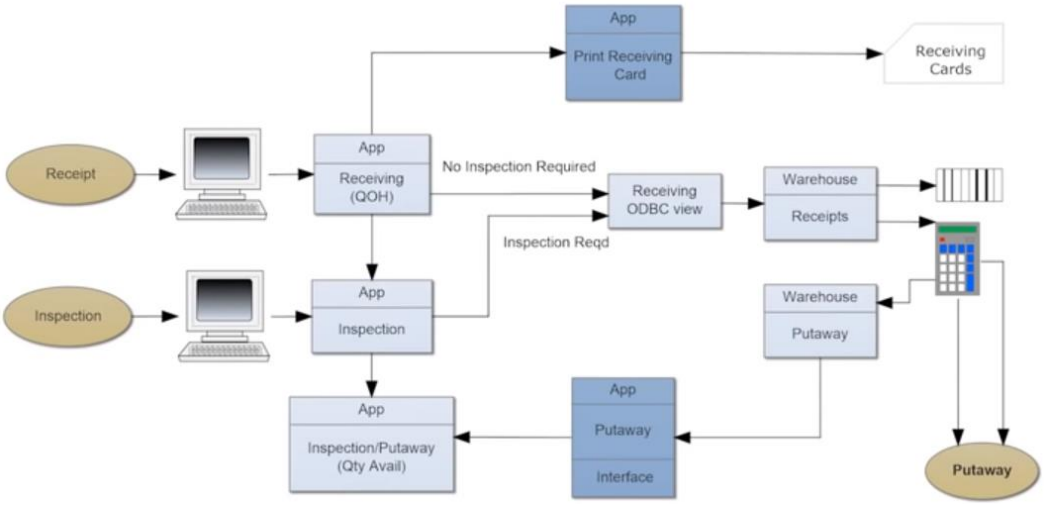


Figure 19: Level 1 diagram source [34]

From there we could go into more detail by adding a new level diagram that could analyse the data of the Putaway external entities. We can continue this iteration as long as it is necessary. Of course, we have existing tools that will help us create these data flows and also navigate through the entity and the different levels.

- Pseudocode
  At a certain point, you will reach the pseudo code representation. It is like a coding language, but it is meant to be read by human.

Synthesis

What we discovered by analysing these tools:

- This data flow diagram is a visual modelling so it is easy to read for novice
- The notation is simple
- It allows to have a top down approach
- It allows to continue the levels until the pseudo code is reached
- The data flow diagrams do not require any expertise or experience to be used

Like we said in the introduction this tool is not really a threat modelling tool, but it was very important to explain in detail how it worked since this method is used by a lot of threat modelling techniques. And finally, the result is not only at the destination of the manager but like we saw, it can be also very useful for the developers since they could go as far as the pseudo code to see the logic for example.

Criteria

Time to implement: Fast

- There are only four notations to learn
- There are loads of tools available to do such modelling

Level of skill: None

- There is no need for special training or certification

Readability: Easy

- It is a visual tool with only four different notations to understand
- It is a visualisation by level, for example a manager does not need to go deep into the levels, but developer could!

Scope: Low

- If we take only iteration of the dataflow diagram the scope will resume only to the studied system. To have an overview of all the systems, the diagrams must be done for all the systems.

STRIDE

Origins

This framework has been developed by Microsoft. The word STRIDE represents the six threats categories:

Spoofing: When attackers try to fake the identity of someone else.

Tampering: When attackers try to intercept and alter the communications.

Repudiation: When attackers succeed in preventing the discovery of the link between their actions and their identity.

Information disclosure: When attackers intercept data.

Denial of service: When attackers successfully interrupt a service.

Elevation of privilege: When attackers succeed in gaining access right that they are not supposed to have.

Purpose

The reason Microsoft decided to use this threat modelling technique is quite simple. They wanted something cheaper, faster, and easier to use to detect and mitigate the risks. Like wat we saw in the previous chapter on the analysis of the risk management methodologies, is that they can be time and money consuming, they are done most of the time at the organisation level for the management and their results are sometimes not even considered. With the threat modelling Microsoft wanted to bring a tool more accessible by the project team that could be easily used and that will allow to have sufficiently detailed results.

Process

The Microsoft threat methodology is composed of four steps (see figure 20). The workflow can be relaunched when it is needed, for example, if an output is added to the system information or by adding a new way of interacting with the system.

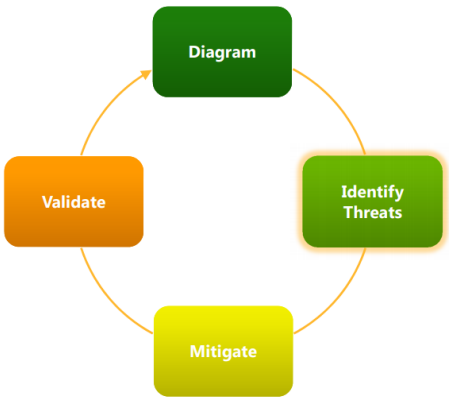


Figure 20: SRIDE workflow [35]

Diagrams

The objectives

The goal of this phase is first to define the scope of the study and to model it with a data flow diagram. The dataflow that is created will be used during the next steps.

The contributors

- The development teams
- The project manager
- The analyst

The steps and how to proceed

We will not come back on how to do a data flow diagram since it has been fully defined in the previous point. Nevertheless, it is important that Microsoft threat modelling added a new notation to this diagram that will represent boundaries.

There are three new boundaries introduced by Microsoft (see figure 21):

1. Trust boundary
   They will model the fact that two components do not trust each other. For example, there could be a trust boundary between a component that requires a login and another that does not.
2. Machine boundary
   This marks the frontier between to servers or machine.
3. Process boundary
   This will model the start or the end of a process. For example, when a command has been encoded and then start the preparation.

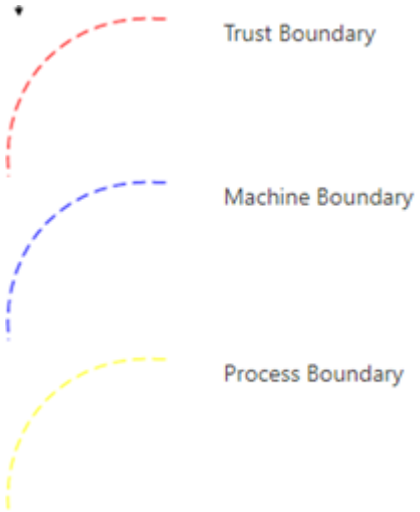


Figure 21: Boundary notation

The documentation says that most of the time a level 1 diagram is enough except in certain very complex system.

Also, during this step all the security assumption must be listed like the presence of a firewall or the possibility of an attack by social engineering.

The produced outputs

- The data flow diagrams enhanced by the boundaries
- A list of existing security measures
- A list of known threat.

To identify threats

The objectives

The goal here is to take all the identified elements in the dataflow diagram and map them to threat categories. In other to that we will use the STRIDE threat categories that we defined before.

The contributors

- A security expert OR the project team helped by the attack tree that STRIDE provides.

The steps and how to proceed

There are two different ways of doing this step, it will depend on the contributors.

1. The security experts are available
   In this case, the security experts can brainstorm together, review all the diagrams and map all the existing threats.
2. No experts are available and the project team is performing the steps.
   If there are no experts available, do not panic, if you remember one of the goals of the Microsoft threat modelling methodology was to make the process available for the project team. In order to do that, they just have to follow a simple algorithm:
   “

```
For each item in Diagram DO
        Switch item.type
                Case(process)
                        Apply STRIDE;
                Case(Data STORE)
                        Apply TID;
                Case(entity)
                        Apply SR;
                Case(data flow)
                        Apply TID;
        End switch
End For ”
```

The produced outputs

- A list of all threats categorized in the STRIDE model.

To mitigate

The objectives

The goal of this step is to define mitigation plan for the vulnerabilities. This is of course the most important step since it will allow give the means for the information system to be secure.

The contributors

- The developers
- The project manager
- The analyst

The steps and how to proceed

Again, to define a mitigation plan with STRIDE there is no need to be a security expert. STRIDE provides a threats list for all the mapping that was done in the previous step that should be taken into account. In figure 22 you can see one of the tree provides by STRIDE.

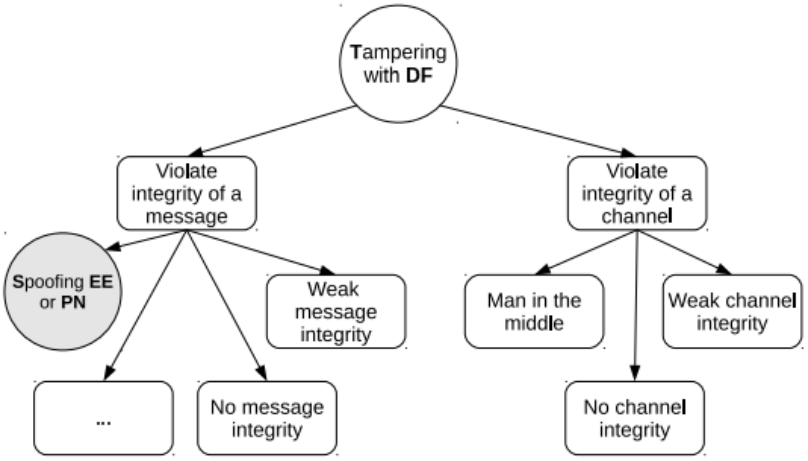


Figure 22: STRIDE tree check [25]

So the team needs to do for each mapping go through the trees and see and assess what could trigger a threat. For the mitigation, if you can easily put it in place, do it, if not the methodology advises to restrain from trying. Mitigation is the role of experts.

The produced outputs

- A list of risks
- A list of advised mitigations

Validate

The objectives

In this step all threats will be documented.

The contributors

- The project lead
- The developer team
- The test team
- The quality officer

The steps and how to proceed

The methodology does not provide a specific template for this step. In the community the misuse case is the format generally used for this phase. This step will be a check of all the previous ones.

- Is the data flow diagram correct?
- Do we have all the threats?
- Are their correctly mapped?
- Do we have mitigation for all the threats?

The produced outputs

- A document with all the threats defined.

Synthesis

During the analysis of this methodology we pointed that:

- The produced output is more for the development team than for the management
- The methodology does not require to be an expert (except for the mitigation plan)
- This methodology can be started by the project manager
- It involves the development team

We can clearly feel that the purpose of this methodology is to detach the heavy workload that a classical risk management brings. It is much easier and faster to implement and provides tool that allow non experts to conduct the study.

	Output	Contributors	Target users
Diagram	-Data flow diagram enhances by the boundaries -List of existing security measures -List of known threat.	-The development teams -The project manager -The analyst	-The project team
Identify threats	-List of all threats categorized in the STRIDE model.	-expert or project team	-The project team
Mitigate	-List of risks -List of advised mitigations.	-project team -expert if mitigation is too complex	-the project manager -the pen testers
Validate	-A document with all the treat defined.	-The project lead -The developer team -The test team -The Quality officer	-The project team

Criteria

Time to implement: Fast

Justifications

- This methodology does not require to involve all the hierarchy
- It focuses on one project/system
- It does not require a lot of workshop

Level of skill: None

Justifications

- The steps are straight forward
- The data flow modelling and the STRIDE classification makes it easy to implement
- The methodology is easy to understand

Readability: Easy

- One could use the data flow diagram and visually explain where the threats are.
- There is not a lot of document created.
- The target audience is partially the one who did the study.

Scope: Low

- It does not take into account the organisation parameters.
- It focuses on one project/system.
- Some threats could easily be missed.

Elevation of Privilege

Origins

This tool has been developed by Adam Shostack and it uses the classification from the STRIDE methodology.

Purpose

The threat modelling tends to be used by only one person, and sometime by juniors since they are easy to implement. Therefore, this task is not always rewarding. The purpose of this tool is to make threat modelling a fun and cooperative activity. It will encourage each participant to participate and they will get an instant feedback on their proposed threat. Also, by trying to fit the threat card to win, the players will be creative which is a good thing to be sure not to miss a threat.

Process

The objectives

The goal of this game is to:

- Win the game!
- Detect the threat on the studied system.

The contributors

- The project team

The steps and how to proceed

First, like for the Microsoft threat modelling methodology, a data flow diagram must be drawn. In the figure 23 we can see an example.

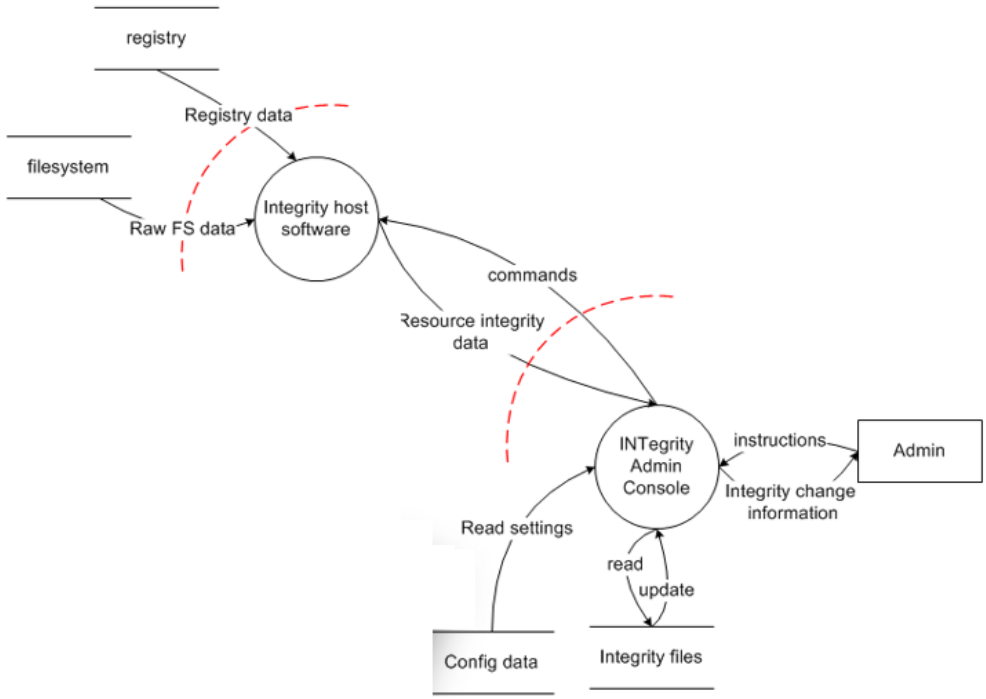


Figure 23: data flow diagram example [source Adam Shostack]

This tool that is in fact a card game composed of 84 cards. See figure 24 an example of card. Each card has 3 information on it:

- The threat classification
  One of the 6 STRIDE categories
- A text with an example
  This is the threat that they have to try to put on the data flow diagram.
- The value
  Depending on the threat, the classification can go from 2 to King

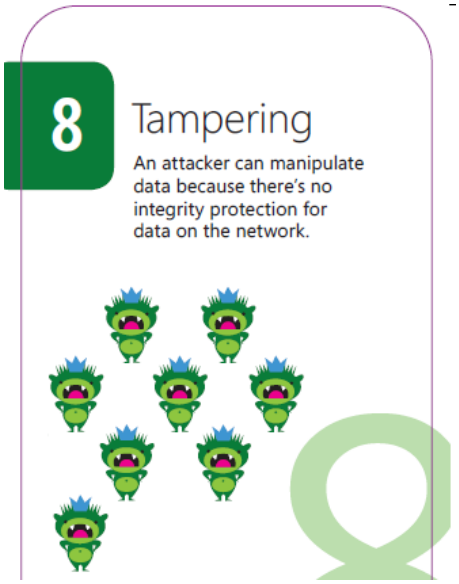


Figure 24: EOF card

The deck is distributed to all the participants (between 3 and 6 people). The one who is starting to play is the one having the 3 of tampering. So, for example the first player reads the text on his card and places it somewhere on the data flow diagram (see figure 25).

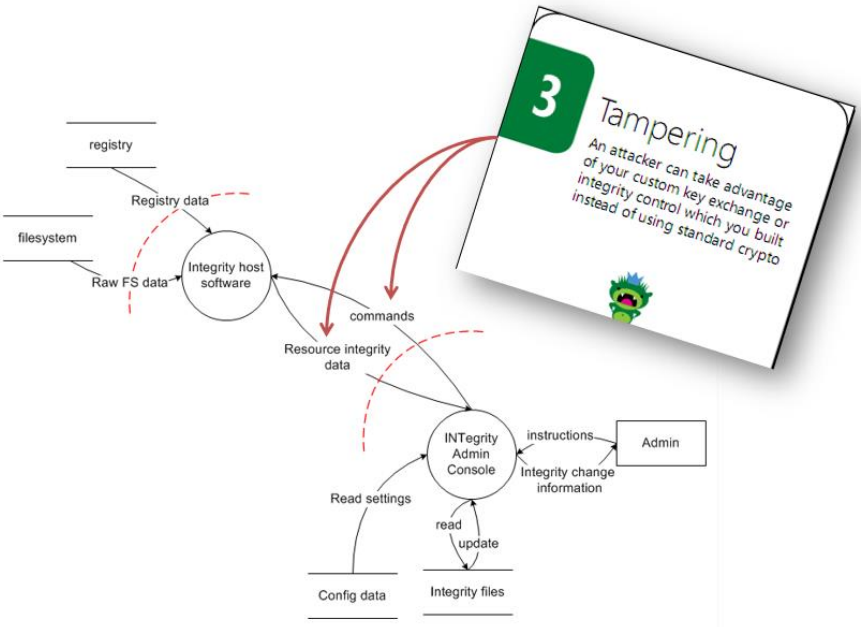


Figure 25: card played by James

Of course the other participant contests this card and then the player needs to argue on why he finds that the element targeted is threaten by the card he just played. If the player accepts finally the card, a 'bug' is created with the justification, the player who played the card and the score (see figure 27). The next player can play one of his cards with the same category (see figure 26) and continue the game.

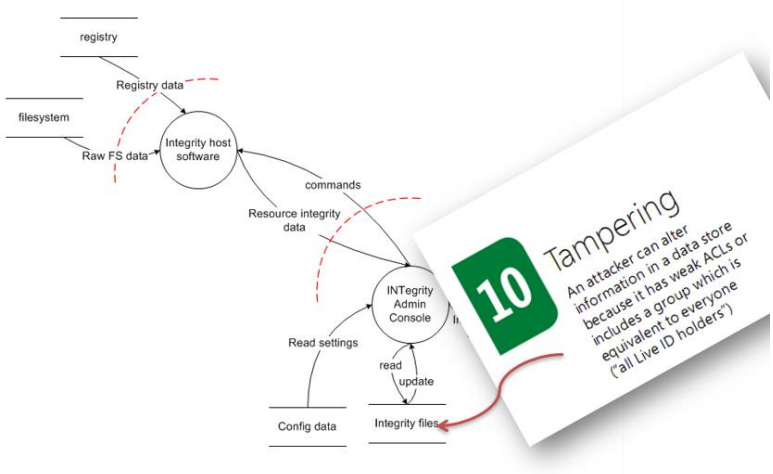


Figure 26: card played by Manu

Player	Points	Card	Component	Notes

Figure 27: notes taken for each hand

If a player does not have a card in his hand with the same category, he can play another category.

After each round, the winner is the one with the highest score. An elevation of privilege card can also be played and in this case, it is the highest valued card that wins.

For the next round, the winner of the previous game can choose the category of the card.

The produced outputs

- A list of documented bugs

Synthesis

- The originality and the fun approach of this game will motivate the team to find threats.
- The players are not afraid to raise issues that could sometimes be known but voluntarily hidden.
- Since all the items of the diagram are not systematically analysed, it could lead to undetected threats.
- It does not consider the organisational threats.
- It pushes the developer to be creative.

- It raises the awareness of the team.

When we read the rules of this tools, we can help to compare it to the poker game used in some Agile implementation methodology. For companies that already have this kind of approach,

It is a perfect tool, and we could imagine having different skills assembled around the table which would bring more points of view and accuracy in the results. Also, like all the cooperative tools, it allows to raise the knowledge of the employees.

	The contributors	The outputs	The targeted group
The game	The project team	-a winner! -a list of bugs for which a control must be found.	-The team that will decide how the controls need to be implement.

Criteria

Time to implement: Fast

Justification

- Very easy to put in place.
- Can be initiated by the project leader without the hierarchy involvement

Level of skill: None

Justification

- Everyone can participate and learn!

Readability: Easy

- Simple list of threats for each component.

Scope: Low

- Like for the STRIDE technique it focusses on the application on a more technical level. It does not take into consideration the organisation parameters.
- If the level of knowledge of the players is too low threats risks to stay undetected.

T-MAP

Purpose

This framework has an asset centric approach. For T-MAP (Threat Modelling Attack Paths analysis) if we have a lot of unsecured access to the system. It means that there are many risks that this system is attacked. It also takes into consideration on which system the access is. If the access allows to consult the lunch menu of the canteen it is less sensitive that the personal data of the employees. To define scenarios that could lead to a threat, T-MAP will use an attack point of view and it will use an "attack path" to detect the scenarios.

Process

The objectives

This framework will define a severity for all the different "attack paths" considering the technical level of the security vulnerability but also it will take into account the threats impacts. T-MAP will then quantify the threat by taking the total of the severity for all the "attack paths". [28]

The contributors

- The security expert.
- The stakeholders concerned by the study.

The steps and how to proceed

1. In order to determine what the valuable assets are, the expert will need first to list all the stakeholders and see what they consider to be the assets.
2. Then the expert need to assess the value of these assets. This will allow him to estimate the necessary security measures in order to protect them. (There is no need to put in place expensive security measure to hide the canteen menu)
3. Analysis based on the attack tree
   Each attack path will define:
   - What security breach the attacker could use to enter the system.
   - How the security criteria (confidentiality, integrity…) can damage the assets of the company. (data breach, reputation…)

In figure 28 we can see different attack path that could be used by the attackers. We can see that there are four layers in the conceptual business representation of an attack path. For each layer we have attributes that are used to describe them.

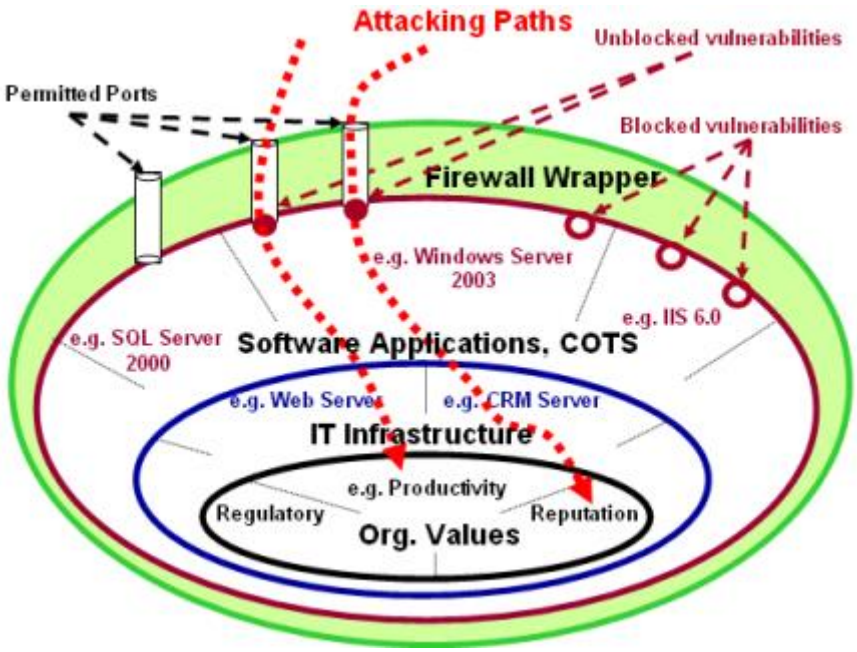


Figure 28 : Attack path. Source [Value Driven Security Threat Modelling Based on Attack Path Analysis]

The four layers are:

1. Access: The available access for an attacker
2. Vulnerability: That could be exploited by the attackers (OS, programmes not up-to-date, etc.)
3. Asset: The treasures to defend
4. Value affected

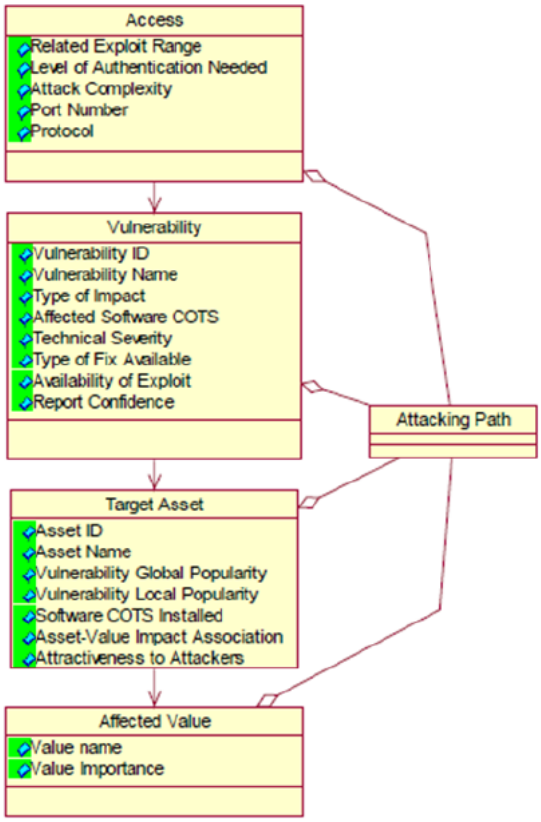


Figure 29: 22 layers attributes. Source [Value Driven Security Threat Modelling Based on Attack Path Analysis]

The next step is to give a value for each attribute that composes an attacking path. We can see the list of attributes in figure 29. When we add all the rated attributes we have calculated the attack path.

Finally, all the countermeasures that could mitigate the attack are evaluated. This will allow to choose the best solution to manage the risk.

The produced document

- Document that lists all the evaluated possible attacks.

Synthesis

After analysing this framework, we note that:

- This framework requires technical knowledge, it is not easy for a developer to put himself in the place of an attacker.
- One of the advantages is that if an asset changes we will not need to run a full analysis, we can just reassess the path that leads to this asset.
- It takes the organisation threats into account
- The results are very extensive and not intend for a simple developer
- It uses an extensive database as base of knowledge

This methodology was not easy to analyse. There is not a lot of literature on it and those that I found were very extensive and not easy to read and understand for someone with my experience.

	The contributors	The output	The target
Implementation	-Experts -Organisation ‘s stakeholders	- Document that list all the evaluated possible attacks.	-experts

Criteria

Time to implement: normal

Justifications

- The most difficult part is to gather all the informations, assets, values,etc.
- Part of the implementation is automatized.

Level of skill: Advanced

Justifications

- It requires specialized security knowledge.

Readability: complex

Justifications

- A very precise and technical description of each path that could lead to a data breach
- It requires security knowledge to understand

Scope: detailed

Justifications

- This framework allows to take into consideration threats from the project but also the organisation.
- It uses a huge database of knowledge to find the attack path.

LINDDUN

Historic

LINDDUN is a threat modelling methodology that was created by researchers at the Leuven University and published in 2015.

Purpose

The data privacy is something we have talked about a lot during these last two years. The cause is probably the new European data protection regulation that has been applied since May 2018. Because this field is very specific and requires regulations or law knowledge, the methodology will help the developers, the analysts, the architects to take into account the data privacy issues as of the beginning of the project (privacy by design) which by the way is required by the new European regulation.[31][32] One of the big advantages is that LIDDUN will allow non data expert to detect data privacy threats.

Process

LINDDUN is composed of 6 steps, three for the threats identification, and three to bring solutions to deal with the identified threats. Like STRIDE, LINDDUN allows the classification of threats in seven categories:

- Linkability
  This category gathers all the threats that could allow a personal data to be linked with other personal data of the same person. For example, if someone has my email address they could go on Facebook and link this email address with my name.
- Identifiability
  This could be linked with the previous category since the same example works. But let us take another example. If someone succeeds in to obtaining my address, they could do a search on the white pages and find my name.
- Non-repudiation
  This category regroups the threats where people could do some process or attackers on behalf of someone and there is no way to prove that they did it or did not. A solution for those threats could be logging for example.
- Detectability
  This one means for example if someone subscribes to a newsletter about European election, one could deduce that this person is pro-European.
- Disclosure of information
  This is more a security threat.
- Unawareness
  When collecting personal data, one must ensure that the data subject is correctly informed.
- Non-compliance
  This could be the result of all the other categories. If they are not sufficiently covered the information system and his context is not considered as compliant.

Now let us define 2 phases of the methodology that each consist in three steps.

Problem Space

The objectives

This first phase is the most important one in the methodology. It is here that the data privacy threat will be identified.

The contributors

- The project team
- The analyst
- The architect
- The project manager
- Eventually a data protection expert

The steps and how to proceed

There are three steps in this phase

1. To create a data flow diagram
   We know that this data flow diagram is a starting point for many threats modelling techniques. This will be used in the next steps. (Please Refer to Chapter Dataflow Diagram for more information.)
2. The second step consists in a simple algorithm like for the STRIDE methodology. For each element of the data flow diagram, check if one of the LINDDUN categories can apply. A little tips for that, if you go on their tree catalogues (figure 30) you can see where the item you are analysing can eventually fit. For example if you are analysing an entity you see that only linkability, identifiability and unawareness could apply.

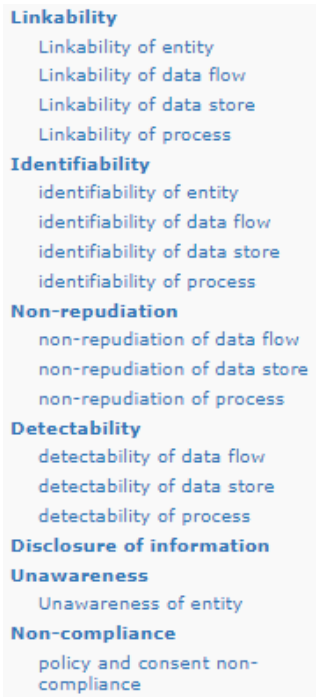


Figure 30: LINDDUN tree catalogue

This step will produce a table that will map each item of the data flow to a threat category.

3. To identify threat scenario
   This step consists in another small algorithm to apply, for each X that we identified in the LINDDUN template table in step two, we need to analyse whether a threat scenario exists. Here again we can use the tree catalogue to help to identify all the threat scenario. For example, let's say that in my table I have an entity that has an X in the linkability column. I click on the linkability of the entity that is in the figure 30, I will be led to a nice attack tree that we can see on figure 31.

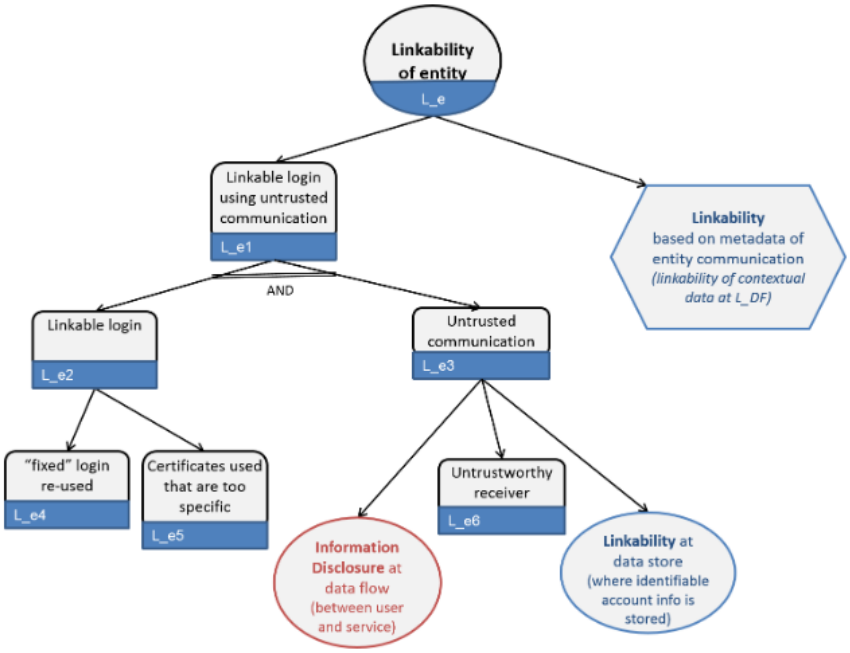


Figure 31: Linkability threat tree

Each leaf corresponds to a threat and if it is applicable to the element we are analysing then the identified threat is documented. For all the remaining leaves, LINDDUN requires to document them as assumption and if a change is done to the assumption, it is easy to check if a new threat is created or not. All the used attack tree can be found on the LINDDUN tree catalogues: https://linddun.org/catalog.php

The produced outputs

- A data flow diagram
- A table that maps for all the items in the data flow, the threat category that could apply
- A list of threats for each mapping done in step 2
- A list of assumptions

Solution space

The objectives

This phase intends to create from the detected threat in the first phase, some mitigation plan to control those threats. The methodology is less specific on who is supposed to deal with those threats. Like the phase before it is composed of three steps.

The contributors

- The management
- The project team
- The security expert
- The data protection expert

The step and how to proceed

1. To prioritize the threats
   This step is less developed in the methodology. The goal here is to do an evaluation and a prioritisation but no real method is provided. There is definitely a need for a risk assessment study that will probably include at some point the management that will decide what risk to mitigate.
2. Elicitation of mitigation strategies
   During this phase the selected threats will be mitigated. For that, we need of course a security expert to put in place the control but also data protection expert. For example, we could see that a threat where by unawareness an employee has downloaded personal data on his computer to print it. This could be a violation of the privacy policy put in place by the company so a solution could be training sessions to raise the awareness of the company on data privacy and protection points.
   Let us not forget that if no experts are available LINDDUN provides mitigation suggestion to elicit the threats like we can see on figure 32.

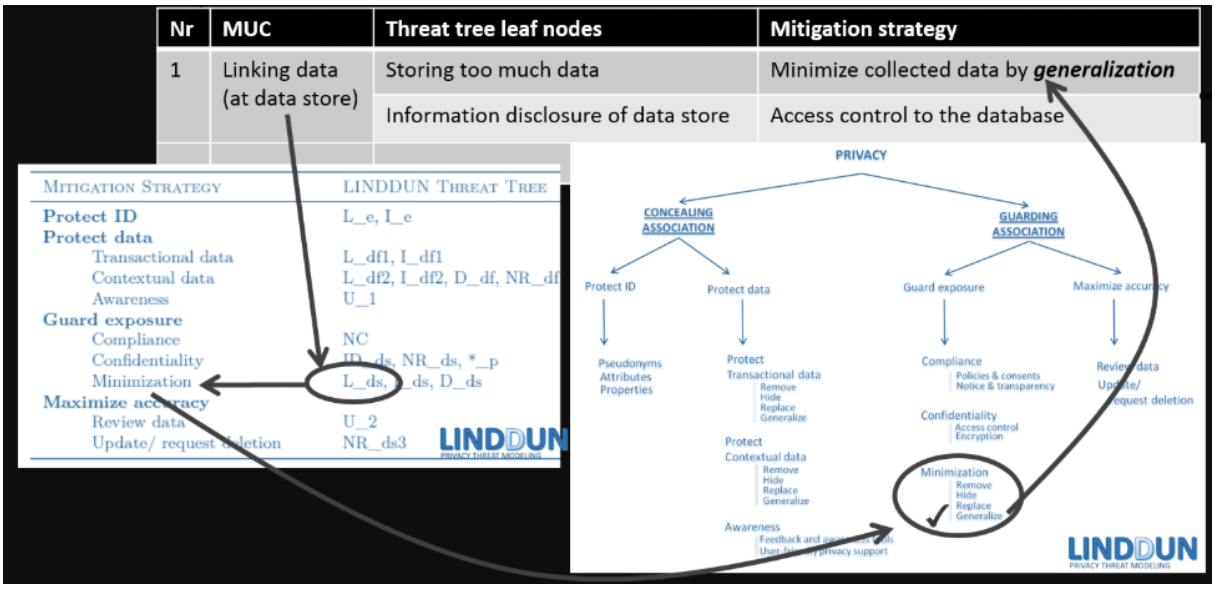


Figure 32: LINDDUN threat suggestion

3. To select corresponding privacy enhancing technology
   Most of the time there are multiple possibilities to mitigate a threat, depending on the context one or another will be selected. To help with that choice, LINDDUN provides a table with suggested solutions for the data privacy threat.

The produced output

- Document with a threat prioritisation.
- A list of mitigation strategies.

- A list of selected mitigation strategies

Synthesis

This is a very interesting methodology especially today with all the fuss we have around the GDPR. It clearly needs to be compiled with others to provide a full risk assessment, but it also fills a hole in all the risk management and threat methodology that we analysed until here. But as we will see in the implementation later, implementing this methodology is not enough to guarantee that the application is compliant.

	The contributors	The outputs	The target
Problem Space	-The project team -The analyst -The architect -The project manager -Eventually a data protection expert	-A dataflow diagram -A table that maps for all the item in the data flow the threat category that could apply -A list of threat for each mapping done in step 2 -A list of assumption	-The project team - The management
Solution Space	-The management -The project team -Security expert -Data protection expert	-Document with a threat prioritisation. -List of mitigation strategies. -List of selected mitigation strategies	-The management -The project team -Security expert -Data protection expert

Criteria

Time to implement: Normal

- The methodology is simple but complete
- For example, in step 3, many threats trees have to be analysed. It takes time.
- A separate risk assessment needs to be conducted

Level of skill: Normal

- We have to be honest, having an awareness of the data protection regulation is more than helpful for this methodology. Nevertheless, no need to be an expert in data protection law and that is the advantage of this methodology.

Readability: Comprehensible

- The produced document is a clear and prioritised list of threats with their mitigation plans.

Scope: Low

- This methodology focusses only on the data privacy threats.

Discussion

After analysing those methodologies, we can already draw some points of attention that we could use for the comparison between risk management and assessment and the threat modelling approaches.

- It is easier to understand.
- It allows to include developers in the process.
- Less organisation-focus, we rarely see mention of organisation or management terms when we look at the goals.
- It is more technical.
- It is faster to implement.
- For most of them, they can start only when the architecture or the model is finished.

It is clear that it is the need of cheaper, faster and more effective security assessment that have brought these tools to life. Another great advantage of these tools is that we can combine them to do what we want! For example, we could imagine using the STRIDE methodology for all the security risk and bring LINDDUN from the beginning of the project to help consider the privacy regulations requirements.

Chapter 5: Experimentation

In this chapter, we will implement one risk assessment methodology and one threat modelling. The goal is not to do a full risk assessment that would take too much time, but we will focus on the data privacy threats. The two selected methodologies are EBIOS and LINDDUN.

Project context

For the European elections 2019, the web communication unit is willing to use a tool that will allow to target data subjects and deliver them with personalised information. Therefore, they also need a website easily customisable to allow users to subscribe and to take steps into their engagement (pledge to vote, recruit friends, organize events…). With the new European regulation on data privacy, the management received strong requirements about the respect of the data privacy regulation for all the webservices. This risk assessment will especially focus on the risks that concern the data protection regulation and the respect of this one. The project itself will be subcontracted to a contractor but for the purpose of this study case we will extrapolate the architecture of the solution to identify the major risks. We will consider the material or the technology from which the management requires guarantees as assets to identify the risks and demand a solution or guarantee from the subcontractor.

EBIOS experimentation

Like we defined in the analysis, the EBIOS methodology is composed of 5 modules, we will not blindly follow all the steps of the module since the goal here is not to do a full risk assessment but for each of them, we will:

- explain what we did and how
- Explain the results
- Give a feedback on the impression during the implementation, if it was easy to implement (easy, medium, hard)

The 5 modules of the EBIOS methodology are:

- Context and scope
- Sources
- Strategic scenario
- Operational scenario
- Mitigation plan

I will divide the analysis of the implementation into two parts:

1. The setup phase

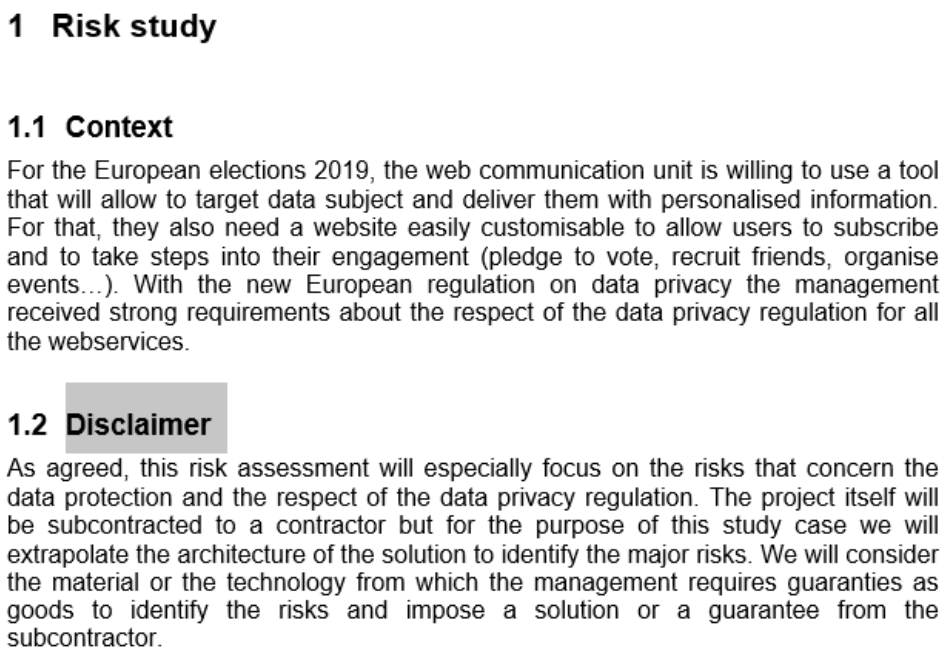
   This phase corresponds to the gathering of information about the context, and the composition of the stakeholders, it is the output of this phase that will allow the identification of the scenario and the risks.

2. The risk identification phase

This is the most critical phase, based on the phase 1, we will identify the dreaded events and the risks that could trigger them.

The setup phase

First step and I am already facing an issue, the syndrome of the white page… Even after having spent days studying and analysing this methodology, I had no clues how to start.
So, my first reflex was to go and find existing implementation example or a template. With EBIOS it was not difficult to find, you have both examples and empty templates. This was quite comforting because when you have template it means you just have to fill them in and follow the steps. Well this feeling did not stay for long. I quickly realised that all the examples that I founded, and the templates were from the previous version of EBIOS so the structure was not exactly the same. Finally, I decided to use my own structure but still keeping the objective of the methodology.
For the first part I ended up with the following structure:



1 Risk study

1.1 Context

For the European elections 2019, the web communication unit is willing to use a tool that will allow to target data subject and deliver them with personalised information. For that, they also need a website easily customisable to allow users to subscribe and to take steps into their engagement (pledge to vote, recruit friends, organise events…). With the new European regulation on data privacy the management received strong requirements about the respect of the data privacy regulation for all the webservices.

1.2 Disclaimer

As agreed, this risk assessment will especially focus on the risks that concern the data protection and the respect of the data privacy regulation. The project itself will be subcontracted to a contractor but for the purpose of this study case we will extrapolate the architecture of the solution to identify the major risks. We will consider the material or the technology from which the management requires guaranties as goods to identify the risks and impose a solution or a guarantee from the subcontractor.

Figure 33: context and scope

In the figure 33, I gave a context to the project but also to the study by precising that the study will focus more on the data privacy risks. After that I naturally realised that an overview of the system was needed. And for that I decided to create a modelling of the architecture. I want to insist on the fact that when I realise that study, I had no knowledge of the modelling or threat modelling techniques! The result, pretty basic, can be seen in figure 34.

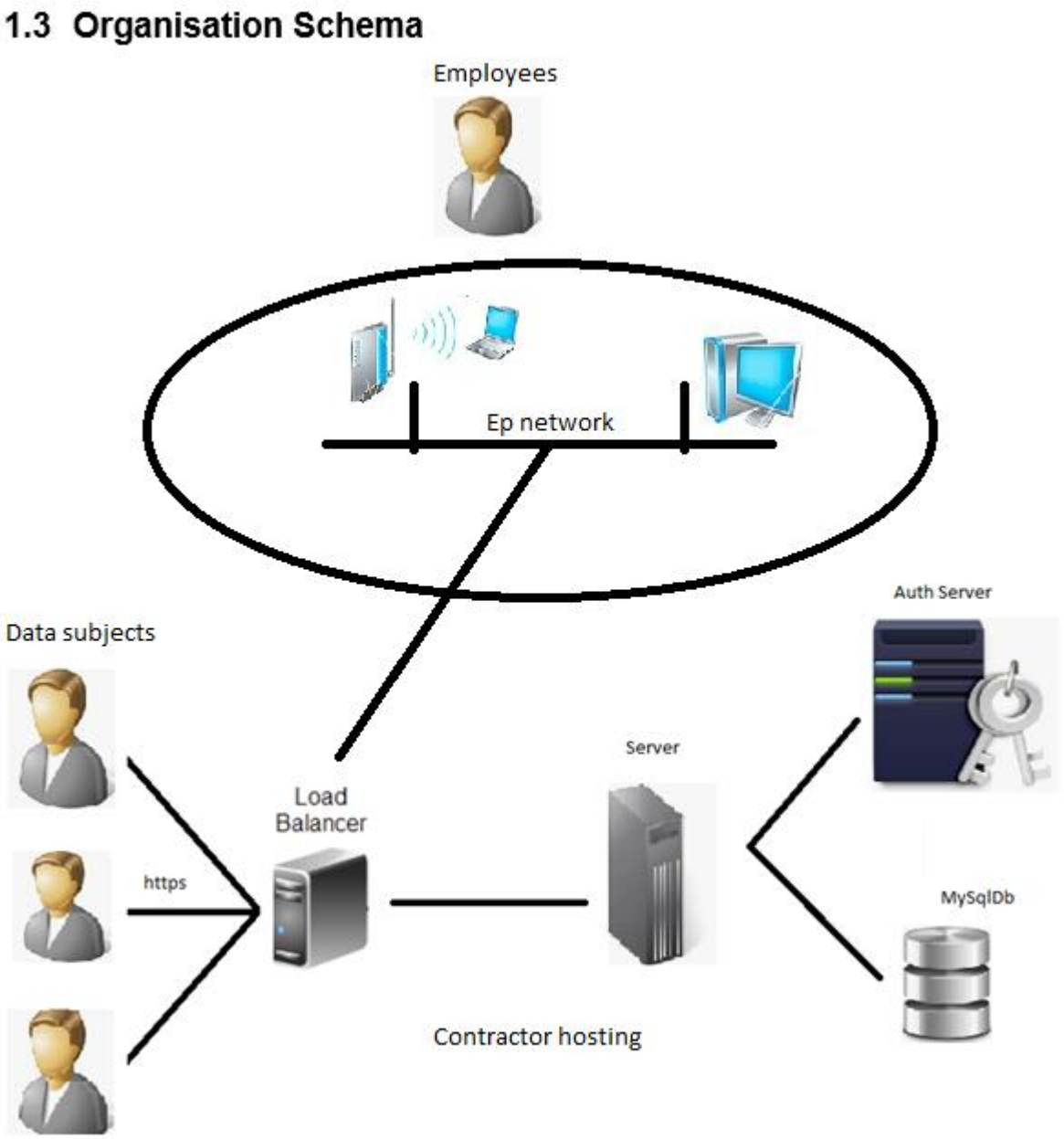


Figure 34: system information schema

This modelling view was also in one of the examples that I found. Of course, the schema was much more detailed but in my context, I had less information about the system and the scope was reduced.

Once the context was defined, I passed to the next points of the methodology which was:

- **The definition of the scope**
  For that I simply explained what subject of the study and the expected goal. In figure 35 we have the description of those two points.

2 The risk management framework

2.1 Study subject

This study will focus on the process on the data by the unit that could lead to a data breach.
There are 2 main interfaces:

- The website: where data subjects come and sign up.
- The user management page: where editors can manage data subjects and send them relevant content

The second point that is very important for the management is the availability of the application. Many campaigns on social media will be scheduled. These campaigns have a big budget so it is crucial that when data subjects are brought to the platform, they are able to sign in right away.

2.2 Goals

To identify the weak spots of security in the SI and in the unit especially for the data protection.
To raise the awareness within the management on the measures to take.
To prove wether the project respects or not the new data privacy regulation.

Figure 35: study scope and goals

This phase again was not too difficult, because the study is not too complex.

- **The identification of the goods (essential and physical)**
  For this phase, as requested by the methodology, I listed all the essential and physical goods that compose the information system. In order to do that I used the modelization that I did in point 1.3. Having a schema helps to have a good overview and insure not to forget something. During this step 4, processes have been identified and 3 physical goods have been listed.

  1. The essential goods (4 Processes)

     - To recruit and build the community.
     - To interact with them in a tailor-made manner and via various channels of communication including email communication, social media, text messages and other tools, available through our web-based platform.
     - Managing the website.
     - Managing the data subject information: it regroups all the information that we gathered from the data subject.

  2. The physical goods
     - The servers: they host the website, the administration interface and the tool itself.
       - The databases: will contain all the data subject's information.
       - The European Parliament networks.
       - The employee desktop and devices.

Note that the schema was not enough, a brain storming was also necessary, I had to ask questions to the business owner to be sure to have all the processes. So again, this step is based on the knowledge of the information system.

- **The security measure already taken**
  For this step I also used the schema to identify all the points where the security was already in place. Of course, it gives you just a hint at where to look. To know the exact details of the already implemented measure you need to have the knowledge, which means organise workshops, interviews, meetings… In figure 36 you can see the identified existing security measures.

2.4 Security measures already taken.

- The access to the buildings is secured by the DG safe. (Badge check, scans, automatic doors…)
- The access to the Wi-Fi network is secured by a certificate and encryption. To have access one must go with his device to DG Itec and ask to install the certificate on his device. Of course, the identification is performed with the badge and the ID card.
- Each user has a folder on the network which is encrypted.
- To access a computer and a session, a password must be provided by the employee, each employee has his own password with a minimal required complexity and a validity of 60 days.
- The Parliament servers have 2 data centres, in case of fire, explosion, network issue all the connections will be redirected to the second data centre.
- There are counter fire measures in both data centres
- Both data centres are equipped with generators.
- The EP network has 2 internet connections in case one has an issue.

Figure 36: identified security measures

- **The definition of the criteria and their evaluation**
  The last step of 'setup', I call that setup because all we have done until now is gather information in order to identify risks, is the definition of the constrain to consider and that will impact the risk assessment. I our case it will be:
  1. The new data protection regulation
     This regulation entered into force in December 2018 fir the European institution is a serious requirement for the project, this regulation has been largely covered by the media and it is the European parliament that voted it. So, it is crucial that the project can prove the compliance with it.

  2. The different stakeholders
     This project is used by a lot of stakeholders, the fact that they are not in the same office even not in the same country, will increase the difficulty of controls.

  3. The data protection officer
     For each decision that has to do with the data privacy, the DPO will have to be consulted, his advice will have to be considered.

Synthesis

Let us have a look to what was produced until now.

Steps	Output	Difficulty
Context	-Context of the study. -Context of the information system	easy
Risk study	-Scope of the study -The essential and physical goods -The security measure already in place	Medium
-Security analysis	-The list of already taken measures	medium

We already have a good list of documents that will allow us to do the next steps. For me the template that I found were very helpful, even I did not used them completely, some of the table were going to into details for the scope. One thing we note is that all the information field until now is knowledge based. Which means that if I had to do this in a real project, I should have passed a lot of time in meetings to get all this information and probably I would have much more information than what I have found alone.

On the other side the exercise is not that difficult, I have to admit that some of the table that was in the template were more complex to fill, that is why I skipped them but I think this is because the scope of the study is not big enough and I did not really have any relevant information for these steps.

The risk identification phase

Here I continue to try to follow as I can the methodology. The next logical step is:

1. **The identification of the threat source**
   For that I used the tree proposed by the methodology that will help me to identify the sources. It presents itself like a table that we need to fill in, see figure 37 to see the one I did.

Types of threat sources	Retained or not	Examples
Internal human resource, malicious, with weak abilities	Yes	✓ An employee could use an unlocked computer to get access to subject personal data. ✓ An employee with access to the database could cause a data breach by exporting data on a usb key
Internal human resource, malicious, with strong abilities	Yes	
Internal human resource, malicious, with unlimited abilities	No, there is no such profile in the unit.	
External human resource, malicious, with weak abilities	No	
External human resource, malicious, with strong abilities	Yes	✓ There are a lot of external people working for the unit from the cleaning team to developers and even project managers. ✓ The subcontractor. ✓ The subcontractor's employee ✓ Attack on subcontractor infrastructure ✓ Hacker trying to steal data subject password
External human resource, malicious, with unlimited abilities	No	
Internal human resource, without malice, with weak abilities	No, if the profile is not involved in the project there is no way he can cause a breach.	
Internal human resource, without malice, with strong abilities	Yes	✓ An employee could print personal data to work on it and might forget to take it at the printer.
Internal human resource, without malice, with unlimited abilities	No, there is no such profile in the unit.	✓
External human resource, without malice, with weak abilities	No	
External human resource, without malice, with strong abilities	No	
External human resource, without malice, with unlimited abilities	No	
Malware	No	
Natural phenomenon	No	
Natural or sanitary disaster	No	
Animal activity	No	
Internal event	Yes	Fire, electricity cut…

Figure 37: threat source

This part is not difficult, and the table allows to do it fast, of course you need to have the answers… And like we saw during the analysis normally this step is done with different contributors.

2. The metrics definition

This step is very important and should normally involve the management. They are supposed to give the security requirement. For this phase I defined the three security criteria that I wanted to consider:

- Availability
- Integrity
- Data privacy

For each of them I added the scale that will be used to evaluate the risks on these criteria. (Refer to point 2.7 of annex for the details).

3. **Apprehended events**

Here we are going to identify all the dreaded events. I found in the template example a table that helped me to format this phase in an easy and readable way. See figure 37 to see the result.

3.1 Apprehended events

Events	Security needs	result	Sources	Impact
Data breach on the data subject's personal data	Limited	✓ The data can be altered, lost, used…	✓ Weak password ✓ Not serious employee ✓ hacker	Critical
No respect of the data protection law	Respected	✓ Loss of credibility ✓ Fines	✓ Lack of employee's awareness ✓ Subcontractor not serious or not compliant	Maximal
The data subject's personal information are altered	mastered	✓ Contact wrongly a user ✓ Loss of subscription	✓ Database issue ✓ Employee's mistake	critical
The website is unavailable	60 minutes	✓ Not able to recruit people ✓ Loss of credibility	✓ Server issue ✓ Server attack	Strong
The administration interface is unavailable	6 hours	✓ Not able to manage people ✓ Not able to contact people ✓ Not able to treat the S.A.R.	✓ Server issue ✓ Server attack	Medium

Figure 38: dreaded events

Again, I extrapolate the requirement since I am alone to do this risk assessment but normally other contributors should express their concerns and help to assess the impacts.

After that I have to say that the methodology started to be too complicated in his implementation, again I think that the scope of the study data privacy is the cause of that difficulty to follow all the steps of the methodology. What I did is follow the principle, but I did not use the table that was provided in the template.

For each dreaded event I have identify possible scenario. In figure 39 you can see an example of analysis for one dread event with:

- The probability
- The impact
- The security requirements
- The possible scenarios

This will allow us to evaluate all these dreaded events to help the management to make decision on what should be mitigated.

3.3 No respect of the data protection law

Adding data into the system without the proper consent

- Probability: Strong
- Impact: Maximal
- Security requirement: Respected
- Apprehended events: No respect of the data protection law
- Scenario
  1) An admin decides to import data into the system from another database
  2) An Eplo collects data himself during an event without getting the consent.
  3) The website collects data without consent.
  4) Cross data with other third-party (Facebook, Twitter).

Figure 39: example of scenario and evaluation for a dreaded event

After the realisation of this step I decided to create a matrix that gives a quick idea of the risks and their impacts. You can see this in figure 40. This representation is much appreciated because it avoids the reading of all the scenarios and only focus on those they need to take into consideration.

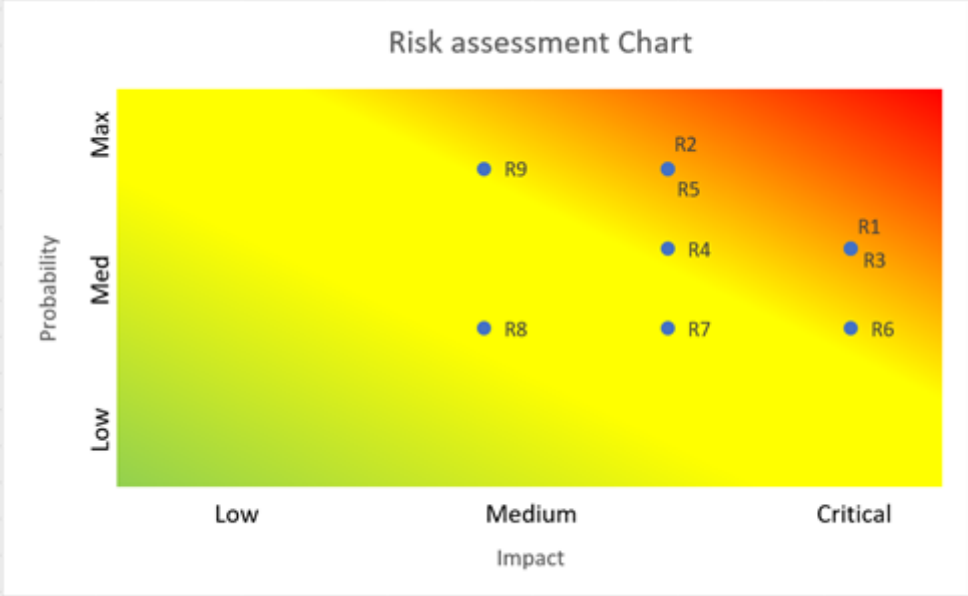


Figure 40: RA chart

4. Action plan

After that, a mitigation plan has been proposed for all the dreaded event. I chose as example (figure 41) the fact that the contractor does not respect the regulation. To be able to put in place this mitigation plan I had to consult with legal service, data protection coordinator, data protection office. And each time I asked question the intermediary had to check for the answer. This is because the regulation is quite new, and nobody had experience with it. This mitigation plan was quite time consuming.

The subcontractor does not comply with the data protection regulation

To mitigate this risk a series of clause will be added to the contract.

- The data processor shall be compliant with the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. In this regard, the data processor shall carry out a Data Protection Impact Assessment in accordance with Article 35 of the General Data Protection Regulation and provide the data controller with the results thereof as a deliverable of the contract.
- As of a date specified by the data processor to the data controller, the personal data collected and processed for the purpose of the contract shall be stored solely in the EU by any means and shall not be transferred outside the EU. Moreover, all data operations necessary for the purpose of the contract shall be processed within the EU (This is a request done by the data protection officer).
- No data operation shall take place without prior written approval of the data controller, including transfers of personal data.
- Interactions with data subject shall only take place via the data controller.
- The data controller shall be entitled to request the data processor to implement any additional technical or organisational measure necessary to comply with the General Data Protection Regulation.
- When the contractor subcontracts its obligations under this contract, it shall do only by way of sub-contracting agreement which impose the same obligations on the sub-contractor as are imposed on the contractor under this contract.

Figure 41: mitigation plan regulation compliance

This was the last phase of my implementation tool

Synthesis

Let us have a look to what has been produced in this phase.

	Output	Difficulty
The identification of the threat source	-List of the source threat(table)	-easy
The metrics definition	-List of criteria -List of scale for the criteria	-easy
Apprehended event	-list of dreaded events -List of scenarios for each event -Evaluation for each dread event -Risk matrix overview	-Medium
Action plan	-list of proposed action plan for each dreaded event	-hard

As you can see most of these steps are easy to perform, the knowledge is very difficult to have and unfortunately except for the last part I was not able to have all the necessary contributors for the assessment. But the last part shows me that the meetings request, to ask information are

very time consuming. This methodology is clearly not applicable alone since she does not provide a lot of tool to help you. Like we said during the analysis threat modelling could be used to help the detection of stakeholders, entity, threat…

Another thing also is that the methodology is clearly not adapted to the data privacy risks. The fact that we list the assets and the stakeholders at the beginning help a little, but it is clearly not enough. People with knowledge need to assess the system to detect all the treat, and there is no existing controls that we certify that all the threat have been identified.

Since it requires a lot of contributors to be relevant and a lot of knowledge/expert to be efficient it confirm the observation done in the analysis part that the methodology is time consuming and not fit for small companies since it required a lot of resources.

We have also confirmed the targeted audience of the result of this methodology. It is clearly the management that will use this document to decide what risk to mitigate. (The risk matrix helps a lot).

Note that naturally a basic modelization of the system has been done at the beginning. Like I said when I did this implementation, I didn't even know what threat modelling was. It proves that naturally a modelling of the system helps to have a good overview and to identify different elements. Cleary in this case a data flow diagram would have been useful.

At some point I was also confused, I am not sure why but I can see to possible reason:

1. I do not have enough experience
   The methodology is composed of 5 modules and a lot of steps, the link between the steps and the result produced is not always easy to understand. Also I found the vocabulary heavy, I am a French speaker and I had to read sometimes four or five time the sentence to finally understand it. With time it became too heavy and that's why I decide to tailor a little bit the template that I founded.
2. The methodology was not fit for data privacy
   This is another possibility, all the tables that I saw in the example makes sense when I read them, but for my case I was sometimes incapable to fill them.

Criteria

For the evaluation I will keep the same value that I had for the methodology analysis.

Time to implement: Long

Justifications

- Specially for all the contributor to involve and the knowledge to gather

Level of skill: Advanced

Justifications

- The methodology is long, the document produced is long
- The link between steps in not easy to understand

Readability: comprehensible

Justifications

- I keep this notation, but the condition is that the result is presented to the manager, with visuals like modelling or risk assessment matrix.

Scope: Detailed

Justifications

- Like for the analysis if the knowledge and the resources are not a problem, the granularity of the result can be very high.

LINDDUN methodology experimentation

For the threat modelling approach, I chose LINDDUN for several reasons:

1. It is a methodology specially designed to detect the data privacy threat, in our case study it is perfect since we decided to focus on those threats.
2. The methodology has been developed in Belgium at the KUL University and has been cited by ADAM Shostack by one of the most serious methodology for the data privacy threats.
3. Contrary to EBIOS, this methodology provides a lot of tools to help in the detection of the threats.

I will try as much as possible not being influence by the knowledge I have on the data protection regulation.

Like we saw in the analysis this methodology is composed in 2 phases of 3 steps each.

Problem Phase

1. Define DFD

Like we saw in the analysis this is the most important point in the methodology, it from this step that all the other will depends, if an entity of the DFD is missing it is a complete group of threat that risk being ignore. In figure 42 you can see the DFD produced for the information system. Personally I found this schema much more interesting that the one I created during the EBIOS implementation, this is partly due to the fact that this one respect a defined notations.

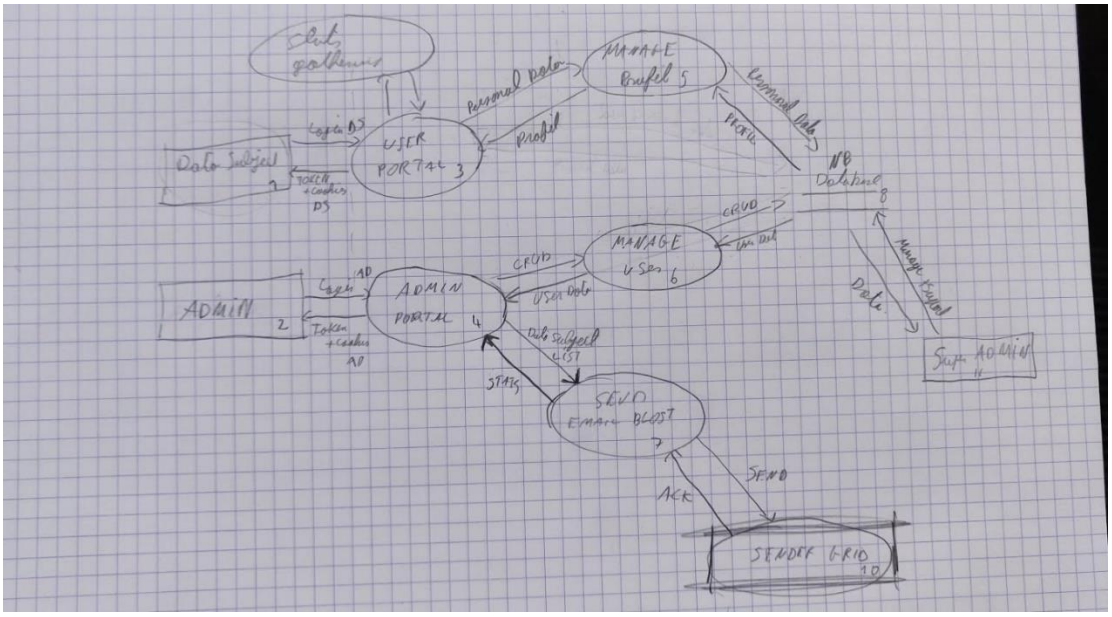


Figure 42: data flow diagram

The definition of the DFD is not a difficult step, you just need to have the architect with you and if he is not available a simple architecture diagram can be sufficient.

2. **Map privacy threats to DFD elements**

Like we saw in the analysis this step is very mechanical. For each element of the data flow diagram, I checked if one of the LINDDUN categories can apply. I used the tips that I defined in the analysis just go through the menu on their website and each time a category could applied I just putted X in the table. You can see in figure 43 the result of this step.

	L	I	N	D	D	U	N
ENTITY							
Data subject	X	X				X	
Admin	X	X				X	
Super admin	X	X				X	
Sender Grid	X	X					X
Stats gathering	X	X				X	X
PROCESS							
User portal	X	X	X	X	X		X
Admin portal	X	X	X	X	X		X
Manage profile	X	X	X	X	X		X
Manage user	X	X	X	X	X		X
Send email blast	X	X	X	X	X		X
Manage profile	X	X	X	X	X		X
DATA STORE							
NB database	X	X	X	X	X		X
DATA FLOW							
Login DS (1-3)	X	X	X	X	X	X	X
Token + cookies ds(1-3)	X	X	X	X	X	X	X
Login AD(2-4)	X	X	X	X	X	X	X
Token + cookies ad(2-4)	X	X	X	X	X	X	X
Personal data(3-5)	X	X	X	X	X	X	X
Profil(3-5)	X	X	X	X	X		X
Crud (4-6)	X	X	X	X	X		X
User data (4-6)	X	X	X	X	X		X
Datasubject list(4-7)	X	X	X	X	X		X
Stats(4-7)	X	X	X	X	X		X
Personal data(5-8)	X	X	X	X	X		X
Profil(5-8)	X	X	X	X	X		X
Crud(6-8)	X	X	X	X	X		X
User data(6-8)	X	X	X	X	X		X
Send(7-10)	X	X	X	X	X		X
Ack(7-10)	X	X	X	X	X		X
Manage and support(8-11)	X	X	X	X	X		X
Data(8-11)	X	X	X	X	X		X

Figure 43: LINDDUN mapping table

I want to insist here on the fact that I did that purely by following the methodology, I did not use my knowledge.

3. To identify threat scenario

Here I did two steps:

First, I listed all the assumptions as requested by the methodology, for that I had to do a brainstorming. And I have to admit I had no way to ensure that I did not forget anything. So, for this step it is strongly recommended to do it with other contributors.

The result is a list of assumption like:

1. The processes that are done in the backend are considered protected since the backend has passed the pen-test done by DG-ITEC. The only threat that could come from inside it means people are having access to the application.
2. For the same raison as point 1, the communications between the processes are also considered safe.
3. The communication between the entity and the system are not considered as safe since the entity can produce data breach if they do not respect the guidelines and also the communication channel is not considered as secure.
4. Then I listed all the threat scenarios, for that again no knowledge is required, I just followed the threat trees that are provided by the methodology, see the analysis for more information. I used the following structure for each threat

    - **Identifier of the threat**
    - **Summary**
      To quickly give a context to the scenario
    - **Primary actors**
      The source of the threat
    - **Basic path**
      List of all the path used by the actor to implement the treat
    - **Consequences**
      List of all the impacts if the threat is implemented
    - Reference to the treat tree node(s)
      This is the unique identifier of the threat in the tree attack.

You can see in figure 44 one of the identified scenario.

T01

Spoofing of the entity user or admin

Summary

The attacker obtains the credentials of a user worst an admin and can then access to the data

Primary mis-actor

- An outsider attacker with a lot of competences.
- An internal attacker with low competences

Basic path

- The attacker gain access to a computer with an already logged account
- The attacker intercepts the communication.
- The attacker stole the session cookies

Consequence:

The attacker gains access to the system

Reference to threat tree node(s)

I_E_12, I_E_13,I_E_20

Figure 44: scenario definition

Let us have a recap on this first phase.

	output	Difficulty
Define a DFD	-Data flow diagram	Easy
Mapping privacy threat	-List LINDDUN mapping	Easy
Threat scenario identification	-List of scenarios -list of assumptions	Easy

For the moment, the comparison with the EBIOS implementation is just huge. It was much simpler at the start, I just had to flow the algorithms defined by the methodology. I must admit when I did this study I had much more experience with risk assessment and threat modelling but still the simplicity of this methodology is, for the moment, bluffing.

Let us continue with the second phase.

Solution space

Like for the first phase, this one is also composed of 3 steps

1. **Prioritize threats**
   Here a risk assessment was supposed to be done, unfortunately LINDDUN does not provide any instruction for this part… This is not blocking for us since we don't have the decision responsibility but still it sad that LINDDUN has a hole here. On the other side we could complete this methodology by using a risk assessment methodology from another framework.

2. **Elicit mitigation strategies & Select corresponding privacy enhancing technologies**
   For the two remaining point I have to say that I have been a little bit confuse by the tool they provided. I tried to look for examples, but unfortunately in the three examples they provided none of them describe in detail this step. So, what I did is simple go through the threats and proposed mitigation plan for each of them. I know I have tailored a little bit the methodology here, but it seems to be the right thing to do. In figure 45 you can see the proposed measures for one of the identified threats.

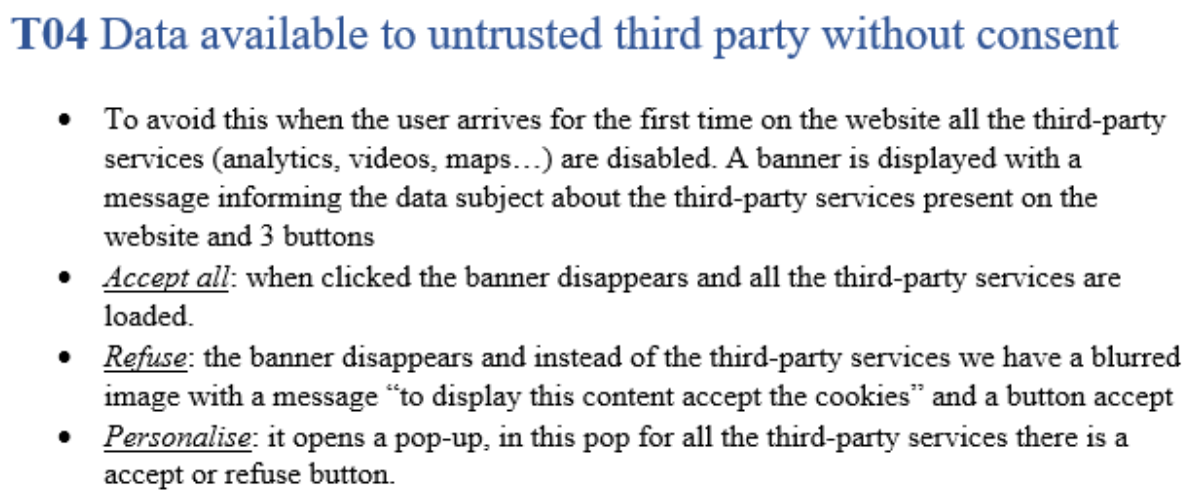


Figure 45: threats mitigation plan

	output	difficulty
Prioritize threats	-risk assessment	-medium
Elicit strategies	-List of mitigation plan	-easy
Select corresponding privacy enhancing	-list of practice to put in place	-easy

Synthesis

This methodology is definitely clearer and easier to implement than EBIOS, the documentation is very easy to understand except for the point five and six that need more concrete example maybe.

The tool that the methodology provides are simple to use, it is just an algorithm to follow for the step 2 and 3.

It is imperative though that the data flow diagram is perfectly executed and completed, if not since the threat detection is automatic, threats might be ignored.

I still see some threats undetected or mitigation plan that should be proposed and that are not. Like the contractual clauses for the sub-contractors for example.

Criteria

Time to implement: Normal

- I'll keep the same notation, the first steps are not complex but if the DFD is big, there is a lot of check and mapping to do when we execute the algorithm.

Level of skill: Normal

- I am convinced that a minimum of data protection knowledge is required to perform this methodology

Readability: Comprehensible

- The produced document is a clear and prioritised list of threats with their mitigation plans.

Scope: Low

- It will detect only the data privacy threat; it could be complete by the utsage of STRIDE. For the security threats.

Discussion

EBIOS

For the first experimentation, EBIOS was selected to do a risk assessment. This methodology was chosen because French documentation was available. It seems to be the easiest choice for a novice French speaker to understand and implement his first risk assessment. But in the end, the methodology and the documentation revealed to be very complex and not easy to implement. In addition, many steps where completely useless to implement for our use case so not all the steps were implemented. An interesting thing is the way the methodology brings us to detect the threats. We have to think a lot about the scenario and a good knowledge of the application is required. Same for the data privacy risks. An experience in this field is absolutely required to be able to identify the risks, the methodology does not help on that. Workshop of several people with all the necessary knowledge is strongly recommended to implement this methodology. We can say after this implementation that the methodology allows to detect the data privacy risk but specialists are absolutely required in the workshop since the methodology does not provide any help to detect those risks.

LINDDUN

On the other side we have LINDDUN, a threat modelling methodology exclusively developed to help the non-expert to deal with data privacy threats. This tool seems to be the best choice since we decided to focus on the data privacy risks. This methodology is very well documented and a little bit tricky to implement at the beginning because of the number of criteria's to check and what they actually mean (LINDDUN) but after a while we get used to it and it becomes straight forward. It was much faster to start implementing it. It required that the DFD is correct. Maybe an architecture diagram could be used and facilitate this modelling. If the DFD is not correctly implemented, there is a risk to miss some threats. The catalogue tree also is very helpful, we just have to follow the attack tree for each entity. I have to admit it was not easy to do the exercise I tried not to use my knowledge of the data privacy regulation when I was implementing this methodology just following the steps and I have to admit that a lot of treats

are detected but not all of them, some area are not covered by the methodology. For example, I was not able to detect that the rights of the data subject were respected. The non-compliance (LINDDUN) should be more developed to take into consideration these points.

Nevertheless, these two examples clearly confirmed what was discovered during the analysis of the methodologies. The threat modelling seems definitely easier to implement and is more convenient and adapted for environment with less expertise by giving practical tools. On the contrary the risk methodology relies more on the expertise of the one who are implementing it. But in any case, the two methods could be used together to enhance and ensures that the scope is covered.

Chapter 6: Comparison

In this chapter we will use the results of the methodologies, framework and tools we analysed to compare them and see in which context those tools should be used. A proposition of possible mix of technologies will also be done to facilitate or to have a better result with certain methodologies.

Criteria and differences

First let us do a recap of our criteria results for all the methodologies.

	Time for implementation	Necessary skills(complexity)	Result readability	Scope
EBIOS	Long	Advanced	Comprehensible	Detailed
FAIR	Long	Advanced	Comprehensible	Detailed
OCTAVE	Normal	Normal	Comprehensible	Detailed
FRAP	Normal	Normal	Comprehensible	Low
STRIDE	Fast	None	Easy	Low
Elevation of privilege	Fast	None	Easy	Low
T-MAP	Normal	Advanced	Complex	Detailed
DFD	Fast	None	Easy	Low
LINDDUN	Normal	Normal	Comprehensible	Low

Table 1: Methodologies Criteria

- The first thing we can clearly notice is that the risk management and risk assessment methodologies are in general heavier to put in place and require more resources and competencies than the threat modelling tools.
- We can see that the scope covered by the risk management methodologies is wider and is able to take more elements into consideration.
- The target result of these tools is also completely different. One is entirely dedicated for the management, to help them make decisions by providing them qualitative or quantitative description of the risks and relation between the impact and the cost of mitigation. The other, threat modelling, is more intended for technical people to help them implement security measures and to communicate the threat.

- The possibility of tailoring is also something that is obvious. When the risk management framework allows and even requires the tailoring of some steps, the threat modelling most of the time imposes classification in predefined list, STRIDE is a good example.
- The threat modelling, especially if we take a software-centric approach, allows to involve the developers. This has the big advantage to raise the awareness of the developers and will help them to make the correct implementation decisions.
- Something that we have in the risk management and not in the threat modelling is the managing of the opportunities. This could be considered in the threat modelling, but it would require tailoring.

Time of implementation

When we analyse the table about the methodologies criteria, we can observe that the risk management approach is in general more complicated than the threat modelling. There are several arguments that explain why. Let us see what the disadvantages of the risk management approach are that explain the evaluation for the time implementation criteria.

Risk management disadvantages

- It requires involvement and support of the hierarchy
  Since the scope of this approach is wider it needs the contribution of a lot of management profiles.
- The methodology is more complex
  For the analysed methodologies, the documentation is quite extensive, and the implementation is then long.
- The number of documents to produce is high
  Most of the time the methodologies are composed of several phases, and each phase needs to produce one or more documents.
- The lack of tools or template
  This has been particularly felt during the experimentation. It was difficult to begin in the absence of a template.
- The workshop needs
  Since the risk management is based on the knowledge of the participant to identify the risks, many meetings are required in order to cover all the risks.

On the opposite, we have several advantages that explain why the threat modelling approach is faster.

Threat modelling advantages

- It can be initialised by the project manager with only the help of the development team.
- For the analysed methodologies, they are easy to understand and not heavy (except T-map)
- Those methodologies provide a lot of tools/ templates to help in the implementation.

The necessary skills

Here again we can see a difference between the risk management and the threat modelling methodology. The fact that the risk management methodology requires more skills is explained

partially by the same arguments as for the implementation time criteria. The most important one is the fact that the threat modelling proposes tools like attack tree or classification based on data flow diagram item that allow non expert profiles to detect threat.

Result readability

Here is one of the big advantages of the threat modelling. When you have something visual it is always easier to understand and to explain or justify. With the risk management we saw in the analysis that a lot of documents were produced which makes the information difficult to find sometimes. Also, for some risk management methodologies, it was advised to have a certification to ensure a proper implementation.

Scope

Here come the disadvantages of the threat modelling methodology. Since it provides tools to detect the threats, it is possible that by strictly following these tools, some threats might be missed. This can be caused by the lack of knowledge. Another disadvantage is that the threat modelling methodology focuses on one information system and dismisses by default external threats.

When to use which methodology

With all these points it is obvious that the risk management and the threat modelling methodologies must be used in different contexts. We will list different contexts and for each framework give an appreciation whether it is advised to use it or not. Note that it is an appreciation based only on the theoretical analysis that has been done in this thesis and confirmed by the implementation done on the use case defined in the chapter 6. For this table we do not consider specialised companies that could have special needs in security risk management, even if they are small. We also consider that each methodology will be used exclusively by the organisation.

	Small company(<50p)	Big company	Short time(budget)	Experience required	For management	For developers
EBIOS	No	Yes	No	Yes	Yes	No
FAIR	No	Yes	No	Yes	Yes	No
OCTAVE	No	Yes	No	Yes	Yes	No
FRAP	No	Yes	No	Yes	Yes	Yes
STRIDE	Yes	No	Yes	No	Yes	Yes
Elevation of privilege	Yes	No	Yes	No	No	Yes
T-MAP	Yes	No	No	Yes	No	Yes
DFD	Yes	No	Yes	No	No	Yes
LINDDUN	Yes	Yes	Yes	No	No	Yes

Table 2: Context use

If we analyse this table, we can see that the threat modelling is clearly easier to put in place for the small companies. This is due to the low implementation cost and the group to which the results are targeted to. What is important for a small company is that the product that it created presents as less vulnerabilities as possible, the context is less important. On the opposite, for a big company, external threats must be taken into consideration. This requires a more analytical approach and requires a larger scope which means more time and more experience required as well.

Size of the company

Let us compare first the risk management and the threat modelling in the context of the size of the company first. The table is quite clear here. The risk management is clearly the preference for the big companies and is not suitable for small companies. This is due to several factors:

1. The scope
    - *Risk management methodology*
      Like we saw in the analysis, the risk management methodology provides the possibility to take into consideration all the aspects of the organisation. Risks like reputational damages would be easily considered since their impact could be catastrophic for the organisation. We can say that the bigger the company is, the longer the list of risks is. The scope from where these risks could come from

is also more extended. And of course, the impact and the consequences if a risk should occur is also bigger.

- *Threat modelling*
  On the other hand, let us take the example of a small company that is doing development of IT solutions. The scope where the risk could come is much more reduced. The most important for these kinds of company is to deliver a product that respects the defined specifications in the allowed budget. And of course, this solution must be robust. So, in this case, the scope of the analysis will be much more focused on the application itself.

2. The strategic decision of the mitigation plan
   - *Risk management methodology*
     Like we said just before the impact of the risks in a big company can be catastrophic on a human or financial point of view. So, in order to decide on a mitigation plan, the study must consider the point of view of all the experts in the company. As we saw in the analysis, the risk management methodologies are taking more high-level contributors and that will allow the decision people to have all the necessary input.
   - *Threat modelling*
     On the other hand, in the smaller companies, like we saw in the previous example, the important thing is to deliver a quality product. Most of the time, the responsibility of this is on the project manager's shoulders. The threat modelling approach will provide him with the tools to implement on the scope of his project.

The budget

In the small or big companies, the profitability is also crucial. Since the smaller company have by definition smaller projects, their budget is also reduced, so it is important for them to use an approach that will allow them to:

- Focus the study on what is really necessary.
- Have the tools that allow to detect the risks even if there is no expert available.
- Increase the efficiency of the development process.

When we look at the column budget of the table context use, we can see a clear distinction between risk management (higher cost) and threat modelling methodology approach. The threat modelling approach is a much lighter and focused in a way that can easily be used by the project manager with the help of his own team to control the threats. The project manager will have all the information to take action to control the risks, and the fact that he used his own team to identify the threats will also raise the awareness of his team and improve the development phase. Let us not forget the time. There is no need in the threat modelling approach to do multiple workshop with experts or people external to the project. The implementation is therefore much faster.

The required experience

Here again there is a clear distinction between the risk management and the threat modelling approach. This is partially explained by the provided tools.

- *The risk management methodology*
  This approach is mostly based on the knowledge, which means that the risks identification will be done by the experts. Some methodologies like FRAP will provide guidelines to organise those meetings, such as the agenda, the required output or the contributors that should attend.
- *Threat modelling*
  With these approaches we will have tools at our disposition that will allow the detection of the threats, even if we do not have experts in the team. I take the LINDDUN methodology as example that will provide the possibility to easily identify the dreaded scenarios and detect the threats for each of them without having knowledge of the data privacy regulation.

We have an exception here with T-MAP framework that ask the developer to have an attacker point of view. This is not easy for a developer. If I quote the words of Adam Shostack "It is like asking to a developer to think like a professional chef". That is why a certain level of knowledge is required for this approach.

The targeted audience

This is something that is clearly defined in the analysis part. When you do a study and you are using a risk management methodology the ultimate goal of the risk assessment part is to provide sufficient information to the management to be able to make decision. If you compare the different contributors in the analysis part for the risk management and for the threat modelling approach, we saw that the risk management tends to involve more high-level profiles like architects, CSO…etc. And the outputs of the different phases are also more targeted for management profiles. This is also something to take into consideration when we choose the approach.

For a project manager, it will be much more interesting to use a threat modelling approach that will make participate his project team and improve the knowledge and the efficiency of his team.

Complementarity

We defined at the beginning of this thesis the differences between risk management, risk assessment and threat modelling. What we can see is that risk management methodologies could be tailored to use or to be completed by threat modelling tools. Let us take the example of an organisation which decides to use OCTAVE to deal with the risk management. We saw the goals of OCTAVE are:

- To create a list of the essential goods of the company
- To list all the vulnerabilities and threats to these goods and the cost if a threat occurs
- To summarize the enhancements of the process to mitigate the risks (risk plan)

All with the purpose of helping the management to make decision.

If we implement it like that, clearly the knowledge will stay at the management level and will not necessarily be shared or consulted by the more technical people. Also, there is a risk to miss threats since the people involved in the risk assessment are not necessary the ones implementing

the solution. A good practice would be to use Elevation of privilege that gives the opportunity to involve developers and is easy to put in place.

What is true for threat modelling is also true for other risks assessment methodologies. For example, we could use FAIR in complement to OXTAVE risks assessment methodology. FAIR would bring a more quantitative information thanks to its sheets. That will help to explain and defend the conclusion of the OCTAVE risks assessment to the management.

It is already done!

It is not obvious but when we analyse the EBIOS methodology we can see the methodology is already using threat modelling more specifically attack-tree. It is just that it is presented as a checklist in the threat sources point.

When we come to a choice, the table of criteria could be used of course but we have to keep in mind that every organisation, every project has its own context. Strictly following one methodology or a specification is not necessarily a good thing and worst it could lead to ignore risks. The risk management methodology and the threat modelling due to their different focus and different documents produced can be considered as two complementary methodologies. But it has a cost in time and requires, sometimes, experts. So the complementarity will be easier implemented by the big companies rather than the small companies that should use only threat modelling if the budget is short.

Lack of skills

It is possible that even in a bigger company the lack of skill prevents the detection of certain threats, like the data privacy threats for example. Like we saw in the experimentation the usage of LINDDUN in the risk assessment phase of OCTAVE will complete the analysis and complete the scope of the study without having to pay an extra consultant.

Chapter 7: Conclusion and recommendations

The information systems are becoming more and more critical in our society. Even laws like the new European data protection regulation bring new needs and vulnerability into information systems. In consequence, more and more tools and methodologies appear to help dealing with these vulnerabilities. All those available tools can be really confusing and yet it is crucial to choose the right approach from the beginning. In the thesis, we have first explained the different concepts that exist, risk management, risk assessment, threat modelling. Then we described and analysed nine tools that could be used. After that we implemented the EBIOS methodology and the LINDDUN technique to one use case to have a practical experience. For each of the analysed tools we have suggested the context in which they should be used. We also explained the differences between the risk management and the threat modelling approach and their possible complementarity.

Risk management

Most of the risk management methodologies are consuming in times and they need to be performed from the beginning of the project (by design) and they absolutely need the management support and implication. There is a relation between the complexity of the risk management methodologies and the scope covered by the detected risks. Most of these methodologies can be and should be tailored to take into account the context of the project, the organisation. Tools like threat modelling are perfect to be included into these risk management methodologies.

Threat modelling

The threat modelling approach does not constitute a full risk management framework. It brings another way to detect and assess the threat. They are in general lighter to put in place but sometimes the scope they cover is too narrow by classification they proposed, for example STRIDE imposes 6 classifications. The big advantage however is that they are much easier to implement and if they are mix or incorporate with other risk management or threat modelling techniques, they will increase the level of details. Also, when risk management produces documents, they are produced for the management most of the time, threat modelling can be used and done for and by the developer teams which present certain advantages like raise the awareness. The implementation of the LINDDUN methodology also proved that threat modelling can provide excellent complementarity to classical risk management methodologies. If you take EBIOS for example you don’t have the necessary tools to help you consider the data privacy risks.

We clearly defined that risk management methodologies and threat modelling techniques have all their interest. The most important thing when the choice is made is to take into consideration the context of the project, the real needs, the budget, the time, the expertise available… All these criteria will help to choose the correct methodology. A note of caution though, choosing a methodology does not mean blindly following the documentation, on the contrary the tailoring

is very important like we saw when experimented the EBIOS one. Remove unnecessary steps, use others or add threat modelling techniques to detect risks can prove to be very efficient.

References

1. https://www.infoq.com/articles/standish-chaos-2015
2. “Le management des risques du projet” Cours de gestion de projet Unamur MA60 Mr. petit.
3. An economic modelling approach to information security risk management Rok Bojanc, Borka Jerman-Blaz ˇ ic ˇ _
4. Euromethod Project, Euromethod Version 1, July 1996
5. J. Laurenz Eveleens and Chris Verhoef, The Rise and Fall of the Chaos Report Figures, IEEE Software January/February 2010
6. K. Ishikawa, La gestion de la qualité, Dunod, 1985
7. Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 4th edition, 2008
8. The Standish Group, The Standish Group Report - CHOAS, 1995
9. Experiences Threat Modeling at Microsoft Adam Shostack adam.shostack@microsoft.com Microsoft
10. EFFECTIVENESS OF THREAT MODELLING TOOLS Lorenz Verheyden 2018
11. Toward a threat model for storage systems Myagmar, Lee & Yurcik, 2005
12. Threat_Modeling_Revisited_Improving_Expressiveness Mirembe & Muyeba, 2008
13. Threat Modeling: Designing for Security A. SHOSTACK
14. ThreadModel-AttackTree Vineet Kumar Saini, Qiang Duan, Vamsi Paruchuri 2008
15. A survey of information security risk analysis methods . rmaghan Behnia, Rafhana Abd Rashid, and Junaid Ahsenali Chaudhry.. February 2012.
16. https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks--real-world-experience.html?page=2
17. Anssi https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
18. IT Risk Assessment: Quantitative and Qualitative Approach Artur Rot
19. guide-methode-ebios-risk-manager 2018
20. Risk Management Insight LLC. FAIR (FACTOR ANALYSIS OF INFORMATION RISK) Basic Risk Assessment Guide. Risk Management Insight LLC, 2006.
21. Measuring and Managing Information Risk (A Fair Approach), Jack Freund and Jack Jones, 2015
22. Risk Analysis – What is FAIR? MARCH 22, 2016 BY ILAOKCWEBSITE2
23. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process Richard A. Caralli James F. Stevens Lisa R. Young William R. Wilson
24. https://pecb.com/whitepaper/risk-assessment-with-octave
25. A descriptive study of Microsoft’s threat modeling technique Riccardo Scandariato · Kim Wuyts · Wouter Joosen
26. Dhillon, D.: Developer-driven threat modeling: Lessons learned in the trenches. IEEE Security & Privacy (2011)
27. Elevation of Privilege The easy way to threat model
28. Value Driven Security Threat Modeling Based on Attack Path Analysis Yue Chen, Barry Boehm, Luke Sheppard

29. Solution-aware Data Flow Diagrams for Security Threat Modeling Laurens Sion, Koen Yskout, Dimitri Van Landuyt, Wouter Joosen
30. FACILITATED RISK ANALYSIS PROCESS (FRAP) Thomas R. Peltier
31. https://linddun.org
32. LINDDUN: a privacy threat analysis framework
33. www.fairinstitute.org
34. www.smartdraw.com
35. https://people.eecs.berkeley.edu/~daw/teaching/cs261-f12/hws/Introduction_to_Threat_Modeling.pdf

Annex 1 EBIOS case study

The Risk management Framework

Study subject

This study will focus on the process on the data by the unit that could lead to a data breach.

There are 2 main interfaces:

- The website: where data subjects come and sign up.
- The user management page: where editors can manage data subjects and send them relevant content

The second point that is very important for the management is the availability of the application. Many campaigns on social media will be scheduled. These campaigns have a big budget so it's important that when data subjects are brought to the platform, they are able to sign in right away.

Goals

Identifying the weak point of security in the SI and in the unit especially for the data protection.

Raise the awareness of the management on the measures to take.

Prove that the project respects or not the new data privacy regulation.

The identified goods

The essential goods (4 Process)

- Recruit and build the community.
- Interact with them in a tailor-made manner and via various channels of communications including email communications, social media, text messages and other tools, available through our web-based platform.
- Managing the website.

- Managing the data subject information: This regroup all the information that we gather from the data subject.

The physical goods

- The servers: they host the website, the administration interface and the tool itself.

- The databases: will contain all the data subject's information's.

Parameters to consider

Several constrains to consider has been identified:

The references that will impact the risk assessment are:

New Data privacy regulation.	*The new regulation 2018/1725 will be the references for this risk assessment.*

The restrictions that will impact the security risk assessment are:

The editors	*The people who will use the user management tool are not always aware about the data privacy and the security.*
The Eplo	*The Eplo are offices present in all the EU countries. They will be responsible to manage the users in their country. Their knowledge of security and of the tool is limited or null and it's not easy to organise a training with them.*
The contractors	*A lot of external staff are working within the unit.*
The subcontractor	*The subcontractor that is going to deploy and manage the hosting of the application is based in US. This subcontractor is considered as processor.*

The hypotheses that will impact the security risk assessment are:

The DPO	*The data privacy became an important subject, it has been voted by the European parliament and the regulation 2018/1725 entered into force 11december 2018. As this tool will be use for the European election 2019 it is important that the regulation is strictly followed. The Data protection officer will have to be consult regularly and we will need to follow his guidelines.*

Threat sources

The Treat sources we want to mitigate are:

Types of threat sources	Retained or not	Examples
Internal human resource, malicious, with weak abilities	Yes	✓ An employee could use an unlocked computer to get access to subject personal data. ✓ An employee with access to the database could cause a data breach by exporting data on a usb key
Internal human resource, malicious, with strong abilities	Yes	
Internal human resource, malicious, with unlimited abilities	No, there is no such profile in the unit.	
External human resource, malicious, with weak abilities	No	
External human resource, malicious, with strong abilities	Yes	✓ There are a lot of external people working for the unit from the cleaning team to developer and even project manager. ✓ The Subcontractor. ✓ The subcontractor's employee ✓ Attack on Subcontractor infrastructure ✓ Hacker trying to steal data subject password
External human resource, malicious, with unlimited abilities	No	
Internal human resource, without malice, with weak abilities	No, if the profile is not involved in the project there is no way he can cause a breach.	
Internal human resource, without malice, with strong abilities	Yes	✓ An employee could for example print personal data to work on it and maybe forget to take it at the printer.

Types of threat sources	Retained or not	Examples
Internal human resource, without malice, with unlimited abilities	No, there is no such profile in the unit.	✓
External human resource, without malice, with weak abilities	No	
External human resource, without malice, with strong abilities	No	
External human resource, without malice, with unlimited abilities	No	
Malware	No	
Natural phenomenon	No	
Natural or sanitary disaster	No	
Animal activity	No	
Internal event	Yes	Fire, network issues

The used matrix

The security criteria are: Availability, Integrity, confidentiality.

In order to express the security requirements, the security criteria are the following:

Security criteria	Definitions
Availability	The fact that the service is accessible when we need it
Integrity	The data held in the database must be complete and correct
Data Privacy	Only people who are allowed to have access to data have it

Availability scale

The following scale will be used in order to express the needs of security in term of availability:

Level of scale	Scale description
12 hours	The service must be available in the next 12 hours
6 hours	The service must be available in the next 6 hours
60 minutes	The service must be available in the hour

Integrity scale

The following scale will be used in order to express the needs of security in term of integrity:

Level of scale	Scale description
Allowed	The data can be wrong if we know it
mastered	The data can be wrong if we know it and the data is restored
Full	The data must be fully correct

Confidentiality scale

Who can have access to the data?

Profile	Profile description
Public	Everyone can access it
Limited	Only the editors in Brussels or in the Eplo offices can have access to this data
Private	Only the admin profile or the data subject itself can have access to this data

Probability

Scale level
1. Low
2. Medium
3. Strong
4. Maximal

Impact

Scale level
1. Low
2. Medium
3. Strong
4. Critical

Special security need

For the special security criteria “respect data regulation” the security need will always be “**respect**” since we are bind by law to respect the regulation.

Risk assessment

In this section we are going to enumerate the menaces that we would like to mitigate and evaluate them by probability and impact with the metrics described in point 2.5

Apprehended events

Events	Security needs	result	Sources	Impact
The data subject's personal data are stolen	Limited	✓ Data breach: The data can be altered, loss, used…	✓ Weak password ✓ Not serious employee ✓ hacker	Critical
Not respect the data protection law	Respected	✓ Loss of credibility ✓ Fines	✓ Employee's awareness ✓ Subcontractor not serious	Critical
The data subject's personal information are altered	mastered	✓ Contact wrongly a user ✓ Loss of subscription	✓ Database issue ✓ Employee mistakes	critical
The website unavailable	60 minutes	✓ Not able to recruit people ✓ Loss of credibility	✓ Server issue ✓ Server attack	Strong
The administration interface unavailable	6 hours	✓ Not able to manage people. ✓ Not able to contact people. ✓ Not able to treat the S.A.R.	✓ Server issue ✓ Server attack	Strong

User Session stolen

- Probability: Strong
- Impact: Low to critical. It depends whether if it's a simple user who got his password, in this case only his data will be compromise but if it's the session of an admin profile then the entire data base could be compromised.
- Apprehended events: The data subject's personal data are stolen
- Security requirement: Limited
- Scenario

  1) The password is too weak.

  2) The connection is intercepted, and the password is read.

  3) The cookie session is stolen

  4) The password in the data bases are stolen

Internal user that causes a data breach

- Probability: Maximal
- Impact: Strong
- Security requirement: Limited
- Scenario
  1) A user forgot to lock his session when he leaves his desktop.

  2) Export data on a support outside the application (hard copy, drive)

Adding data into the system without the proper consent

- Probability: Strong
- Impact: Maximal. Being in violation with the data privacy Regulation.

- Security requirement: Respected
- Apprehended events: Not respect the data protection law
- Scenario
  1) An admin decides to import data into the system from another database

  2) An Eplo collect data themselves during an event without getting the consent.

  3) The website collect data without consent.

Send private data to a third party

- Probability: strong
- Impact: Maximal. Being in violation with the data privacy Regulation.

- Security requirement:Private
- Scenario
  1) By customising the website it's possible to add some third-party embedded code like (Analytics, YouTube videos, google maps, twitter post...) Those third-party service could collect data on the data subject so it's important to alert the user on that and first ask for his consent.

Not being able to answer to a subject access request

- Probability: Strong
- Impact: Maximal
- Security requirement: ?
- Scenario
  1) The user would like to submit a subject access request but doesn't have any point of contact.

  2) The user submits a subject access request but nobody handles it.

The subcontractor does not comply with the Data privacy regulation.

- Probability: medium
- Impact: critical
- Security requirement: Limited
- Scenario
  1) The subcontractor uses subcontractor that are not compliant

  2) The subcontractor does not have an adequacy mechanism for hosting his data in the US

The website is not available

- Probability: medium
- Impact: Strong
- Security requirement: 60 minutes
- Scenario
  1) the server got a Ddos attack

  2) The server crashes

  3) Too many users connected and generate a lot of request on the server.

The database is accessed by non-authorise actor

- Probability: medium
- Impact: Strong
- Security requirement:Limited
- Scenario
  1)network access from outside

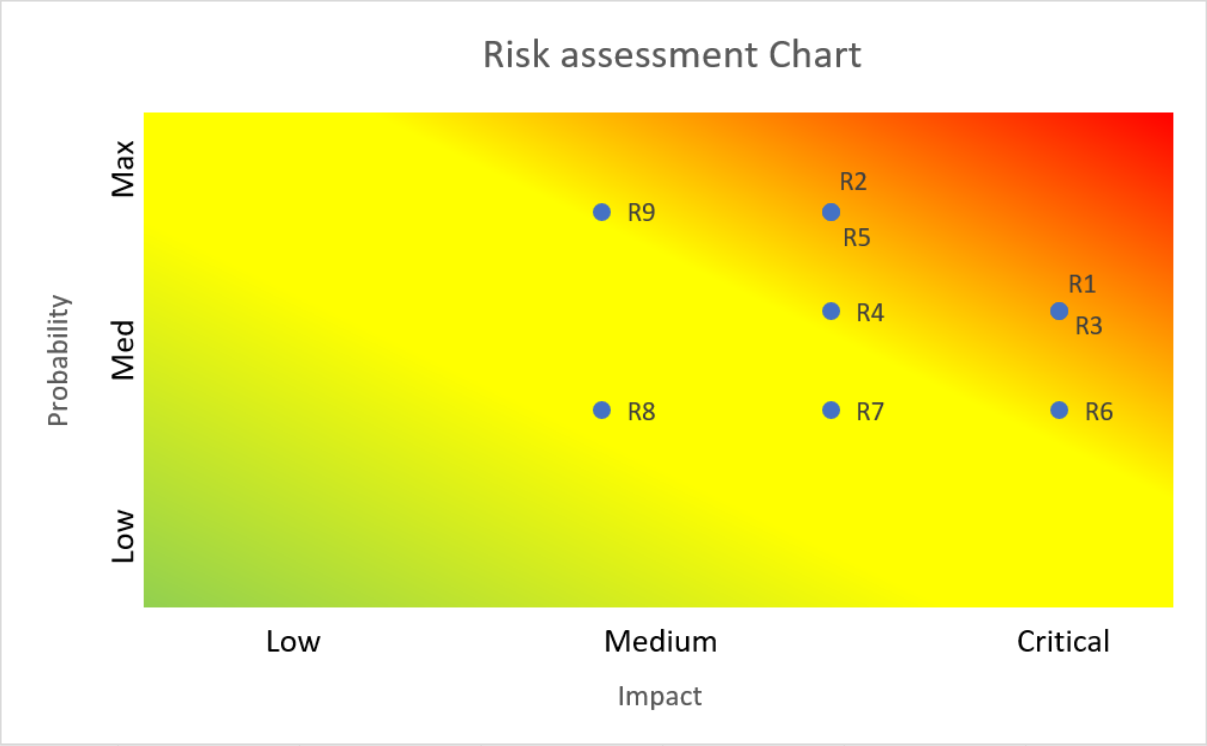
  2)network access from inside

The database is lost or its integrity compromised

- Probability: medium
- Impact: Critical
- Security requirement:Full
- Scenario
  1) The database server crashes

  2) The hard drive is compromised

  3) Someone else uses the same database and successfully overwrite some data.



Action plan to mitigate the risks

User Session stolen

To mitigate this menace several measures will be put in place.

- The subcontractor will have to set a minimum complexity for the password of 8 characters with at least one number, one letter and one special character. The system will also oblige the user to change his password every 90 days.
- Control panels and public pages will have to be protected by SSL encryption.
- Strong Encryption such as AES256 or TLS 1.2 for all “highly sensitive” communications, including transfer of customer data into their nation database must be used.
- All passwords will be hashed using the Bcrypt hashing algorithm and will never be stored in clear text.
- The secure flag for the session cookie has to be set so the cookie is sent only if the connection is secure.

Internal user that causes a data breach

- Like we said when we defined the perimeter of this study, a very important point is the data privacy. This new interest is there because of the new GDPR regulation that entered into force in May 2018. This regulation says that for all the new projects, the data privacy by design must be applied and the awareness of the employees must be raised. To mitigate the risks here several training will be organised about the tools itself, what we can do with it, how to process the data subject.

- A basic training will also be organised to present the new regulation, during this training concept like free and informative consent, data subject right, how to process rightfully the data…

- All the users have their own loggin and password, this will allow to log all the process done in the application and eventually detect a data breach.

Adding data into the system without the proper consent

- Part of this menace will be mitigated with the previous points measure (training and raising the awareness)
- Only the admin profile will be able to add data into the system, and first they need to get the green light from the data protection expert from the unit. The

expert will analyse if the data have been rightfully collected with a legal basis and if they can be used on the platform.

- On the website, in the subscription form there is a check box unticked by default that explain why we need the data asked to the data subject. Furthermore, in this text there is a link to the data privacy policy of the website. Only when the user checks this box, he is able to submit the form. The consent will be stored with a timestamp in the database.

Send private data to a third party

On this subject the regulation is quite clear, the data subject must be aware if his data is sent to a third party and his consent must be obtained before sending his data. That's what they call opt-out by default.

- To avoid this when the user arrives for the first time on the website all the third-party services (analytics, videos, maps…) are disabled. A banner is displayed with a message informing the data subject about the third-party services present on the website and 3 buttons

1. *Accept all*: when clicked the banner disappears and all the third-party services are loaded.
2. *Refuse*: the banner disappears and instead of the third-party services we have a blurred image with a message "to display this content accept the cookies" and a button accept
3. *Personalise*: it opens a pop-up, in this pop for all the third-party services there is a accept or refuse button.

Of course, this pop-up can be displayed later by a link in the footer.

Not being able to answer to a subject access request

The data subject has the right to submit subject access request and the unit have 1 month to reply. If needed they can warn the subject and tell him that the process can take up to 2 months.

- To allow the user to do these requests a functional mail box will be created (dataProtection@groundgame.eu). This functional mail box will be consulted every week by the data protection specialist of the unit. This person will have one month to analyse the request, accept it or not and reply to the user. To help him, the specialist can consult the data protection coordinator of the DG and the data protection officer of the European Parliament. The data controller will have to be added in the loop when a decision is reached and will have to validate it.
- To keep a trace of all data breach or S.A.R. a Jira project will be created in which every incident will be logged.

The subcontractor does not comply with the data protection regulation

To mitigate this risk a series of close will be added to the contract.

- The data processor shall be compliant with the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. In this regard, the data processor shall carry out a Data Protection Impact Assessment in accordance with Article 35 of the General Data Protection Regulation and provide the data controller with the results thereof as a deliverable of the contract.
- As of a date specified by the data processor to the data controller, the personal data collected and processed for the purpose of the contract shall be stored solely in the EU by any means and shall not be transferred outside the EU. Moreover, all data operations necessary for the purpose of the contract shall be processed within the EU(This is a request done by the data protection officer).
- No data operation shall take place without prior written approval of the data controller, including transfers of personal data.
- Interactions with data subject shall only take place via the data controller.
- The data controller shall be entitled to request the data processor to implement any additional technical or organisational measure necessary to comply with the General Data Protection Regulation.
- Where the Contractor subcontracts its obligations under this contract, it shall do only by way of sub-contracting agreement which impose the same obligations on the sub-contractor as are imposed on the contractor under this contract.

The website is not available

- Continuous monitoring of the system libraries and configuration must be performed.

- Weekly analysis of traffic will be performed to update the appropriate WAF rules, analyse system usage and performance, and to discuss new threat vectors that need to be proactively mitigated.

- 24/7 monitoring of the system that will automatically detect and trigger an incident if an urgent change is required to improve the performance of the system.

The database is accessed by non-authorised actor

- The application will have an isolated database, where the data is separate from other customers' data.

- Access to the databases can only occur within the Virtual Private Network where the application lives and cannot be accessed without the authorization to that network.
- Server access will be reserved to the Engineering Teams and will only be used to analyse issues to the infrastructure or problems.
- All access and interaction must be logged.

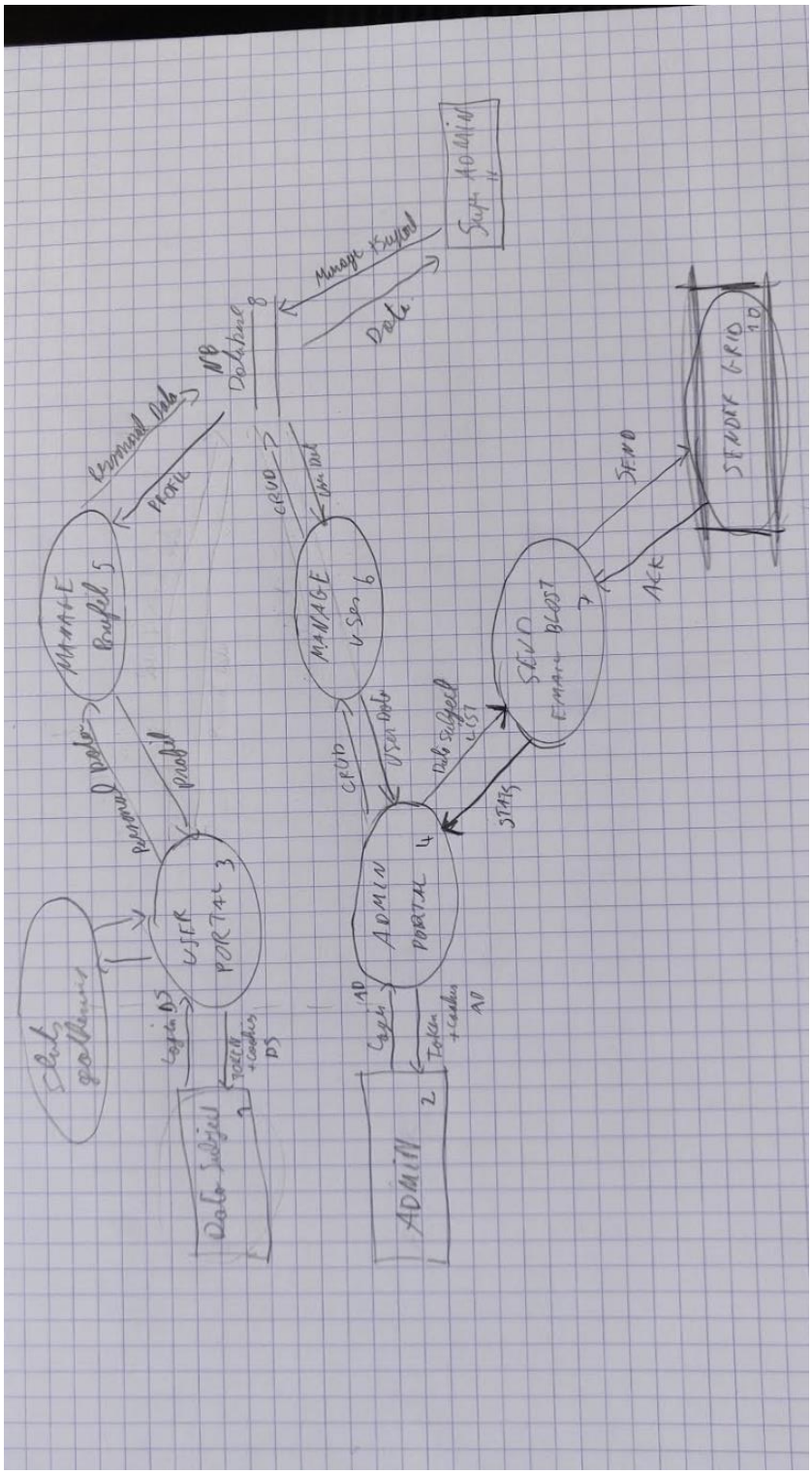
The database is lost or its integrity compromised

- The integrity of data will be reasonably protected from loss and degradation through daily redundancy backups.

- The data will also be backed up in the cloud on a weekly basis, to ensure that copies exist in the case of catastrophic database failure.

Annex 2 LINDDUN case study

Data flow diagram



MAPPING TABLE template

The data flow diagram is used to create the following table.

	L	I	N	D	D	U	N
ENTITY							
Data subject	X	X				X	
Admin	X	X				X	
Super admin	X	X				X	
Sender Grid	X	X					X
Stats gathering	X	X				X	X
PROCESS							
User portal	X	X	X	X	X		X
Admin portal	X	X	X	X	X		X
Manage profile	X	X	X	X	X		X
Manage user	X	X	X	X	X		X
Send email blast	X	X	X	X	X		X
Manage profile	X	X	X	X	X		X
DATA STORE							
NB database	X	X	X	X	X		X
DATA FLOW							
Login DS (1-3)	X	X	X	X	X	X	X
Token + cookies ds(1-3)	X	X	X	X	X	X	X
Login AD(2-4)	X	X	X	X	X	X	X
Token + cookies ad(2-4)	X	X	X	X	X	X	X
Personal data(3-5)	X	X	X	X	X	X	X
Profil(3-5)	X	X	X	X	X		X
Crud (4-6)	X	X	X	X	X		X
User data (4-6)	X	X	X	X	X		X
Datasubject list(4-7)	X	X	X	X	X		X
Stats(4-7)	X	X	X	X	X		X
Personal data(5-8)	X	X	X	X	X		X
Profil(5-8)	X	X	X	X	X		X
Crud(6-8)	X	X	X	X	X		X
User data(6-8)	X	X	X	X	X		X
Send(7-10)	X	X	X	X	X		X
Ack(7-10)	X	X	X	X	X		X
Manage and support(8-11)	X	X	X	X	X		X
Data(8-11)	X	X	X	X	X		X

Identify threat scenario

Assumptions

For the analysed system we do the following assumptions:

5. The processes that are done in the back-end are considered protected since the back-end has passed the pen-test done by DG-ITEC. The only threat that could come from inside it means people are having access to the application.
6. For the same raison as point 1 the communications between the process are also considered safe.
7. The communication between the entity and the system are not considered as safe since the entity can produce data breach if they do not respect the guidelines and also the communication channel is not considered as secure.
8. The data base is not considered as secure since admin have access to it and can retrieve information.
9. There is a risk of non-repudiation since the communication could be intercept and an attacker could take action in the name of the user.
10. Detectability is a threat since one could deduce that is a user pledge to vote on the plat-form it means that he is pro-eu.
11. The non-compliance is one of the main threats, specially whit this project that is used for the European elections.
12. The dataflow that is used to send email is a threat since personal data are sent to a third party.
13. For the same reason as the point 8, likability of the dataflow (7-10) is also a threat since third party could use the personal data.
14. Identifiability of the data flow 8-11 is a threat since there is no control on what data is consult by the super admin.
15. The spoofing of the data flow 1-3 and 2-4 are considered as threat since it could lead to a data breach.
16. The unawareness concern sonly the entity Data subject since they are the only one who provide personal data.
17. As for the back-end the database is considered secured from outsider attacks.
18. Attack between the system and third party like grid sender are not considered as a threat.
19. All the back-end processes are considered not corruptible.
20. The login system is considered as secure and well implemented.

Threat scenarios

For this part the threat tree of LINDDUN is used. https://linddun.org/catalog.php

T01

Spoofing of the entity user or admin

Summary

The attacker obtains the credentials of a user worst an admin and can then access to the data

Primary mis-actor

- An outsider attacker with a lot of competences.
- An internal attacker with low competences

Basic path

- The attacker gain access to a computer with an already logged account
- The attacker intercepts the communication.
- The attacker stole the session cookies

Consequence:

The attacker gains access to the system

Reference to threat tree node(s)

I_E_12, I_E_13,I_E_20

T02

The data subject is not aware of what information are collected and why.

Summary

The data subject not clearly informed on the data that are collected and the purpose.

Primary mis-actor

- The data controller and the developers that implement the portal.

Basic path

- Data are collected without explicit consent when the user land on the website.
- Data that are not really needed are collected.

Consequence:

The data subject is not correctly informed, and the consent is not valid.

Reference to threat tree node(s)

U_3,U_4,U_5

T03

Non compliance of sub-processor(sender-grid)

Summary

The contractor could use sub-contractor that does not respect the regulation.

Primary mis-actor

- The contractor

Basic path

- Use third party services without obliged them to respect the regulation.

Consequence:

The data subject rights are not respected and the platform is not compliant. It could lead to administrative fines and reputational damages.

Reference to threat tree node(s)

NC_3

T04 without consent

Data available to untrusted third party

Summary

The data are transmitted by mistake to third party actors

Primary mis-actor

- The developer team
- The ground game team

Basic path

- The developers or the ground game team uses third party features like google analytics, embedded Youtube link, twitter wall that could send data to third party

Consequence:

Personal data are sent to third party actors that could link the data.

Reference to threat tree node(s)

L_DF_6, L_DF_7,I_DF_5,I_DF_6

T05

The data are cross linked with other databases.

Summary

Even if in this project there is no sensitive data collected, the cross reference with other database could lead to sensitive data collection.

Primary mis-actor

- The ground game team
- The contractor who have access to the database

Basic path

- The ground game team has access to other database, they could for example cross reference data subject that comes to an event with the application data base to target them.
- The contractor could link the EP database and cross reference it with social media to get additional information.

Consequence:

Additional personal data could be collected without the consent to the data subject.

Reference to threat tree node(s)

L_DS_3

T06

Process on personal data is done with no real or bad purpose.

Summary

Administrators and super administrators have illimited access to personal data. It is important that control on this access is implemented.

Primary mis-actor

- The ground game team
- The super administrators

Basic path

- Someone access to the data base with no real reason and extract information.

Consequence

The data are processed whit no defined purpose.

Reference to threat tree node(s)

NR_P_1

Select corresponding privacy enhancing technology

In this section solutions will be proposed to mitigate the risks.

T01 Spoofing of the entity user or admin

- The subcontractor will have to set a minimum complexity for the password of 8 characters with at least one number, one letter and one special character. The system will also oblige the user to change his password every 90 days.
- Control panels and public pages will have to be protected by SSL encryption.

- Strong Encryption such as AES256 or TLS 1.2 for all “highly sensitive” communications, including transfer of customer data into their nation database must be used.
- All passwords will be hashed using the Bcrypt hashing algorithm and will never be stored in clear text.
- The secure flag for the session cookie has to be set so the cookie is sent only if the connection is secure.

T02 The data subject is not aware of what information are collected and why.

On the website, in the subscription form, there is a check box unticked by default that explain why we need the data asked to the data subject. Furthermore, in this text there is a link to the data privacy policy of the website. Only when the user checks this box, he is able to submit the form. The consent will be stored with a timestamp in the database

T03 Noncompliance of sub-processor(sender-grid)

Where the Contractor subcontracts its obligations under this contract, it shall do only by way of sub-contracting agreement which impose the same obligations on the sub-contractor as are imposed on the contractor under this contract.

T04 Data available to untrusted third party without consent

- To avoid this when the user arrives for the first time on the website all the third-party services (analytics, videos, maps…) are disabled. A banner is displayed with a message informing the data subject about the third-party services present on the website and 3 buttons
- *Accept all*: when clicked the banner disappears and all the third-party services are loaded.
- *Refuse*: the banner disappears and instead of the third-party services we have a blurred image with a message “to display this content accept the cookies” and a button accept
- *Personalise*: it opens a pop-up, in this pop for all the third-party services there is a accept or refuse button.

T05 The data are cross linked with other databases.

- The application will have an isolated database, where the data is separate from other customers’ data.
- No process on the personal data can be done without the agreement of the data controler

T06 Process on personal data is done with no real or bad purpose.

- No access to the data can be done without a proper credential and access rights.
- All the process on the data must be logged.
- The contractor will have defined procedure for the maintenance team and the support team that also have access to the databases.