UNIVERSITÀ POLITECNICA DELLE MARCHE

Faculty of Engineering
Department of Information Engineering
Master of Science in Biomedical Engineering

TOOLS FOR CYBER RISK ASSESSMENT OF COMPLEX INFRASTRUCTURES

Supervisor
Prof. Marco Baldi

Candidate
Giovanni Claudio Mele

Co-Supervisor
Massimo Battaglioni

Giulia Rafaiani

Academic Year 2020-2021

Index

1. Introduction

Cyber risk can be defined as any risk of financial loss, disruption, or damage to the reputation of an organisation due to some sort of failure of its information technology systems. Within organizations, cybersecurity must be one of the main focuses and companies should work to implement a cyber risk management strategy to be protected against constantly advancing and evolving cyber threats.

Cyber risk has become one of the highest priorities for organizations as they embrace digital transformation. Additionally, many organizations are increasingly reliant on third-party vendors or programs. While these resources can unlock and drive business success, they also introduce new threats.
One of the most common mistakes for organizations is not having a comprehensive understanding of the inherent risk that they take on when working with these additional resources. When the involved people know what they are dealing with and know what to do in case of danger, organizations can better manage risk before it becomes a bigger problem.

The three main components that define cyber risk are:

- **threat:** potential cause of an accident, which can cause damage to a system or organization;

- **vulnerability:** in cybersecurity, a vulnerability refers to weakness that can be exploited by attackers to gain unauthorized access;

- **consequence:** actual harm or damages that occur as a result of a network disruption. Typically, an organization will incur in both direct and indirect consequences as they work to remediate the problem. Depending on the attack, consequences may affect an organization finances, operations, reputation, and regulatory compliance status.

Risk assessment is inherently difficult due to its unpredictability; usually, the probability of occurrence of an event is estimated on the basis of history, together with the possible consequences, but this makes the results subject to errors [1].

The risk can be assessed in several ways: quantitatively, qualitatively or semi-quantitatively. Each of these methods has advantages and disadvantages.

Quantitative risk assessment methods use numeric probability where the probability expresses the chance that the event occurs. With quantitative approaches, risk is determined by the probability of an event and the likelihood of a loss. The results of the quantitative assessment are repeatable and reproducible and therefore, the estimation of the probabilities and impacts of the events can be compared directly and objectively. However, estimating likelihood and impact is challenging and may require interpretation and explanation [1].

Qualitative risk assessment methods typically use a series of methods, principles and rules based on non-numerical values for risk assessment. The advantages of qualitative methods are that these approaches are time and cost efficient because no exact value has to be determined and the areas of improvement can be easily identified. However, the disadvantage of qualitative methods is that they are not precise, as different experts could give very different results [2]. Additionally, they provide no measurement for the impact and therefore it is difficult to conduct a cost-benefit analysis [1].

Semiquantitative risk assessment methods usually use a variety of methods and rules for risk assessment using ranges, scales, or numbers. The scales and intervals can be easily translated into qualitative terms, but at the same time allow comparisons among values in different intervals or even within the same interval [2]. However, results combination and interpretation become more difficult because of different rating scales [1].

Both quantitative and qualitative assessments are usually carried out through three different types of approaches:

1. the first one implies the use of regulations concerning the world of information security; the information security risk management process can be summarized as follows:

    - context analysis;

    - identification of threats and vulnerabilities;

    - risk analysis to determine the consequences and estimate the probability of occurrence of a threat;

- evaluation of the consequences and priorities definition;

- evaluation of further countermeasures to be applied.

2. The second approach is based on checks/questionnaires deriving from lists of best practices. Through checks and/or interviews, the implementation of the controls defined by the framework chosen as reference is requested, and the level of implementation of these controls is evaluated within the organization through the calculation of an index, called maturity index. A negative deviation from a best practice is considered to be equivalent to an increase in risk.

3. The third approach uses risk scenario simulation techniques, through international frameworks of the ISACA family (such as COBIT for Risk [3]). This technique is suitable for the description of easily understandable risk scenarios related to the operational reality of the organization.

Two of the most used methods for the quantitative cyber risk assessment are: the method described by Hubbard and Seiersen in the book *"How To Measure Anything In Cybersecurity"* [4] (so-called **HTMA method)**, and the one described by Freund and Jones in *"Measuring and Managing Information Risk – A FAIR Approach"* [5] (so-called **FAIR method**).

Both methods offer a cyber risk assessment based on the use of estimates provided by cybersecurity experts as an input for a **Monte Carlo simulation**. On the one hand, the HTMA method allows to estimate the total risk due to a set of events and calculates the risk as a product of probability and impact. On the other hand, the FAIR method is oriented to the analysis of single scenarios and calculates the risk as a product of frequency and impact. The use of frequency makes it possible to consider the situation in which an event may occur several times in a certain time interval.

Another method for the quantitative cyber risk assessment is the **"Logistic Curve Method"** (this method is still under development, and it is not yet consolidated in the literature as HTMA and FAIR methods). This model takes as input the indexes of **complexity** and **maturity** of the organization and provides as output the likelihood of success of a single attack. This likelihood, weighted according to the **attractiveness** of the organization, is used to estimate the **likelihood** of having an adverse event in a certain period.

The relationship between complexity and maturity is modelled using the logistic function for two main reasons: the first one is that the logistic function has a trend that corresponds to that of the relationship between maturity and likelihood of success of an attack (an increase in maturity produces a decrease in the likelihood of success in a non-linear way, in fact, this decrease is more contained for very high or very low maturity values); the second reason is that using the so-called generalized logistic function, the complexity index can be introduced as a further parameter.

The Logistic Curve Method **(**a **scoring cyber risk assessment method)** uses questionnaires for the assessment of maturity and complexity; this allows the organization under examination to carry out a self-evaluation, without the need of the assessment provided by the cybersecurity experts. This model allows evaluating the actual cyber posture of the organization and estimating the likelihood starting from this, rather than relying on past events.

The aim of this work is to connect scoring and statistical cyber risk assessment methods. By using the outputs obtained with the Logistic Curve Method as inputs for the HTMA method, it is possible to obtain the assessment of the likelihood of occurrence of an adverse event and use it to perform the Monte Carlo simulation.

In order to do this, the logistic curve method has been implemented in an interactive web application entirely developed in R, using the Shiny package.

Using a table that correlates the 15 most frequent cyber threats to the 15 essential cybersecurity controls and another table in which it is possible to insert an assessment of the implementation of these controls, it is possible to evaluate the maturity index of the organization under exam for each type of threat. The complexity index and the value of the organization attractiveness can also be evaluated in the appropriate sections of the application.

As an output, the application offers the possibility to download a file (in the form of a CSV file) containing likelihood and impact related to each of the threats mentioned above, that can be used as an input for the HTMA method.

2. Scoring cyber risk assessment methods

Quantitative approaches are usually based on scoring systems that associate a certain score to a technological/organizational context.

The scoring cyber risk assessment methods offer a consistent and rigorous approach to assess and compare risks and risk management strategies; they are useful for providing a structured way to rank risks according to their probability, impact, or both, and for ranking risk reduction actions for their effectiveness. This is achieved through a predefined scoring system that allows to map a perceived risk into a category, where there is a logical and explicit hierarchy between categories.

These methods use questionnaires, surveys, or interviews for the risk assessment; this allows the organization under exam to evaluate the actual posture of the organization and estimate the probability of being attacked.

2.1 Logistic Curve Method

The Logistic Curve Method (so called because the relationship between complexity and maturity is modelled using the logistic function), based on **scoring systems**, **quantitatively** assesses the likelihood of occurrence of an adverse event. It takes **complexity and maturity indices** as input and gives as output the likelihood of success of a single cyber-attack. The latter, weighted according to the **attractiveness** of the organization, is used to estimate the likelihood of suffering an attack over a certain period.

This method consists of three steps:

1. **complexity assessment;**
2. **maturity assessment;**
3. **likelihood assessment.**

2.1.1 Complexity Assessment

In order to assess the complexity of the IT infrastructure, proceed with the compilation of the sheet "Complexity". This contains all the necessary controls for the evaluation of the complexity index; five main categories are considered: Network and Infrastructure, Technologies on IP Networks, Applications, Online Services, IT Department.

In the first section, "General Information", required data must be entered, while in the following sections, where required, questions must be answered using a drop-down menu (Figure 2.1). Some controls do not need a response from the user, as their complexity degree is automatically assigned based on the answers provided in the previous section.

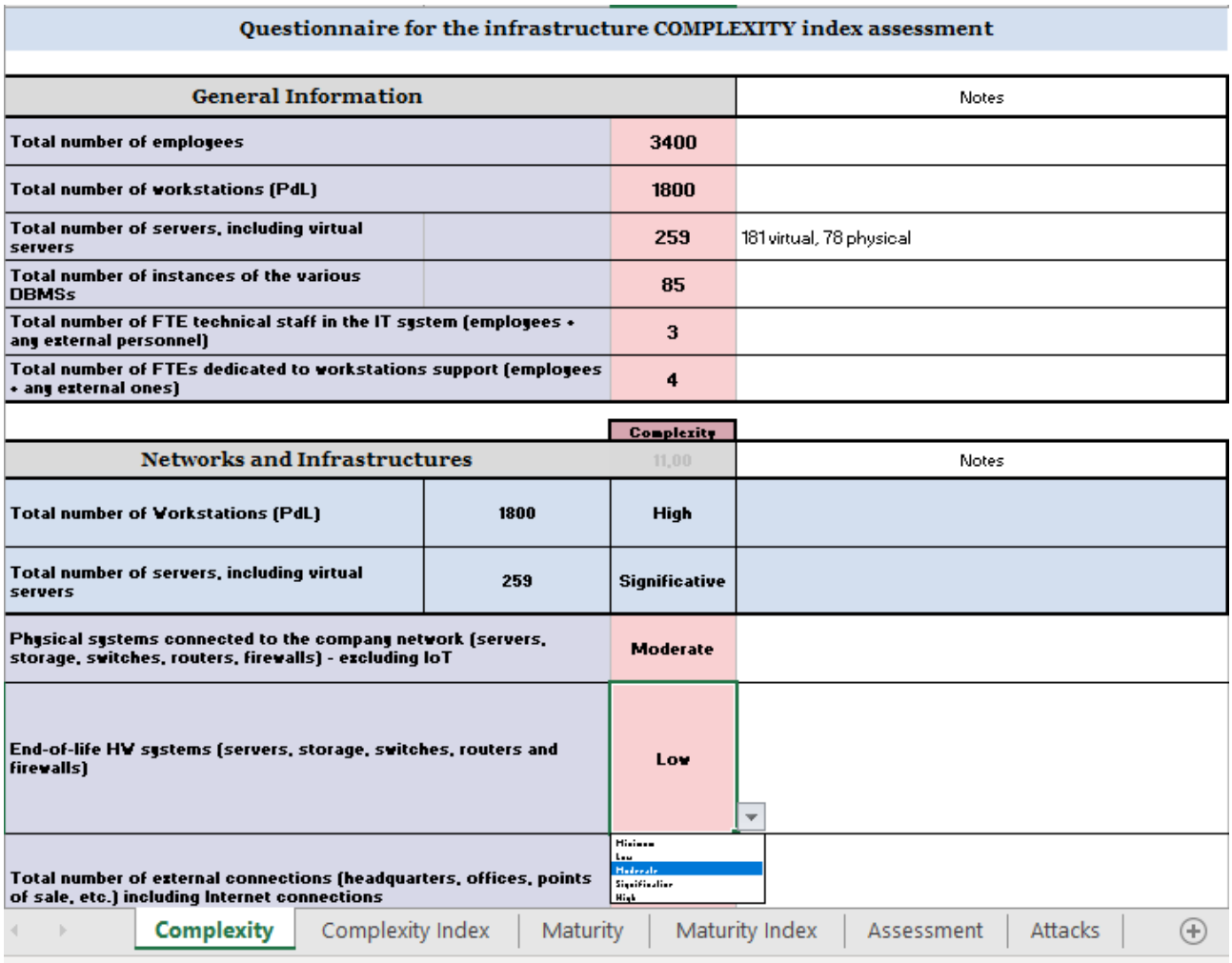


Figure 2.1. Extract of a questionnaire for the complexity assessment.

There are five selectable answers for each control (Minimum, Low, Moderate, Significative, High), in increasing order of complexity. The choice of the answer is guided through the descriptions, shown in the right column, of the value attributed to the selectable level of the drop-down menu. Figure 2.2 shows the controls section of the category "Applications" and the five columns that guide the answers to each question. It is possible to notice how the descriptions of the five levels of complexity aim to make the measure as objective as possible.

Applications		4,00	Notes	Score	Weights	Weighted average	Minimum	Low	Moderate	Significative	High
Total number of instances of the various DBMSs	85	High		5	130%	6,5	Minimum number of instances: (0-3)	Few applications (4-10)	Various applications (11-20)	Significant number of applications (21-40)	>40
Number of DBMS used, including the different versions within the same DBMS		High		5	120%	6	Number of DBMS and different versions <=1	Number of DBMS and different versions between 2 and 5	Number of DBMS and different versions between 5 and 10	Number of DBMS and different versions between 10 and 20	Number of DBMS and different versions>= 20
Use of identity access management systems		Low		2	60%	1,2	Use of Active Directory only	Active directory + LDAP	Active directory + SSO	IAM systems not integrated with HR	IAM integrated with HR systems
Applications and / or processes that process personal data		High		5	100%	5	The organization only processes personal data of employees	The organization also processes personal data of customers / users who are natural persons for the exclusive purpose of billing the products / services provided	The organization processes personal data of customers / users for other purposes besides billing (e.g. marketing, provision, etc.)	The organization processes sensitive personal data of customers / users OR carries out profiling treatments (including non-sensitive data)	The organization processes personal data of customers / users on a large scale
Application integration level		Significative		4	90%	3,6	The organization only processes personal data of employees	Integration of 2 core applications	Integration of between 3 and 5 core applications	Integration of 5-10 core applications	Integration of more than 10 core applications

Figure 2.2. Category "Applications" and the five columns that guide the user in the selection of the answer for each question.

In order to obtain a numerical evaluation of the complexity, a score is associated with each answer. For "Minimum" complexity the score is 1, for "Low" complexity, 2, for "Moderate" complexity, 3, for "Significative" complexity, 4, and for "High", 5. Within each category, a weight is associated with each control. This way, the score of the most important controls will have a larger weight in the final calculation of complexity. The result of the weighted average is then associated with a qualitative level of complexity to make it easier and more immediate to understand; the level is assigned as follows:

- score < 1.5 -> "Minimum";
- score < 2.5 -> "Low";
- score < 3.5 -> "Moderate";
- score < 4.5 -> "Significative";
- score ≥ 4.5 -> "High".

Figure 2.3 shows an example of how the complexity score is calculated for the category "Applications".

Applications		4,00	Notes	Score	Weights	Weighted average
Total number of instances of the various DBMSs	85	High		5	130%	6,5
Number of DBMS used, including the different versions within the same DBMS		High		5	120%	6
Use of identity access management systems		Low		2	60%	1,2
Applications and / or processes that process personal data		High		5	100%	5
Application integration level		Significative		4	30%	3,6
						4,46
						Significative

Figure 2.3. Complexity calculation example for the category "Applications".

The following sheet ("Complexity Index") reports the results of the complexity assessment. A summary table shows the values resulting from the complexity evaluation for each category of controls. The table also shows the arithmetic mean and a weighted average of the complexity of the entire technological chain; the weighted average weights are simply the ratio of the number of controls in each of the five categories to the total number of controls. For convenience and to facilitate understanding, the scores are multiplied by 2, in order to obtain a decimal scale. So, complexity is evaluated through an index, between 0 and 10, which describes the intrinsic complexity of the IT infrastructure. In the same sheet, a histogram graphically summarizes all the scores contained in the summary table. An example of summary table and of a histogram are shown in Figure 2.4 and Figure 2.5, respectively.

Summary Results of the Inherent Complexity Profile:

Inherent Complexity Profile (by Category)	Inherent Complexity Level	Complexity Weighted	N# Questions	Weight %
Networks and Infrastructure	Moderate	5,95	11	37,93%
Technologies on IP Networks	Moderate	5,00	4	13,79%
Applications	Significative	8,92	5	17,24%
Online Services	Moderate	5,33	3	10,34%
IT Department	Low	3,25	6	20,69%
Weighted average complexity	Moderate	5,71	29	

Figure 2.4. Example of summary table and calculation of complexity index.

Figure 2.5. Histogram that graphically summarizes weighted complexity for each category, arithmetic mean and weighted average of the complexity of the entire technological chain.

2.1.2 Maturity Assessment

The assessment of the organization maturity can be defined as the measure of the organization level of adherence to the controls defined by a specific reference framework. The organization should make an assessment based on the controls of one or more existing frameworks (for example CIS [9], ENISA [10], ISO [11] [12], FNCS [13]). The choice of the framework and, therefore, the set of the considered controls, determines the scope of application of the model. Using CIS controls, for example, the organization will determine its cybersecurity compliance, while controls proposed by ENISA will help the organization to assess its data protection compliance. The evaluation can be carried out simply by determining, through a yes/no choice, whether the control is fully implemented or not, or by evaluating how each control is implemented using a scale, assigning higher scores as the completeness of the control implementation increases (as previously done for the complexity assessment).

In the present model, we have considered the CIS v.7.1 [9] controls as the reference framework to evaluate the complexity. Therefore, the purpose of the assessment will be the IT security. CIS

proposes 20 main controls, which are in turn subdivided into sub-controls. Since the considered controls are very precise and specific in their requests, it has been chosen to use the binary option to evaluate their implementation. In order to proceed with the maturity assessment of the overall infrastructure, the user must fill in the checklist in the "Maturity" sheet using the drop-down menu. For each sub-control, it is possible to select one of the following answers:

- YES – to be selected when the control is considered satisfactorily applied.
- NO – to be selected when the control is considered applied only partially or in a non-compliant way.
- N/A - to be selected if the control is not applicable in the considered context.

An example of answers for the first control and related sub-controls is shown in Figure 2.6.

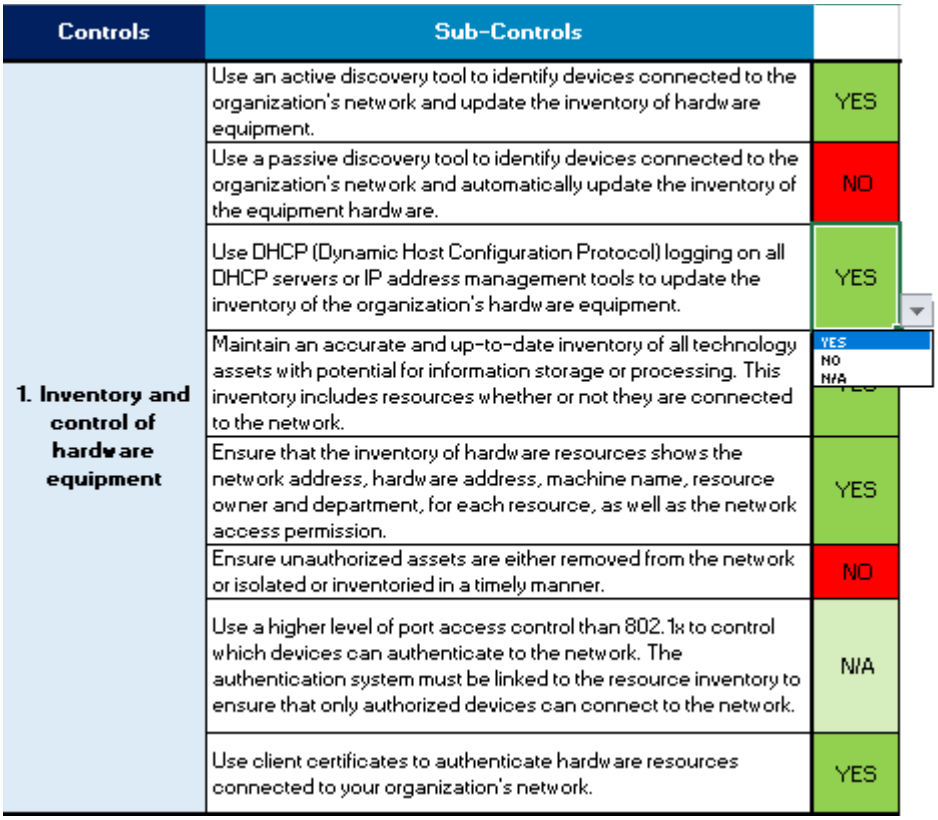


Figure 2.6. Example of sub-controls and possible answers.

To obtain a numerical evaluation of the maturity, a score is associated with each answer. If the answer is "YES", the score will be 1, while for sub-controls to which it has been assigned "NO" as answer, the score will be 0. "N/A" controls will be excluded from the numerical evaluation. Moreover, within each control, a weight is associated with each sub-control. In this case, the weights were assigned based on the Implementation group (IG) of the sub-controls. IGs are guidelines for prioritizing the use of CIS controls, focused on balancing resources constrains and effective risk reduction. Therefore,

a greater weight was assigned to sub-controls belonging to all three IGs and a progressively lower weight to the sub-controls belonging to IG2 and IG3 and to those belonging only to IG3. This way, the score of the most important sub-controls, i.e., those that must be implemented by all types of organizations, will have a greater weight in the final calculation of the maturity. A maturity value is associated to each of the 20 controls through a weighted average. The scores are multiplied by 10 to obtain values on a decimal scale.

Figure 2.7 shows an example of maturity assessment for the first control.

Controls	Sub-Controls		IG 1	IG 2	IG 3	Score	Weight	Weighted Average
1. Inventory and control of hardware equipment	Use an active discovery tool to identify devices connected to the organization's network and update the inventory of hardware equipment.	YES		X	X	1	95%	7,05
	Use a passive discovery tool to identify devices connected to the organization's network and automatically update the inventory of the equipment hardware.	NO			X	0	85%	
	Use DHCP (Dynamic Host Configuration Protocol) logging on all DHCP servers or IP address management tools to update the inventory of the organization's hardware equipment.	YES		X	X	1	95%	
	Maintain an accurate and up-to-date inventory of all technology assets with potential for information storage or processing. This inventory includes resources whether or not they are connected to the network.	YES	X	X	X	1	120%	
	Ensure that the inventory of hardware resources shows the network address, hardware address, machine name, resource owner and department, for each resource, as well as the network access permission.	YES		X	X	1	95%	
	Ensure unauthorized assets are either removed from the network or isolated or inventoried in a timely manner.	NO	X	X	X	0	120%	
	Use a higher level of port access control than 802.1x to control which devices can authenticate to the network. The authentication system must be linked to the resource inventory to ensure that only authorized devices can connect to the network.	N/A		X	X	N/A	95%	
	Use client certificates to authenticate hardware resources connected to your organization's network.	YES			X	1	85%	

Figure 2.7. Example of calculation of the weighted average for the first control.

The following sheet ("Maturity Index") reports the results of the maturity assessment in a similar way to those of the previously seen complexity. A summary table shows the values resulting from the maturity assessment for each control. The table also shows the arithmetic mean and the weighted average of the entire technological chain complexity; the weighted average weights are simply the ratio between the number of sub-controls present in each of the 20 controls and the total number of sub-controls. Maturity is then assigned through an index between 0 and 10. In the same sheet, there is also a histogram that summarizes all the scores of the summary table.

An example of summary table and of histogram are shown in Figure 2.8 and Figure 2.9, respectively.

Summary Results of the Maturity Profile:

	Maturity Profile *(by Category)*	Maturity Index	N° Questions	Weight %
1	Inventory and control of hardware equipment	7,05	8	4,68%
2	Inventory and Control of Software Assets	8,26	10	5,85%
3	Continuous Management of Vulnerabilities	4,34	7	4,09%
4	Controlled Use of Administrative Privileges	7,88	9	5,26%
5	Secure Configuration of Hardware and Software of Mobile Devices, Laptops, Workstations and Servers	6,20	5	2,92%
6	Maintenance, Monitoring and Analysis of Audit Logs	5,87	8	4,68%
7	Email and Web Browser Protection	8,95	10	5,85%
8	Malware Defense	7,60	8	4,68%
9	Limitation and Control of Network Ports, Protocols and Services	7,65	5	2,92%
10	Data Recovery Functionality	6,26	5	2,92%
11	Secure Configuration for Network Devices, such as Firewall, Router and Switch	5,87	7	4,09%
12	Defensive perimeter	7,06	12	7,02%
13	Data protection	7,66	9	5,26%
14	Access Control based on "what do I need to know"	8,87	9	5,26%
15	Wireless Access Control	6,91	10	5,85%
16	Account Monitoring and Control	5,96	13	7,60%
17	Adopt a Safety Awareness and Training Program	6,42	9	5,26%
18	Application Software Security	8,73	11	6,43%
19	Incident Management and Response	6,06	8	4,68%
20	Red Team Exercises and Penetration Test	6,15	8	4,68%
	WEIGHTED AVERAGE MATURITY	**7,08**	171	100%

Figure 2.8. Example of summary table and maturity index calculation.

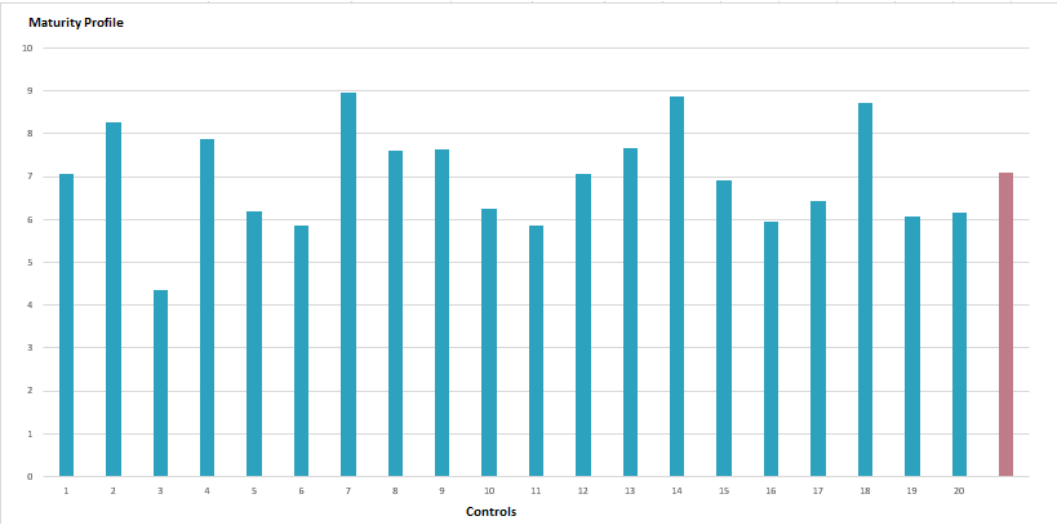


Figure 2.9. Example of histogram showing the Maturity scores for each sub-control and the weighted average maturity (red bar).

2.1.3 Likelihood Assessment

To quantitatively assess the likelihood that an adverse event occurs, the model takes as input the maturity and the complexity indices and gives as output the likelihood of success of a single attack. The latter, weighted according to the **attractiveness** of the organization, is used to estimate the **likelihood** of having an adverse event in a certain period of time.

In the proposed model, a generalised logistic function is used to model how the likelihood of success of an adverse event (data breach and/or attack) changes depending on the maturity of the considered infrastructure or organization.

It is assumed that the likelihood of success does not reach 0 and 1 in a finite regime; even in the worst case, there is always a probability that no adverse event occurs, and, vice versa, even when the maturity index reaches its maximum value, we cannot exclude the possibility that an adverse event will occur.

Figure 2.10 shows an example of the probability of success assessment for a complexity index equal to 5.71 and a maturity index equal to 7.08.

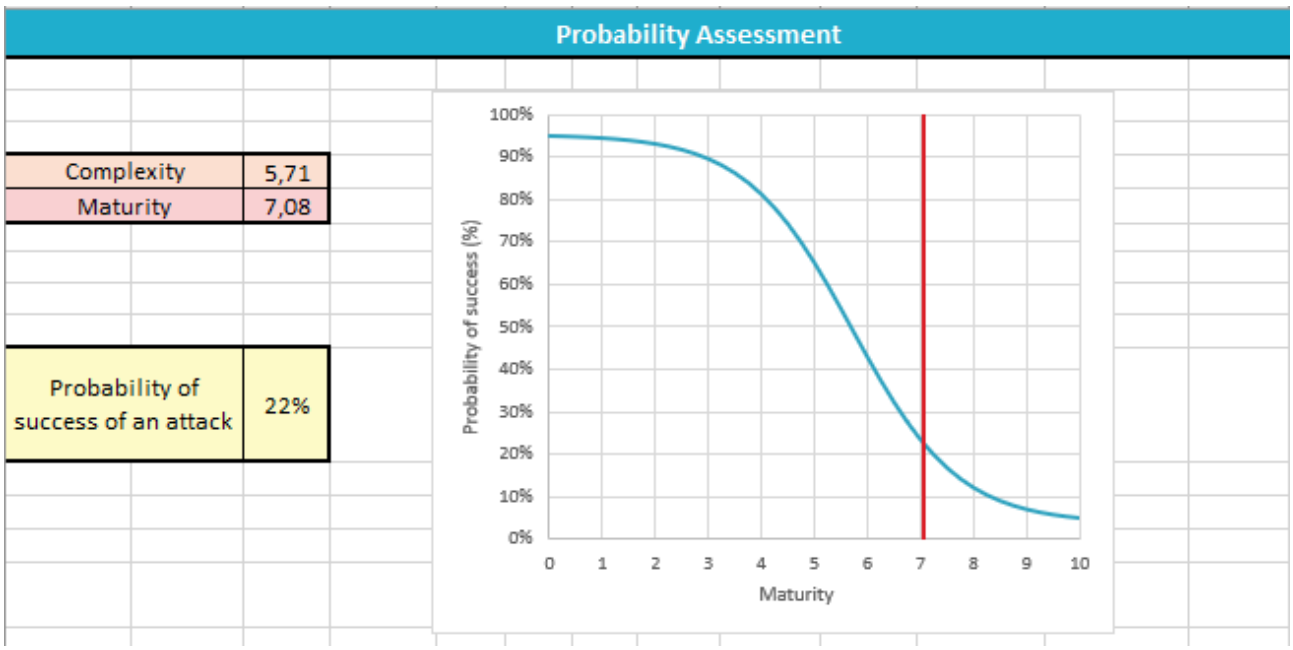


Figure 2.10. Example of probability of success assessment with a complexity index equal to 5.71 and a maturity index equal to 7.08.

Another parameter that has been considered in the model is the attractiveness of the organization: it depends on the type of business, the type of processed data, the purpose of the organization, and so on. Different organizations will have different attractiveness and will exposed to different levels of risk. The attractiveness also allows to estimate the number of attack attempts (n) to which the organization will be subjected in a given period of time. The attack attempts are uncorrelated, that is, it is assumed that the attackers repeat the same attack without changing its characteristics based on the outcome of the previous attacks.

The previously obtained likelihood of success is weighted according to the attractiveness of the organization.

The weighted likelihood of success, together with the number of attack attempts, is used to estimate the likelihood that the considered organization will suffer a successful attack in one year.

Figure 2.11 shows an example of the obtained results (likelihood of having a successful attack in one year): it is possible to select the organization type using a drop-down menu; attractiveness and number of potential attacks per year are automatically associated when a particular type of organization is selected, based on the attacks data shown in Figure 2.12.

Figure 2.11. Example of probability of having a successful attack in one year having n = 8.

				Critical	High	Medium
Multiple Targets	395	23,7%	29,9%	71	64	260
Online Services / Cloud	247	14,8%	91,5%	130	88	29
GOV - Mil - LEAs - Intel	203	12,2%	-19,4%	30	70	103
Healthcare	186	11,1%	17,0%	40	49	97
Banking / Finance	141	8,4%	-10,2%	16	38	87
Research - Education	100	6,0%	-8,3%	30	30	40
Software / Hardware / Vendor	83	5,0%	-23,9%	9	23	51
Entertainment / News	70	4,2%	-31,4%	15	24	31
Others	53	3,2%	76,7%	19	16	18
GDO / Retail	50	3,0%	28,2%	40	9	1
Critical Infrastructures	37	2,2%	-35,1%	3	15	19
Hospitability	27	1,6%	-40,0%	2	11	14
Org / ONG	18	1,1%	0,0%	9	4	5
Security Industry	17	1,0%	325,0%	3	9	5
Telco	17	1,0%	54,5%	2	7	8
Gov. Contractors / Consulting	11	0,7%	-21,4%	6	4	1
Automotive	10	0,6%	11,1%	7	3	0
Religion	3	0,2%	0,0%	0	3	0
Chemical / Medical	2	0,1%	100,0%	1	0	1
TOTAL	1670	100,0%				
	70,83	4,2%				

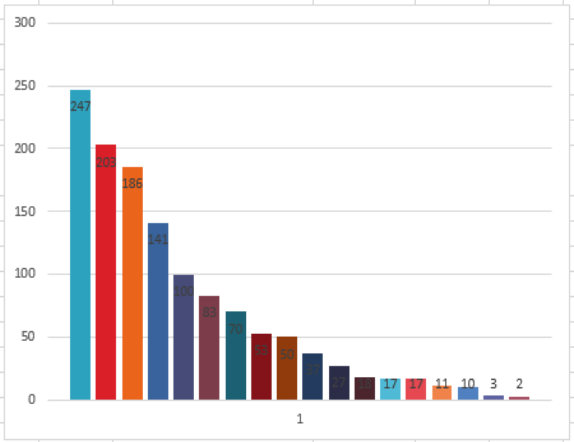


Figure 2.12. Number of attacks per year related to the type of organization.

3. Statistical cyber risk assessment methods

The cyber risk assessment and the factors that contribute to it can be evaluated in different ways: quantitatively, qualitatively, or semi-quantitatively.

Quantitative assessment uses methods to assess risk that produce repeatable and reproducible results, and therefore the estimation of probabilities and impacts of the events can be compared objectively.

However, the probability and impacts assessment is very challenging, and the results may require interpretations and explanations. In addition, the problems arising from costs and the possibility of having the necessary tools to carry out the evaluations must be considered.

Two known methods for the quantitative assessment of cyber risk are:

1) The method described in the book "How to Measure Anything in Cybersecurity Risk" by Douglas W. Hubbard and Richard Seiersen (abbreviated to **HTMA**) [4].
2) The method described in the book "Measuring and Managing Information Risk - A FAIR Approach" by Jack Freund and Jack Jones (called **FAIR** method) [5].

Elements that the two methods have in common are the use of the estimates from cybersecurity experts for the construction of probabilistic models and the use of Monte Carlo simulation as a tool for processing inputs.

The role of cybersecurity experts in the quantitative approach is to provide estimates of likelihood (in the form of probabilities/frequencies) and impact (in the form of monetary losses) that will be used to calculate the risk associated with the events. The HTMA and the FAIR methods, however, require experts' estimates in different ways and, as a consequence, differ in the type of probabilistic model based on these estimates.

Regarding the Monte Carlo simulation [7], the idea behind it is to evaluate the behaviour of a random variable by observing numerous random samples extracted from a pseudo-population that is as close as possible to the real population. The pseudo-population generally consists of a set of mathematical procedures designed to generate sets of numbers that are close samples drawn from the real population. The Monte Carlo simulation consists of the following steps:

1) specify the pseudo-population of the random variable of interest so that it can be used to generate samples.
2) Sampling the pseudo-population with a strategy appropriate to the phenomenon of interest.

3) Compute θ in the pseudo-sample and store it in a vector $\boldsymbol{\theta}$ (θ indicates the estimator of the variable of interest whose behaviour is to be evaluated).
4) Repeat steps 2 and 3 t times, where t is the number of iterations chosen for the simulation (trials).
5) Construct the relative frequency distribution of the values θ_t, which constitutes the Monte Carlo estimate of the sampling distribution of θ under the conditions specified by the pseudo-population and sampling procedures.

A Monte Carlo simulation can be seen as an analysis for "What-if" scenarios, such as those that are often done in Excel; the difference is that in Monte Carlo simulation the generation of scenarios is automated and is based on the random sampling of aleatory variables.

An aleatory variable represents the realization of an event that can assume a range of values. The probability of occurrence of each of these values is determined by the cumulative distribution function (CDF) of the variable, or $F(X)$. $F(X)$ is a function that, starting from a value of X (aleatory variable), for example x, returns the probability that a random sample of the variable with that distribution function has a value lower than x:

$$F(x) = P(X \leq x)$$

The definition of the pseudo-population consists in modelling the aleatory variable of interest as a relationship between constants, deterministic variables, and other known aleatory variables. An algorithm that uses this relationship to calculate the value assumed by the variable of interest starting from the randomly generated values is defined for the variables whose distribution is known. In this way, the random sampling of the variable of interest is simulated and its distribution, not known a priori, can be studied. The difficulties of the Monte Carlo simulation are the initial modelling effort, and the translation of the model into an algorithm that is able to correctly generate random values for the involved aleatory variables.

In the next section, the HTMA method will be illustrated in detail.

3.1 HTMA method

In the book “How to Measure Anything in Cybersecurity Risk”, Hubbard and Seiersen propose a method for quantitative assessment of cyber risk (HTMA method). This consists of four steps:

1) definition of the list of cyber events whose risk is to be assessed;
2) estimation of probability of occurrence and impact of each event;
3) scenario generation through Monte Carlo simulation;
4) results interpretation.

3.1.1 Definition of the list of cyber events whose risk is to be assessed

Risk is defined as "a state of uncertainty in which some of the possibilities involve a loss, a catastrophe or another unwanted outcome". The list must therefore include events involving a cyber risk; the number and the nature of the events to be listed are decided by who is conducting the analysis: the risks can be associated with a single vulnerability, a system, a business unit, or the entire organization.

3.1.2 Estimation of probability of occurrence and impact of each event

For each listed event, the organization cybersecurity experts have to estimate:

- **the probability of occurrence (likelihood);** it is the probability that the event occurs in a given time interval. Since a probability between 0 and 1 is associated with each event, this model does not consider the possibility that the same event may occur several times during the considered time interval.
- **The impact associated in case the event occurs, in the form of monetary loss (impact)**; it is the monetary loss associated with the occurrence of the event in a given time interval. It is estimated through a confidence interval of 90%, i.e. an interval of possible values for that parameter, identified by an upper limit (UB) and a lower limit (LB).

3.1.3 Scenario generation through Monte Carlo simulation

The listed events, with their respective probabilities of occurrence and impacts, are used as input for the Monte Carlo simulation. An example of the structure of the input is shown in Table 3.1.

EVENT	LIKELIHOOD	LB	UB
e_1	p_1	LB_1	UB_1
e_2	p_2	LB_2	UB_2
…	…	…	…
e_i	p_i	LBi	UB_i
…	…	…	…
e_n	p_n	LB_n	UB_n

Table 3.1. Inputs for the Monte Carlo simulation; the table shows the list of the events with the relative probability of occurrence and impact.

As previously seen, performing a Monte Carlo simulation means to study the trend of an aleatory variable of interest by simulating a random sampling through the generation of a large number of scenarios, in which each time the variable is calculated through the relationship that binds it to other known variables.

In this case, the random variable of interest is the **total annual risk** deriving from the cyber events in the list, expressed as monetary loss. The value of the total annual risk corresponds to the sum of the impacts of the events that occurred and, therefore, for each scenario, it depends on which events occur and the entity of loss associated with them.

Therefore, within a single scenario:

- the occurrence of each event must be simulated (occurred / did not occur), based on its probability;
- for the events that have not occurred, impact is set equal to 0, while for each event that has occurred the associated impact must be generated, compatibly with the range identified by its confidence interval of 90%;

- the generated impacts for all the events that occurred must be added up, in order to obtain the total impact that corresponds to the total annual risk.

To simulate the occurrence of each event e_i, proceed as follows:

- take p_i as input;
- generate a random number $r \in [0, 1]$ from the uniform distribution $U(0, 1)$; if $r < p_i$, the event occurred; if $r \geq p_i$, the event did not occur.

To generate an impact I_i compatible with the confidence interval of 90% of the event proceed as follows:

- take as input: LB_i and UB_i of the 90% confidence interval (CI);
- associate impact I_i with a lognormal probability distribution, deriving relative mean and standard deviation from LB_i and UB_i in the following way:
  - $\mu = \frac{\ln(UBi)+\ln(LBi)}{2}$
  - $\sigma = \frac{\ln(UBi)-\ln(LBi)}{3{,}29}$
- extract a random sample from the population whose distribution was defined in the previous step: this value corresponds to the impact I_i of the event.

The Monte Carlo simulation consists in repeating this procedure many times (1000, 10000, …). This way, it is possible to construct the distribution of the total annual risk starting from the values assumed by this variable in each generated scenario. Each iteration of the simulation expects to apply the procedure described above to each event of the input table.

For a number t of scenarios and indicating with **ALE_k (Annualized Loss Exposure)** the total annual risk obtained for each scenario k, the output shown in Table 3.2 is obtained.

SCENARIO	TOTAL ANNUAL RISK
1	ALE_1
2	ALE_2
…	…
k	ALE_k
…	…
t	ALE_t

Table 3.2. Output of the Monte Carlo simulation; the table reports the total annual risk (ALE, Annual Loss Exposure) for each scenario (for a number t of scenarios).

3.1.4 Results interpretation

The results obtained with the Monte Carlo simulation are used to create the **Loss Exceedance Curve, or LEC** (Figure 3.1)**,** which corresponds to the graphic representation of the Complementary Cumulative Distribution Function (CCDF) of the total annual risk (or ALE).

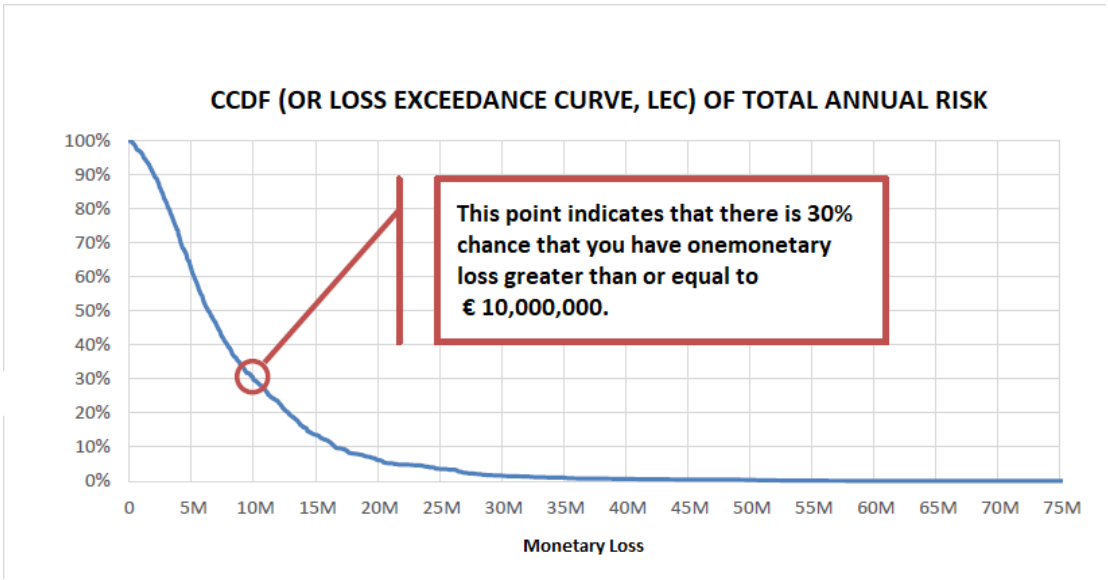


Figure 3.1. Example of Loss Exceedance Curve (LEC), or Complementary Cumulative Distribution Function (CCDF), of the total annual risk obtained with the results of the Monte Carlo simulation.

Each point of LEC, identified by a point l on the abscissa axis and a point *p* on the ordinate axis (l, *p*), represents the probability *p* that there will be a loss greater than or equal to l.

If the probability of occurrence and the impacts associated with the events have been estimated with reference to a situation in which only mandatory or necessary security measures are present, the obtained LEC represents the **Inherent Risk (inherent or intrinsic risk)** of the organization.

On the same graph in which the LEC of the Inherent Risk was represented, two other curves can be shown: the LEC of the Risk Tolerance and the LEC of the Residual Risk.

The LEC for **Risk Tolerance** can be constructed by asking the management to make explicit some points (l, *p*) and then interpolate a curve between them (for example, "a greater possibility or equal to 20% is considered acceptable for an impact of € 10,000 ", " a possibility greater than or equal to 60% is considered acceptable for an impact of € 1000 ", and so on).

Assuming the introduction of additional safety measures or the transfer of part of the risk through insurance, the Monte Carlo simulation can be repeated by modifying the probabilities and impacts associated with each event in an appropriate manner, thus obtaining the LEC related to the **Residual Risk**.

The three curves can be represented on the same graph, as shown in Figure 3.2.

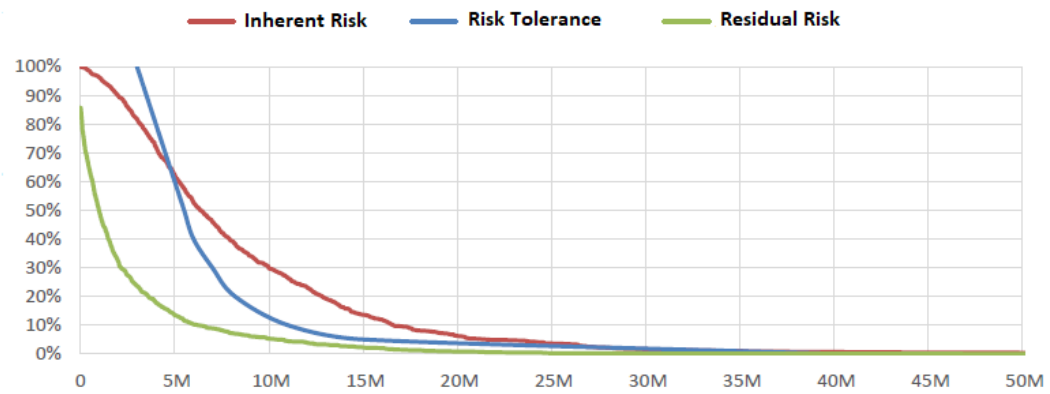


Figure 3.2. Graph representing LEC for Inherent Risk (red), Risk Tolerance (blue) and Residual Risk (green).

This graph is a useful tool for supporting decisions regarding cyber risk, as it allows you to immediately compare the present risk of the organization, its risk tolerance, and any benefit in terms of total annual risk reduction that would be achieved by implementing a specific strategy.

4. Joining scoring and statistical cyber risk assessment methods

Some quantitative cyber risk assessment methods, as HTMA and FAIR methods, require an historic of events for the assessment of the probability of occurrence, in particular the probability of suffering a cyber-attack due to a certain threat. Even when this historic exists, it hardly takes into account the company's cyber posture; therefore the probability assessment is applied to a company that is potentially different from the one on which the history is based.

To solve the problem, the model proposed in this work uses the **Logistic Curve method** to overcome this type of probability assessment: it provides an objective assessment of the likelihood of suffering an attack due to a cyber threat during a certain period of time (one year in this case) that considers the cyber posture of the organization, evaluated through the assessment of maturity and complexity indices provided by scoring cyber risk assessment methods. The outputs obtained from the Logistic Curve method will then be used as inputs for the HTMA method.

4.1 Maturity index assessment

The necessary steps for the assessment of the maturity index are described in the following sub-chapters.

4.1.1 Controls evaluation

In this model, the **15 essential cybersecurity controls** (Table 4.1) have been used for the maturity assessment. For each of these controls, it is necessary to provide an assessment of its implementation.

1	An inventory of systems, devices, software, services, and IT applications in use within the company perimeter exists and is kept up to date
2	The web services (social networks, cloud computing, e-mail, web space, etc.) offered by third parties to which you have registered are those strictly necessary
3	Critical information, data and systems for the company are identified so that they are adequately protected
4	It has been appointed a contact person who is responsible for coordinating the management and for the protection of information and IT systems
5	Laws and/or regulations with relevance in terms of cybersecurity that are applicable for the company are identified and respected
6	All devices that allow it are equipped with regularly updated protection software (antivirus, antimalware, etc ...)
7	Passwords are different for each account, of adequate complexity and the use of the most secure authentication systems offered by the service provider is evaluated (e.g., two-factor authentication)
8	Personnel authorized to access, remotely or locally, to the IT services have personal users that are not shared with others; access is suitably protected; old accounts that are no longer used are deactivated
9	Each user can only access the information and systems that he needs and/or is competent for
10	The staff is adequately sensitized and trained on the risks of cybersecurity and on the practices to be adopted for the safe use of company tools (e.g. Recognize e-mail attachments, use only authorized software, ...). The company's management takes care to prepare the necessary training for all company personnel to provide at least the basic notions of safety
11	The initial configuration of all systems and devices is carried out by expert personnel, responsible for their safe configuration. The default login credentials are always replaced
12	Backups of critical information and data for the company (identified in control 3) are periodically performed. Backups are stored securely and periodically verified
13	Networks and systems are protected from unauthorized access through specific tools (e.g., Firewall and other anti-intrusion devices/software)
14	In case of an incident (e.g., an attack or malware is detected) the security officers are informed, and the systems are secured by expert personnel
15	All software in use (including firmware) are updated to the latest version recommended by the manufacturer. Obsolete and no longer updatable devices or software are disused

Table 4.1. 15 essential cybersecurity controls [6].

For each of these controls, one of the following possible values must be assigned:

- **1** - to be selected when the control is considered satisfactorily applied.
- **0** - to be selected when the control is considered only partially applied or in a non-compliant way.
- **N/A** - to be selected if the control is not applicable in the considered context.

"N/A" controls will then be excluded from the numerical evaluation. An example of assessment of the implementation of these controls is shown in the Figure 4.1.

	Controls	Evaluation
1	An inventory of systems, devices, software, services and IT applications in use within the company perimeter exists and is kept up to date	1
2	The web services (social networks, cloud computing, e-mail, web space, etc.) offered by third parties to which you have registered are those strictly necessary	0
3	Critical information, data and systems for the company are identified so that they are adequately protected	0
4	It has been appointed a contact person who is responsible for coordinating the management and for the protection of information and IT systems	0
5	Laws and/or regulations with relevance in terms of cybersecurity that are applicable for the company are identified and respected	1
6	All devices that allow it are equipped with regularly updated protection software (antivirus, antimalware, etc ...)	1
7	Passwords are different for each account, of adequate complexity and the use of the most secure authentication systems offered by the service provider is evaluated (e.g. two-factor authentication)	1
8	Personnel authorized to access, remotely or locally, to the IT services have personal users that are not shared with others; access is suitably protected; old accounts that are no longer used are deactivated	0
9	Each user can only access the information and systems that he needs and/or is competent for	0
10	The staff is adequately sensitized and trained on the risks of cybersecurity and on the practices to be adopted for the safe use of company tools (eg. Recognize e-mail attachments, use only authorized software,...). The company's management takes care to prepare the necessary training for all company personnel to provide at least the basic notions of safety	1
11	The initial configuration of all systems and devices is carried out by expert personnel, responsible for their safe configuration. The default login credentials are always replaced	1
12	Backups of critical information and data for the company (identified in control 3) are periodically performed. Backups are stored securely and periodically verified	0
13	Networks and systems are protected from unauthorized access through specific tools (e.g. Firewall and other anti-intrusion devices/software)	0
14	In case of an incident (e.g. an attack or malware is detected) the security officers are informed and the systems are secured by expert personnel	
15	All software in use (including firmware) are updated to the latest version recommended by the manufacturer. Obsolete and no longer updatable devices or software are disused	1

Figure 4.1. Example of assessment of the implementation of the 15 essential cybersecurity controls.

4.1.2 Controls and threats correlation table

In the proposed model, the **15 most frequent threats according to the ENISA (European Union Agency for Cybersecurity) report** [8] have been considered (shown in Figure 4.2).

Figure 4.2. ENISA Threat Landscape 2020 – Top 15 Threats [8].

A table was built containing the 15 essential cybersecurity controls as rows, and the above mentioned threats as columns.

With this table, it is possible to establish a relationship between the implementation or non-implementation of a given control and the possibility of suffering a cyber-attack of a certain type. It is required to enter a value that will indicate how much the organization is exposed to the various threats in case a certain control is not implemented.

Four possible values have to be selected, each of which indicates how much a certain control is related to the different types of threats:

- **0**: if the control is not implemented, the organization is not exposed to this type of attack;
- **1:** if the control is not implemented, the organization is slightly exposed to this type of attack;
- **2**: if the control is not implemented, the organization is exposed to this type of attack;
- **3:** if the control is not implemented, the organization is very exposed to this type of attack.

Given the value $v = \{0, 1, 2, 3\}$ the corresponding weight $v/3$ will be used for the maturity assessment.

4.1.3 Maturity index

Once the assessment of the controls' implementation and of the controls/threats relationship has been obtained, for each threat, the maturity index is calculated through the following steps:

1. only weights different from 0 are considered;
2. multiply the weights by the implementation value of the relative control (excluding "N/A" controls) and sum the obtained results (denoted as w);
3. calculate the sum of all weights (denoted as W);
4. the maturity index (m) is obtained through the following formula: $m = 10\frac{w}{W}$.

4.2 Complexity index assessment

The **complexity index** is obtained through questionnaires, which contain all the necessary controls for the assessment divided into 6 different categories: "*General Information", "Networks & Infrastructure", "Technologies on IP Networks", "Applications", "Online Services", and "IT Department".*

For the category "General Information", it is necessary to enter the requested data (Figure 4.3). For the other categories it is required to answer the questions through one of the following values:

- **minimum;**
- **low;**
- **moderate;**
- **significative;**
- **high.**

To obtain a numerical evaluation of the complexity, a score is associated with each answer: for "Minimum" complexity, the score is **1**, for "Low", **2**, for "Moderate" complexity, **3**, for "Significative", **4**, and for "High" complexity, **5**.

Within each category, a **weight** is associated with each control (except for category "General Information", shown in Figure 4.3); this way, the score of the most important controls will have a greater impact on the final computation of the complexity.

	GeneralInformation	Value
1	Total number of employees	3400.00
2	Total number of workstations (PdL)	1800.00
3	Total number of servers, including virtual servers	259.00
4	Total number of instances of the various DBMSs	85.00
5	Total number of FTE technical staff in the IT system (employees + any external personnel)	3.00
6	Total number of FTEs dedicated to workstations support (employees + any external ones)	4.00
7	Maximum number of PdL x each FTE assigned to support	400.00
8	Maximum number of asset data centers (server + DB instances) for each FTE assigned to the information system	50.00
9	PdL x each FTE in charge of the support	450.00
10	DC Asset x each FTE involved in the SI	114.67

Figure 4.3. Example of complexity assessment for the category "General Information".

Figure 4.4 shows an example for the category "Networks & Infrastructures".

	NetworksAndInfrastructures	Evaluation	Score	Weight
1	Total number of Workstations (PdL)	Low	2.00	110.00
2	Total number of servers, including virtual servers	Low	2.00	110.00
3	Physical systems connected to the company network (servers, storage, switches, routers, firewalls) - excluding IoT	Significative	4.00	120.00
4	End-of-life HW systems (servers, storage, switches, routers and firewalls)	Moderate	3.00	100.00
5	Total number of external connections (headquarters, offices, points of sale, etc.) including Internet connections	High	5.00	100.00
6	Number of non-secure connections (non-users) from outside (FTP, Telnet, rlogin, VNC ..)	Low	2.00	80.00
7	Customers or partners with dedicated connections	Minimum	1.00	90.00
8	Access to Wireless Networks	Minimum	1.00	90.00
9	Use of personal devices capable of connecting to the company network	Low	2.00	100.00
10	Number of installations of SERVER Operating Systems in End-of-life (without official support from the manufacturer)	Moderate	3.00	100.00
11	Number of installations of CLIENT Operating Systems in End-of-life (without official support from the manufacturer)	Minimum	1.00	100.00

Figure 4.4. Example of complexity assessment for the category "Networks and Infrastructures".

Once the data of each category are entered, proceed as follows:

1. for each control of each category (excluding the category "General Information") it is calculated:

$$\frac{score \times weight}{100}$$

The average is calculated from the obtained result and then multiplied by 2, to obtain a decimal scale and facilitate understanding (the result will be denoted as *cw,* **weighted complexity**);

2. a weight (%), *c*, is associated to each category and it is calculated as:

$$c = \frac{number\ of\ controls\ in\ the\ category}{total\ number\ of\ controls}$$

3. the complexity index (*M*) is obtained as:

$$M = \frac{\sum_1^i (cw_i \times c_i)}{100}$$

where *i* is the number of categories.

4.3 Attractiveness evaluation

For attractiveness evaluation, it is possible to choose between 5 different values:

- **very low;**
- **low;**
- **average;**
- **high;**
- **very high.**

In this model, a weight has been associated with each of these values: if the attractiveness evaluation is "Very Low", the weight is **-40%**, if the attractiveness is "Low", the weight is **-30%,** if it is "Average", the weight is **-20%**, if it is "High", the weight is **-10%** and if the attractiveness is "Very High", the weight is **0%**.

These weights are examples of parameters used in this model, but they are not fixed and can also be changed.

The attractiveness of the organization allows also to estimate the **number of attack attempts** it will be subjected to in a given period of time (one year in this case). The relationship between the attractiveness evaluation and the potential number of attacks per year is shown in Figure 4.7.

Attractiveness	Very Low	Low	Average	High	Very High
	2	4	6	8	10

Figure 4.7. Table showing the relationship between attractiveness value and potential number of attacks per year.

4.4 Likelihood assessment

Once the maturity index, the complexity index and the attractiveness value have been collected, there are two more steps to perform for the likelihood assessment:

1. assessment of the **weighted probability of success of an attack**;
2. assessment of the **likelihood of a successful attack in one year**.

4.4.1 Weighted probability of success of an attack

To assess the weighted probability of success of an attack, a table consisting of three columns is created:

- **column 1**: it contains a numerical interval from 0 to 10, with interval step equal to 0.25.
- **Column 2**: the values in this column are calculated through the following formula:

$$y(t) = A + \frac{K - A}{(1 + Qe^{-B(t-M)})^{1/v}}$$

where:

$B = -1$

$Q = 1$

$v = 1$

$$A = \frac{-0.9 \times e^{M} + 0.05 \times e^{10} - 0.95}{e^{10} - 1}$$

$$K = \frac{(e^{-M} \times (0.9 \times e^{10}) - 1.9) + (0.95 \times e^{10} - 1.85)}{e^{10} - 1}$$

$t = corresponding\ value\ in\ the\ first\ column$

$M = Complexity\ index$

- **Column 3**: the values contained in this column are calculated as the absolute value of the maturity indices minus *t*.

The minimum value of the third column is then calculated, and the corresponding value of the second column is denoted as "***min***".

The **weighted probability of success of an attack** is evaluated as:

$$P = (min + min \times a) \times 100$$

where ***a*** is the attractiveness weight.

This process must be repeated for each of the 15 threats to obtain the weighted probability of success of an attack for each type of threat.

4.4.2 Likelihood of a successful attack in one year

To assess the likelihood of having a successful attack in one year, a table with 3 columns is created:

- **column 1**: its row elements are values of a numerical interval that goes from the number of attack attempts (obtained through the attractiveness assessment) to 1, with an interval step equal to 1.
- **Column 2**: the elements in this column are calculated through the following formula:

$$(min \times (1 - min))^{u-1}$$

where *min* is the value obtained in the previous chapter and *u* is the corresponding value in the first column.

The **likelihood of having a successful attack in one year** is given by the sum of the values contained in the second column of the table.

This process must be repeated for all the threats in order to assess the likelihood of a successful attack for each type of threat.

Using the proposed method, it is possible to obtain a list of the 15 most frequent threats with the relative likelihood of occurrence; an impact, in terms of monetary loss, is also reported for each of the threats (Table 4.2) represented by a lower limit (LB) and an upper limit (UB). Impacts are just examples that can represent medium and large organizations.

Threat	LB	UB
Malware	1000$	2500000$
Web-based attacks	100000$	2000000$
Phishing	1000$	1600000$
Web application attacks	1000$	500000$
Spam	1000$	1600000$
DDoS	50000$	2000000$
Identity theft	1000$	100000$
Data breach	10000$	4000000$
Insider threat	10000$	700000$
Botnets	50000$	2000000$
Physical manipulation, damage, theft, and loss	1000$	60000$
Information leakage	10000$	4000000$
Ransomware	300$	170000$
Cyberespionage	1000$	70000$
Cryptojacking	1000$	10000$

Table 4.2. Table showing possible upper (UB) and lower limit (UB) for impacts related to different type of cyber threat.

The so-obtained result can then be used as an input for the HTMA method, providing an assessment of the likelihood of occurrence of an attack to perform the Monte Carlo simulation.

5. Software implementation

The method described above has been implemented in an interactive **web application** developed entirely in R.

The R language was chosen mainly owning the following advantages: being a language oriented to statistical analysis, R offers numerous tools for data manipulation. R's functionalities are also extendable through numerous packages, such as the **Shiny package** used for the development of the web application.

5.1 Web application

The web application is divided into a home page and five sections.

The home page ("*Home*") (Figure 5.1) explains how the tool works and offers a brief explanation of the structure of the application itself.

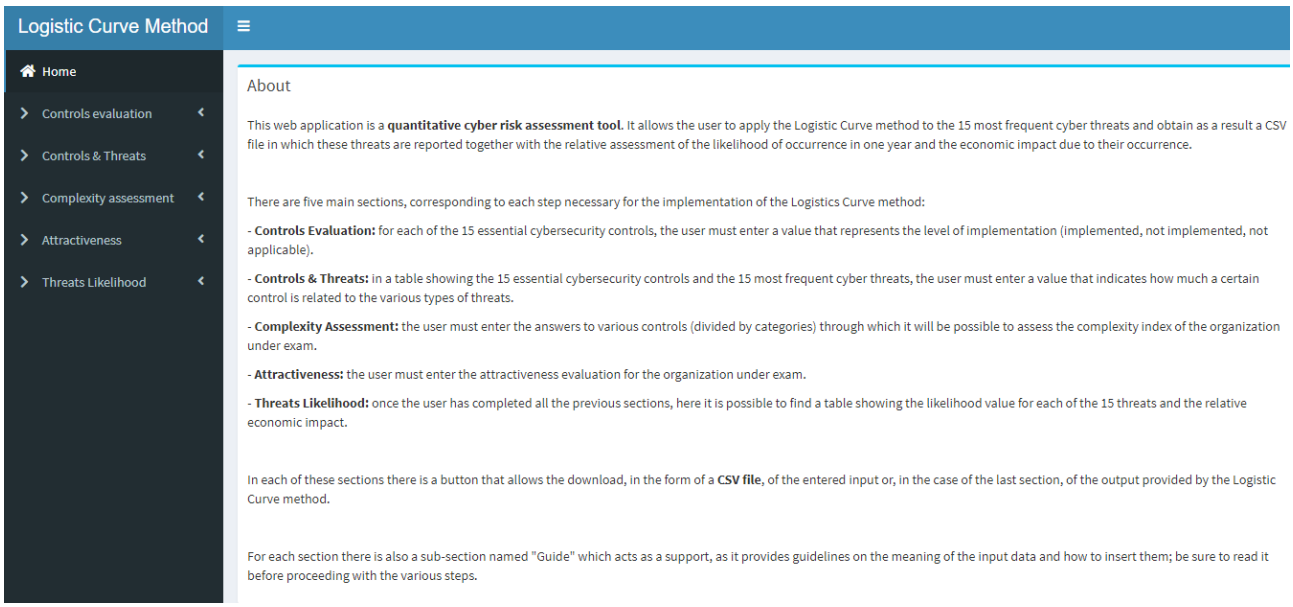


Figure 5.1. Web application home page ("Home").

Using the menu on the left, the user can access the various sections, "*Controls evaluation*", "*Controls & Threats*", "*Complexity assessment*", "*Attractiveness*" and "*Threats Likelihood*".

5.1.1 Controls evaluation

The "Controls evaluation" section is in turn divided into two sub-sections: "*Guide*" (Figure 5.2) and "*CSV Controls evaluation*" (Figure 5.3).

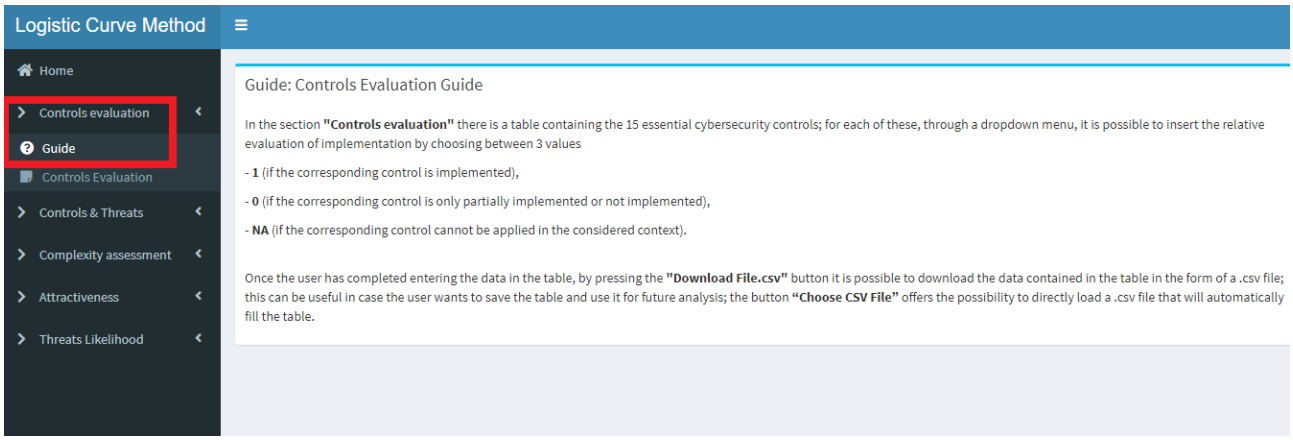


Figure 5.2 Controls evaluation section, sub-section "Guide".

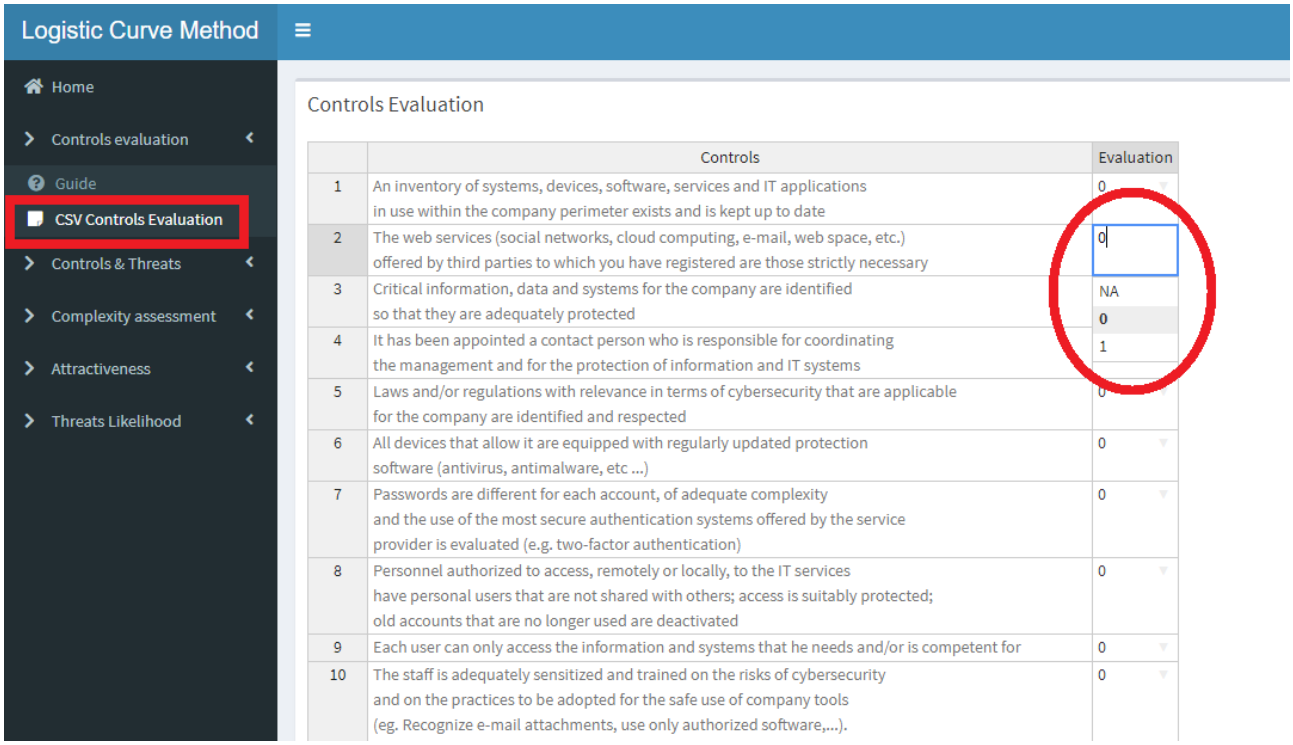


Figure 5.3 Controls evaluation section, sub-section "CSV Controls Evaluation".

The sub-section "*Guide*" acts as a support, as it provides guidelines on the meaning of the input data and how to insert them.

In the sub-section "*CSV Controls evaluation*" there is a table containing the 15 essential cybersecurity controls [6]; for each of them, through a drop-down menu, it is possible to insert the relative evaluation of implementation by choosing between 3 values:

- **NA**: the corresponding control cannot be applied in the considered context;
- **0**: the corresponding control is only partially implemented or not implemented;
- **1**: the corresponding control is implemented.

Once the user has completed entering the data in the table, it is possible to find two buttons below it (Figure 5.4):

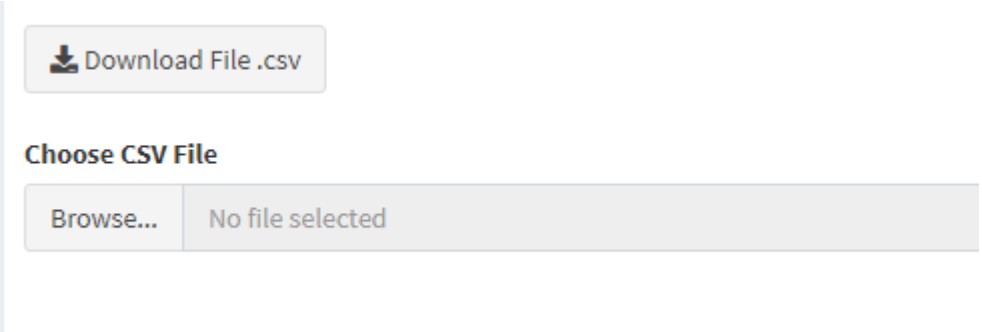


Figure 5.4 Download button (upper) and input button (lower).

- by pressing the ***"Download File.csv"*** button it is possible to download the data contained in the table in the form of a .csv file; this can be useful in case the user wants to save the table and use it for future analyses;
- the button ***"Choose CSV File"*** offers the possibility to directly load a .csv file that will automatically fill the table.

5.1.2 Controls & Threats

The "Controls & Threats" section is in turn divided into two sub-sections: "*Guide*" (Figure 5.5) and "*CSV Controls & Threats*" (Figure 5.6).

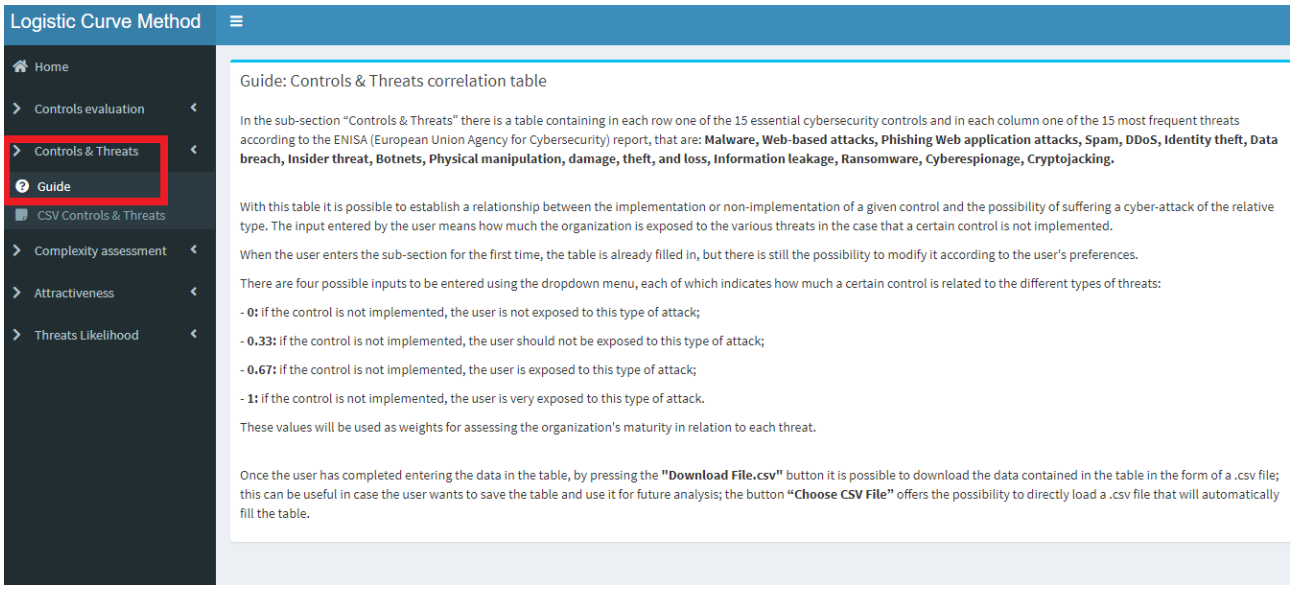


Figure 5.5. Controls & Threats section, sub-section "Guide".

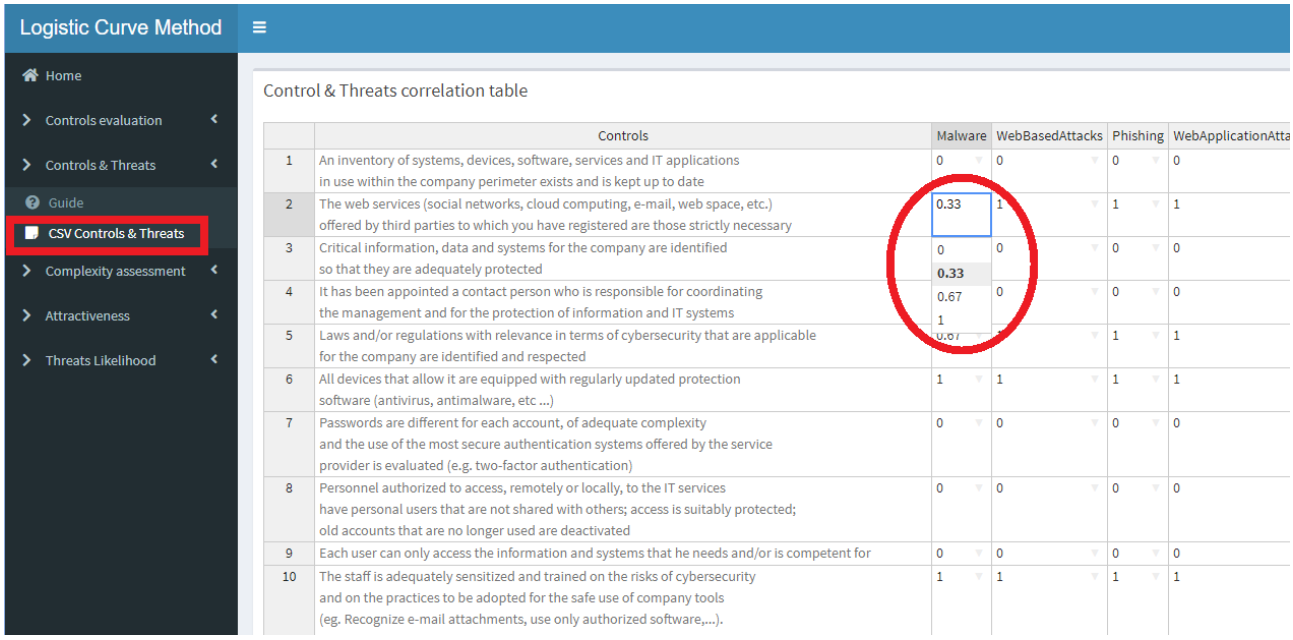


Figure 5.6. Controls & Threats section, sub-section "CSV Controls & Threats".

The sub-section "*Guide*" acts as a support, it provides guidelines on the meaning of the input data and how to insert them.

In the sub-section *"CSV Controls & Threats"* there is a table containing in each row one of the 15 essential cybersecurity controls and in each column one of the 15 most frequent threats according to the ENISA (European Union Agency for Cybersecurity) report [8].

With this table, it is possible to establish a relationship between the implementation or non-implementation of a given control and the possibility of suffering a cyber-attack of the relative type. The input entered by the user represents how much the organization is exposed to the various threats in the case that a certain control is not implemented.

When the user enters the sub-section for the first time, the table is already filled in, but there is still the possibility to modify it according to the user's preferences.

There are four possible inputs to be entered using the dropdown menu, each of which indicates how much a certain control is related to the different types of threats:

- **0**: if the control is not implemented, the user is not exposed to this type of attack;
- **0.33:** if the control is not implemented, the user should not be exposed to this type of attack;
- **0.67**: if the control is not implemented, the user is exposed to this type of attack;
- **1:** if the control is not implemented, the user is very exposed to this type of attack.

These values will be used as **weights** for assessing the organization's maturity in relation to each threat.

Once the user has completed entering the data in the table, at the bottom of the page there are two buttons (Figure 5.7):

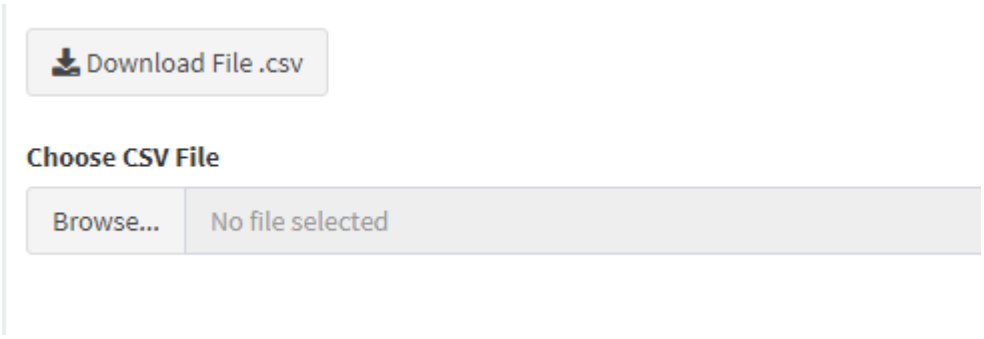


Figure 5.7. Download button (upper) and input button for a .csv file (lower).

- by pressing the ***"Download File.csv"*** button it is possible to download the data contained in the table in the form of a .csv file; this can be useful in case the user wants to save the table and use it for future analyses;
- the button ***"Choose CSV File"*** offers the possibility to directly load a .csv file that will automatically fill the table.

5.1.3 Complexity assessment

The "Complexity assessment" section is in turn divided into seven sub-sections: "*Guide*" (Figure 5.8), "*General Information*" (Figure 5.9), *"Networks and Infrastructures"* (Figure 5.10), *"Technologies on IP Networks"* (Figure 5.11), *"Applications"* (Figure 5.12), *"Online Services"* (Figure 5.13), and *"IT Department"* (Figure 5.14).

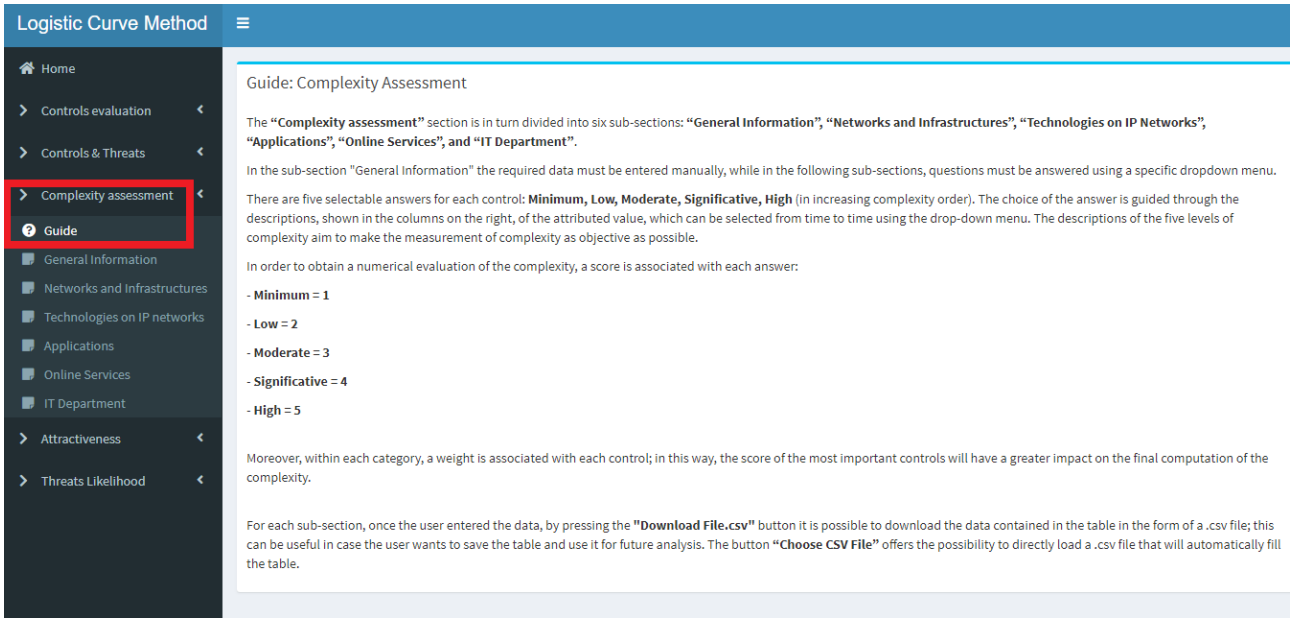


Figure 5.8. Complexity assessment section, sub-section "Guide".

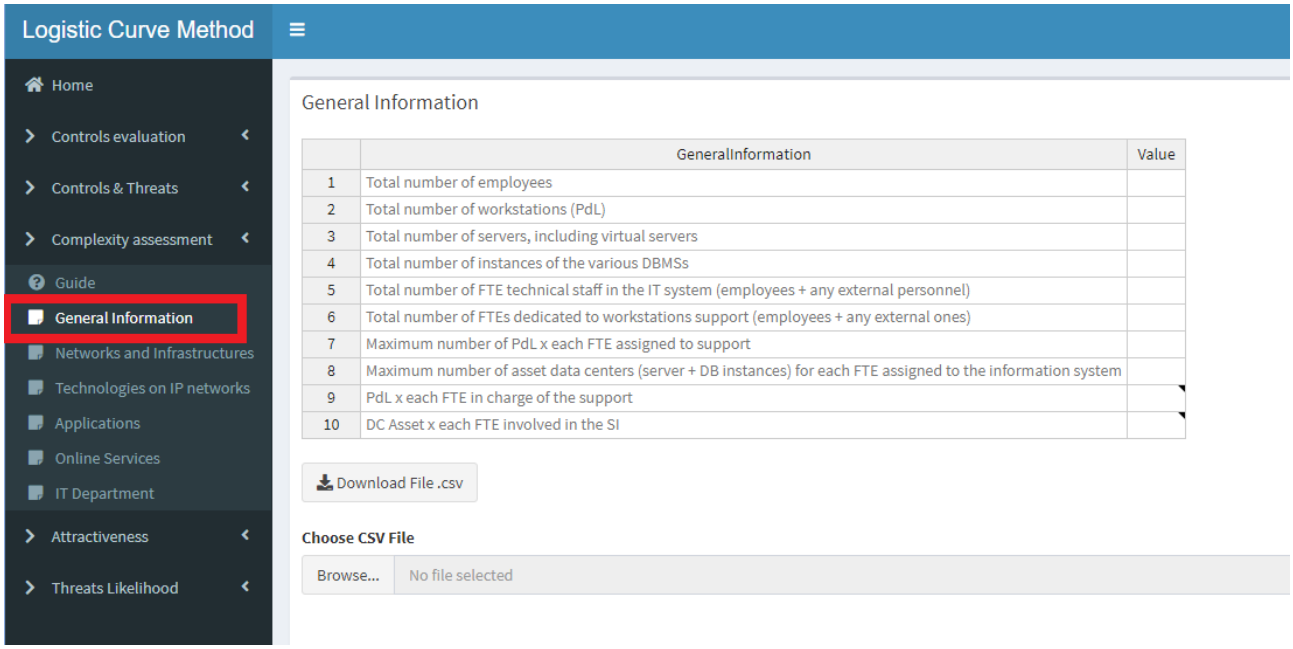


Figure 5.9. Complexity assessment section, sub-section "General Information".

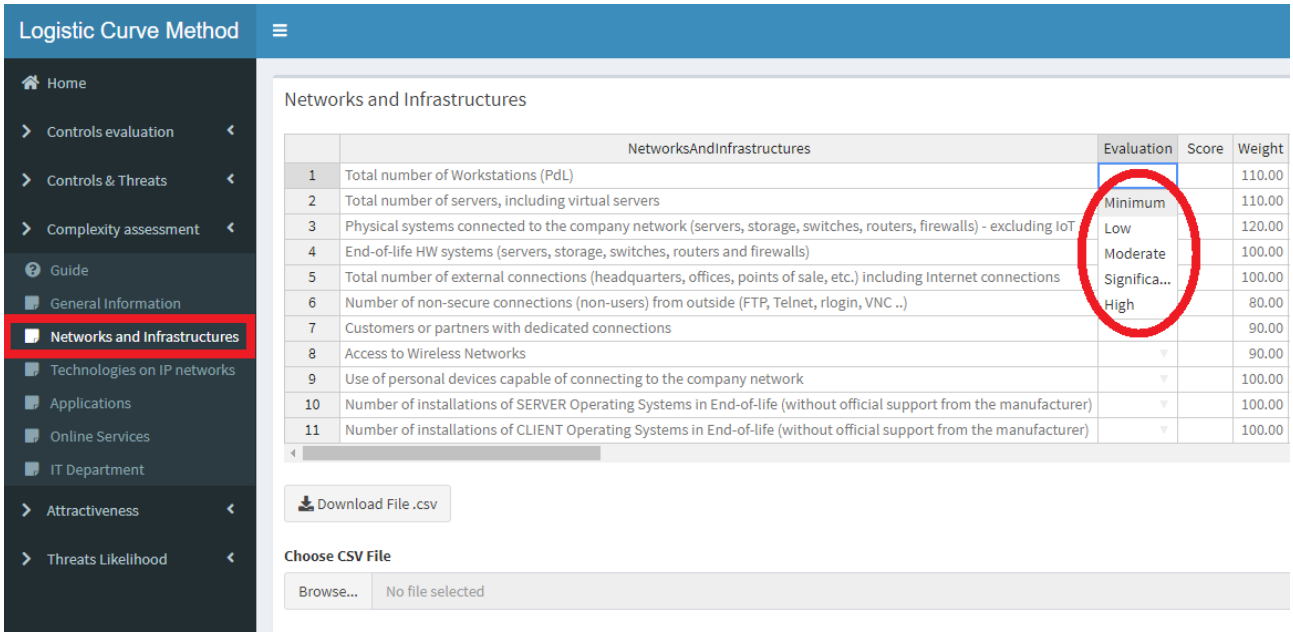


Figure 5.10. Complexity assessment section, sub-section "Networks and infrastructures".

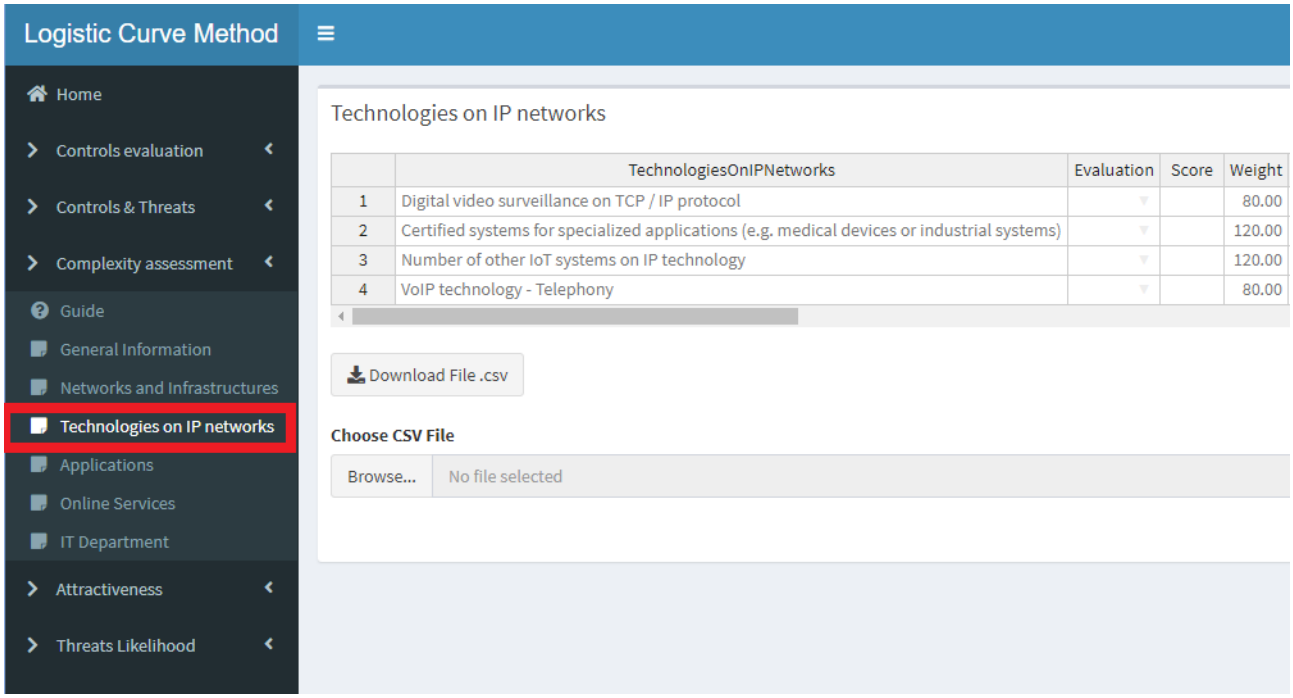


Figure 5.11. Complexity assessment section, sub-section "Technologies on IP networks".

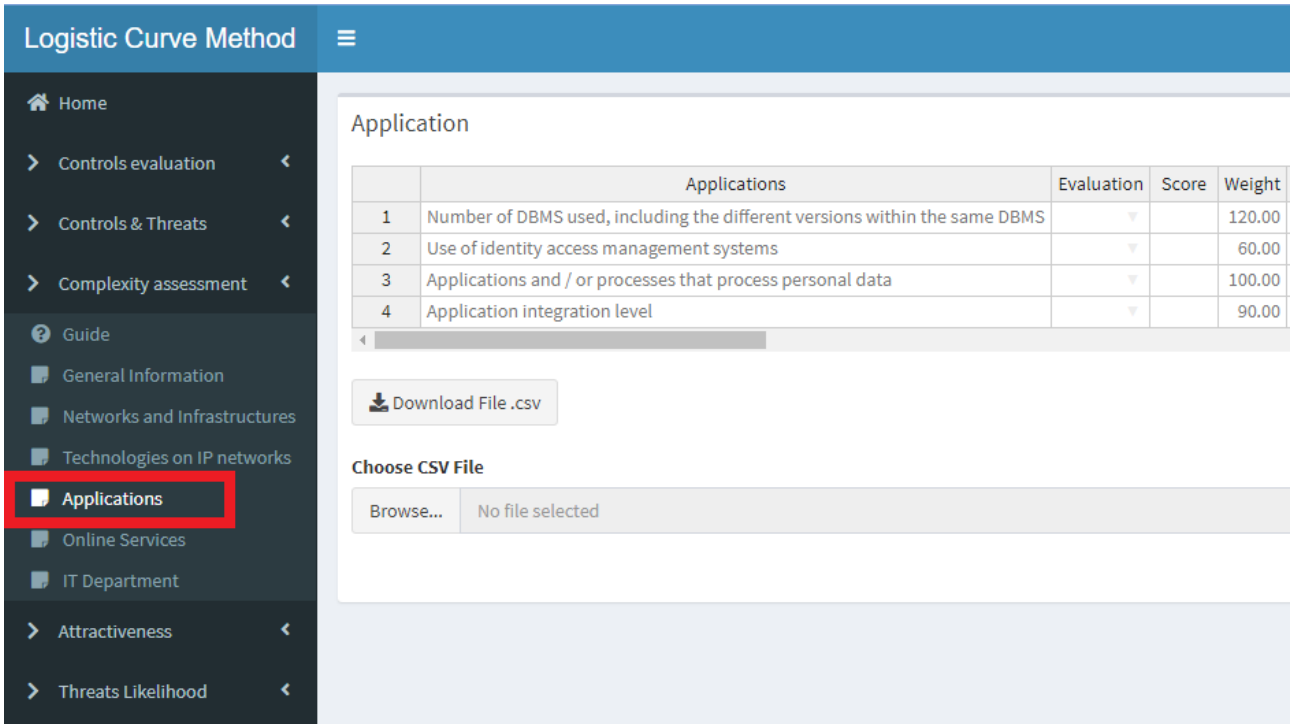


Figure 5.12. Complexity assessment section, sub-section "Applications".

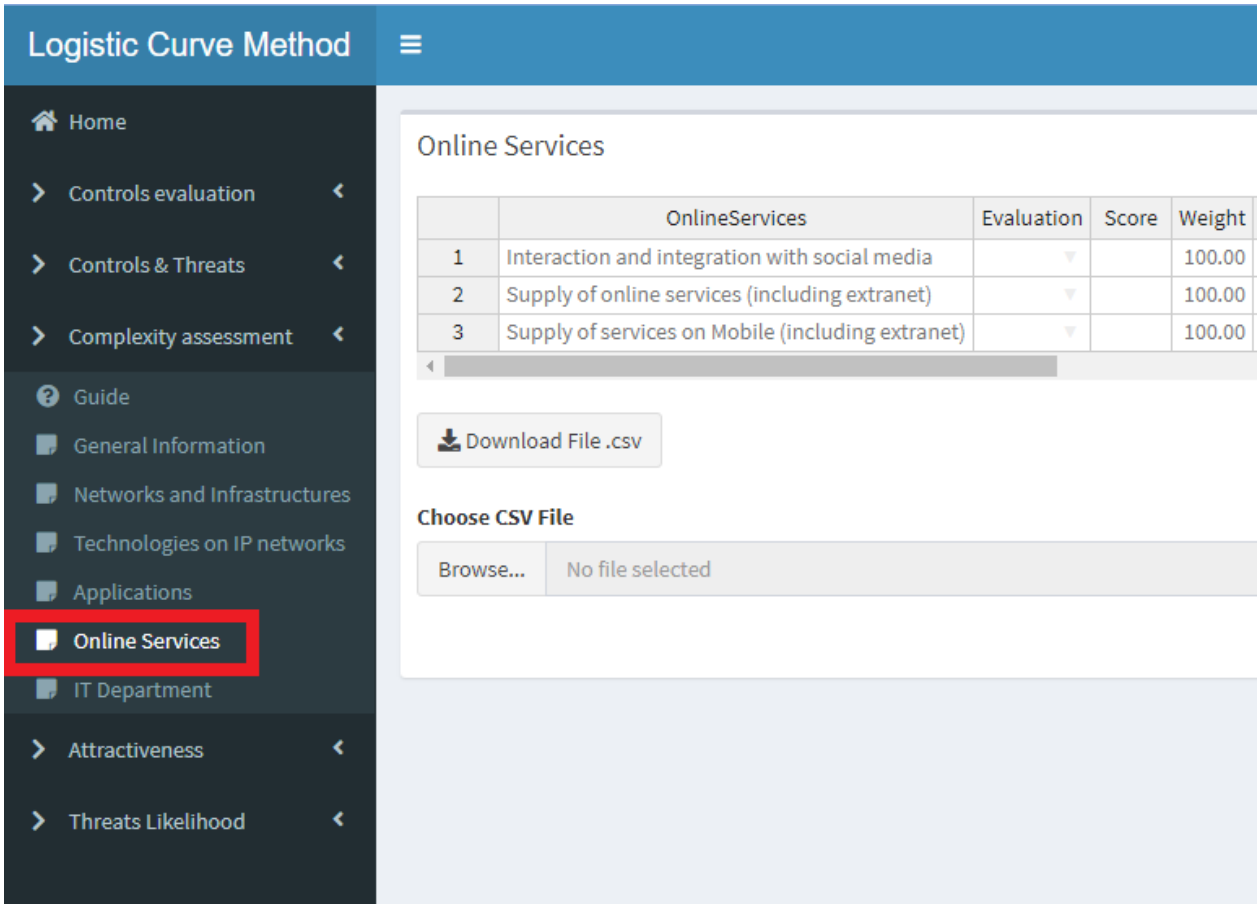


Figure 5.13. Complexity assessment section, sub-section "Online Services".

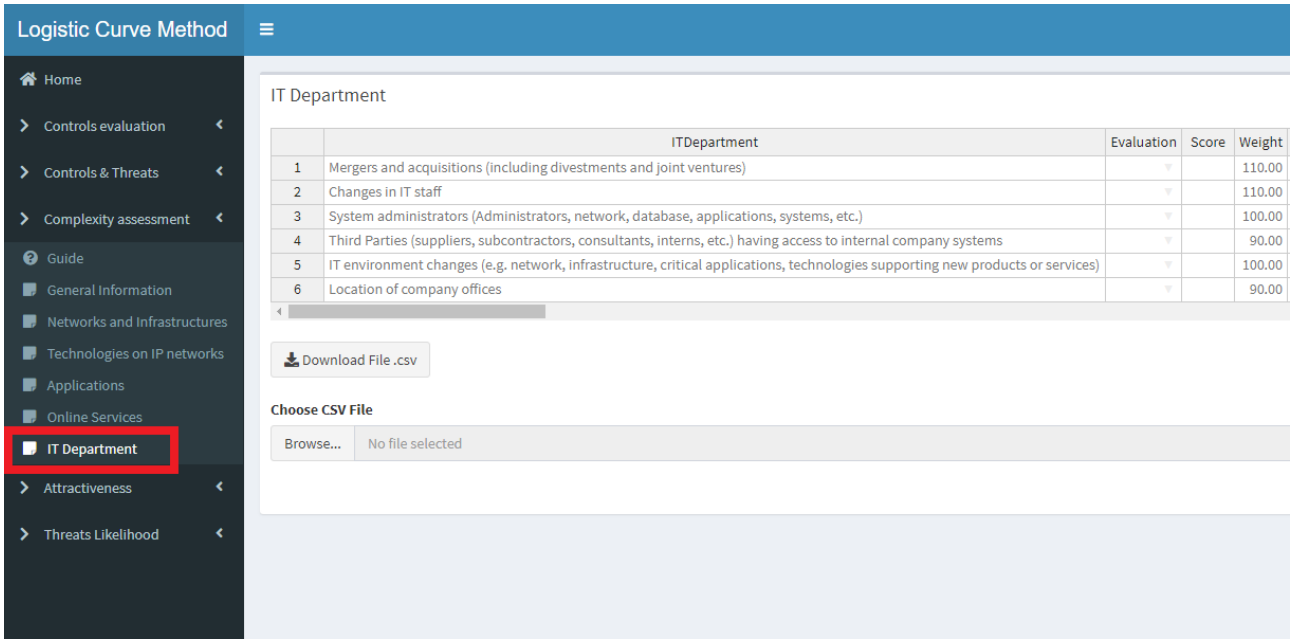


Figure 5.14. Complexity assessment section, sub-section "IT Department".

The sub-section "*Guide*" (Figure 5.8) acts as a support, as it provides guidelines on the meaning of the input data and how to insert them.

In the sub-section *"General Information"* (Figure 5.9) the required data must be entered manually, while in the following sub-sections, questions must be answered using a specific dropdown menu.

There are five selectable answers for each control: **Minimum**, **Low**, **Moderate**, **Significative**, **High** (in increasing complexity order). The choice of the answer is guided through the descriptions, shown in the columns on the right, of the attributed value, which can be selected from time to time using the drop-down menu. The descriptions of the five levels of complexity aim to make the measurement of complexity as objective as possible.

In order to obtain a numerical evaluation of the complexity, a score is associated with each answer:

- minimum → 1;
- low → 2;
- moderate → 3;
- significative → 4;
- high → 5.

Moreover, within each category, a **weight** is associated with each control; in this way, the score of the most important controls will have a greater impact on the final computation of the complexity.

For each sub-section, once the user entered the data it is possible to find two buttons below the tables (Figure 5.15.):

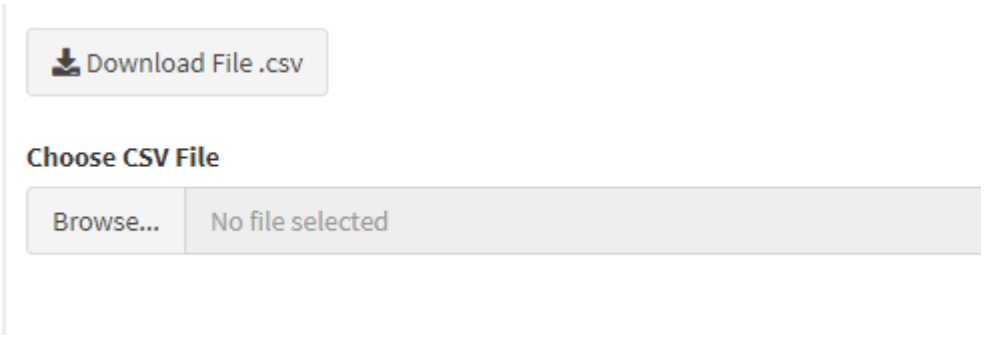


Figure 5.15. Download button (upper) and input button (lower).

- by pressing the ***"Download File.csv"*** button it is possible to download the data contained in the table in the form of a .csv file; this can be useful in case the user wants to save the table and use it for future analyses;
- the button ***"Choose CSV File"*** offers the possibility to directly load a .csv file that will automatically fill the table.

5.1.4 Attractiveness

The "Attractiveness" section is in turn divided into two sub-sections: "*Guide*" (Figure 5.16) and *"Attractiveness Evaluation"* (Figure 5.17).

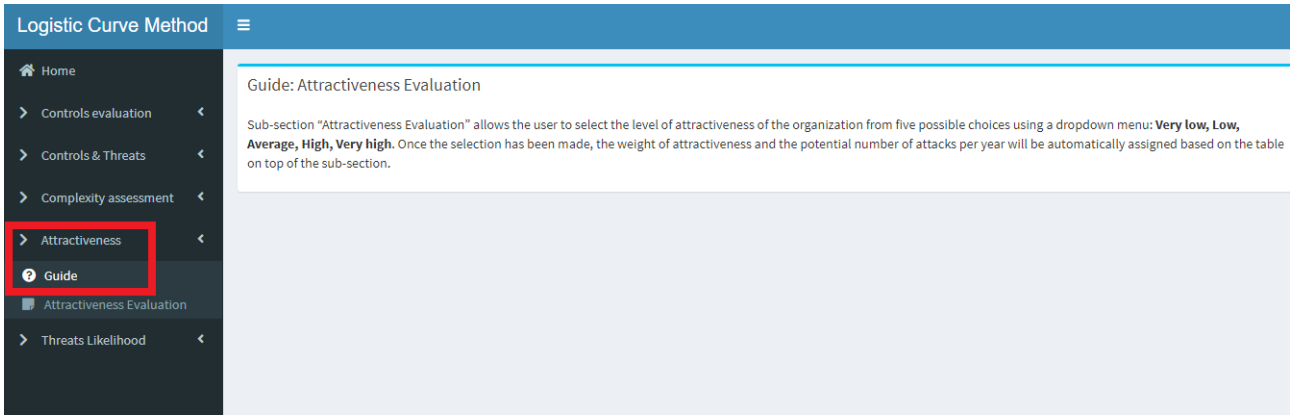


Figure 5.16. Attractiveness section, sub-section "Guide".

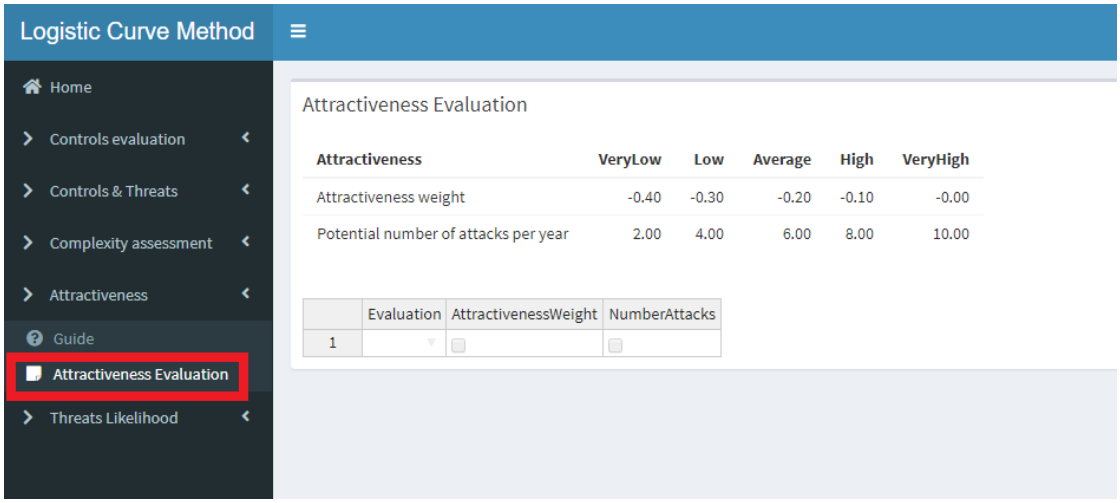


Figure 5.17. Attractiveness section, sub-section "Attractiveness Evaluation".

The sub-section "*Guide*" acts as a support, as it provides guidelines on the meaning of the input data and how to insert them.

Sub-section *"Attractiveness Evaluation"* allows the user to select the level of attractiveness of the organization from five possible choices using a dropdown menu: **Very low**, **Low**, **Average**, **High**, **Very high**. Once the selection has been made, the weight of attractiveness and the potential number of attacks per year will be automatically assigned based on the table on top of the sub-section (Figure 5.17).

5.1.5 Threats Likelihood

The "Threats Likelihood" section is in turn divided into two sub-sections: "*Guide*" (Figure 5.18) and *"CSV Threats Likelihood"* (Figure 5.19).

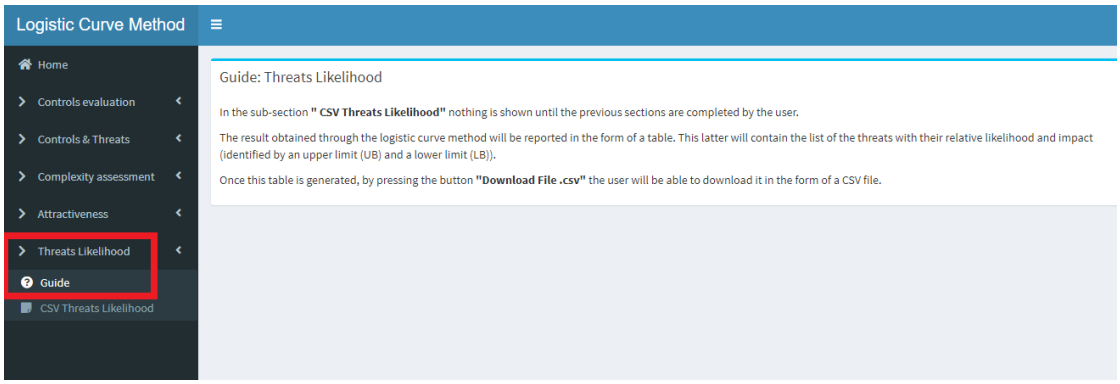


Figure 5.18. Threats Likelihood section, sub-section "Guide".

The sub-section "*Guide*" provides the user with indications on the output that will be shown in the following sub-section.

The sub-section "*CSV Threats Likelihood*" initially does not show any results (Figure 20):

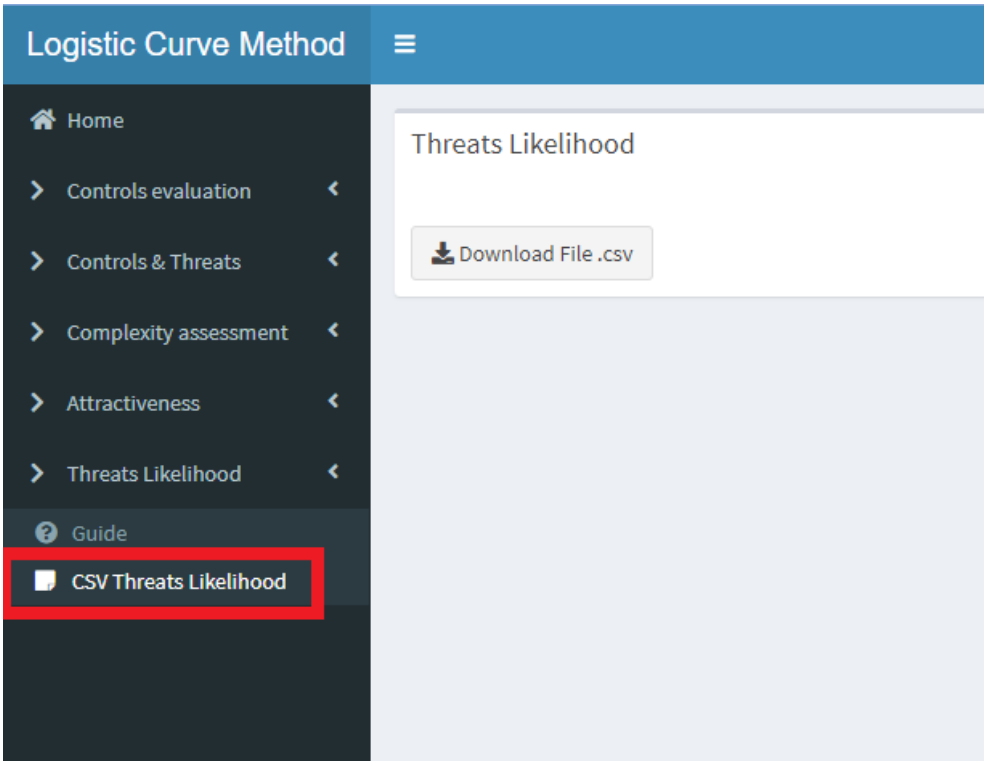
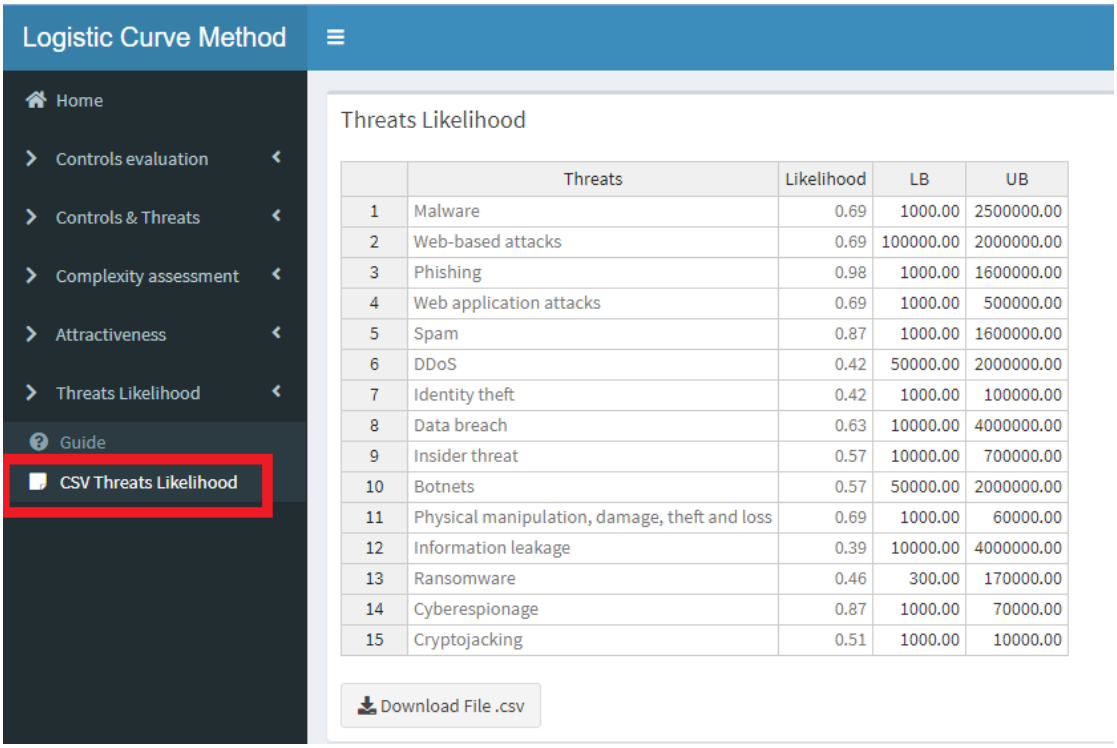


Figure 5.19. Threats Likelihood section, sub-section "CSV Threats Likelihood".

Once the user completes the data entry in all the previous sections, the likelihood is calculated through the Logistic Curve method using the maturity and complexity indices, and the attractiveness obtained from the previous sections. The results are shown in the form of a table (Figure 5.20):



	Threats	Likelihood	LB	UB
1	Malware	0.69	1000.00	2500000.00
2	Web-based attacks	0.69	100000.00	2000000.00
3	Phishing	0.98	1000.00	1600000.00
4	Web application attacks	0.69	1000.00	500000.00
5	Spam	0.87	1000.00	1600000.00
6	DDoS	0.42	50000.00	2000000.00
7	Identity theft	0.42	1000.00	100000.00
8	Data breach	0.63	10000.00	4000000.00
9	Insider threat	0.57	10000.00	700000.00
10	Botnets	0.57	50000.00	2000000.00
11	Physical manipulation, damage, theft and loss	0.69	1000.00	60000.00
12	Information leakage	0.39	10000.00	4000000.00
13	Ransomware	0.46	300.00	170000.00
14	Cyberespionage	0.87	1000.00	70000.00
15	Cryptojacking	0.51	1000.00	10000.00

Figure 5.20. Threats Likelihood section, sub-section "CSV Threats Likelihood": once the user completes all the previous sections the results (Likelihood assessment for each threat) are shown in this sub-section in the form of a table containing also the impact associated to each threat.

Impacts associated to each threat are already inserted in the table once it is generated, but it is possible to modify them according to the user's preferences. These values are entered as an example and can represent medium and large organizations.

By pressing the ***"Download File.csv"*** button below the table, it is possible to download the data contained in the table in the form of a .csv file (";" is used as separator).

6. Numerical results

In this section, few examples of how the web application works will be shown; in particular, it will be shown how the likelihood assessment changes according to the value of the complexity and maturity indices.

The **weights** that relate threats and controls are considered to be constant in all the shown cases (the table in the section “Controls & Threats” will not be modified); **attractiveness** too is kept constant, and it is set as “Average” for each case.

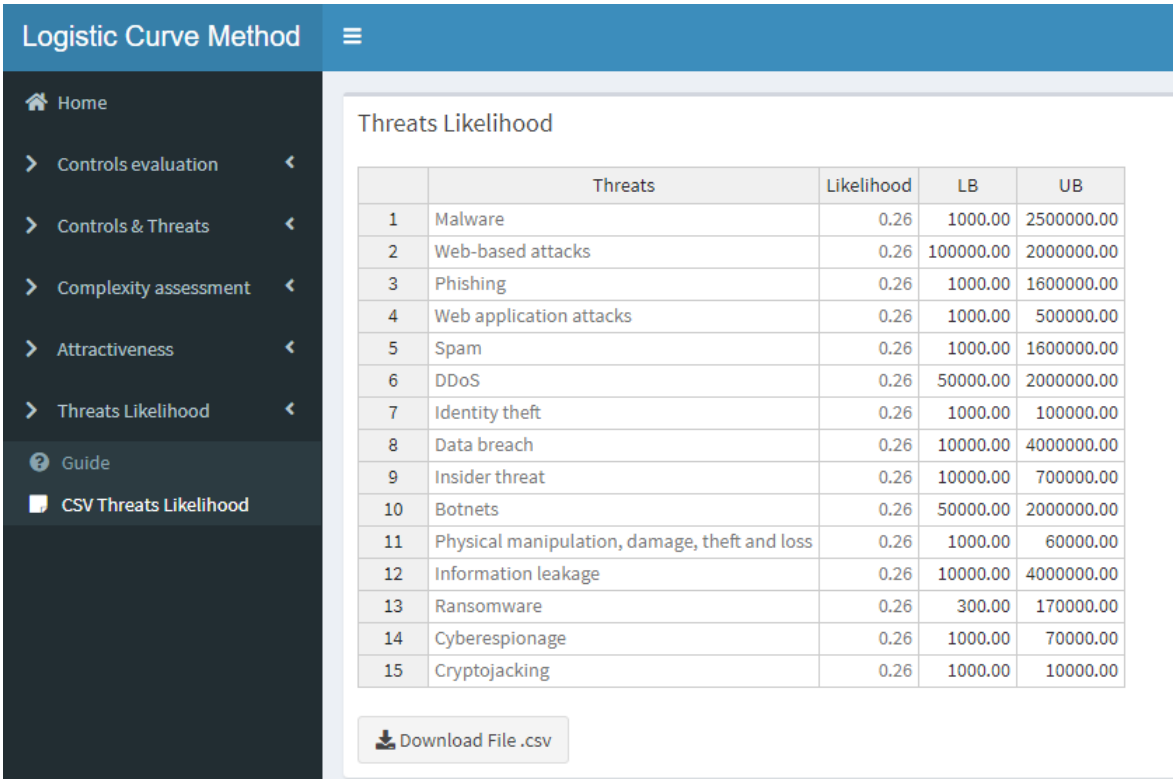
Once the likelihood evaluation has been completed, the CSV file containing the final table in the "Threats Likelihood" section has been downloaded and used as input for the qRisk application [5].

qRisk is a quantitative risk assessment tool, with cyber risk as its main focus. The tool comes in the form of a web application entirely developed in R language; it implements both the FAIR method and the HTMA method. The latter is what it will provide as input the CSV file downloaded from the web application proposed in this work.

6.1 Constant complexity and different maturity index

In this first case study, the complexity index was set equal to 5:

- if the **implementation assessment of each control is set equal to 1,** the results obtained for the likelihood assessment are reported in Figure 6.1.



	Threats	Likelihood	LB	UB
1	Malware	0.26	1000.00	2500000.00
2	Web-based attacks	0.26	100000.00	2000000.00
3	Phishing	0.26	1000.00	1600000.00
4	Web application attacks	0.26	1000.00	500000.00
5	Spam	0.26	1000.00	1600000.00
6	DDoS	0.26	50000.00	2000000.00
7	Identity theft	0.26	1000.00	100000.00
8	Data breach	0.26	10000.00	4000000.00
9	Insider threat	0.26	10000.00	700000.00
10	Botnets	0.26	50000.00	2000000.00
11	Physical manipulation, damage, theft and loss	0.26	1000.00	60000.00
12	Information leakage	0.26	10000.00	4000000.00
13	Ransomware	0.26	300.00	170000.00
14	Cyberespionage	0.26	1000.00	70000.00
15	Cryptojacking	0.26	1000.00	10000.00

Figure 6.1. Likelihood assessment obtained with complexity index equal to 5, "Average" attractiveness, and all controls equal to 1, i.e., implemented.

These results were then downloaded and used as input for the HTMA method on the web application qRisk.

The report containing the results obtained from qRisk shows the input for the Monte Carlo simulation (Figure 6.2), the set Risk Tolerance (Figure 6.2) and the Loss Exceedance Curve (LEC) of both the current analysis risk and Risk Tolerance. (Figure 6.3).

Table 1: Monte Carlo Simulation input (Risk List)

Event	Probability	LB 90% CI	UB 90% CI
Malware	0.26	€1,000	€2,500,000
Web-based attacks	0.26	€100,000	€2,000,000
Phishing	0.26	€1,000	€1,600,000
Web application attacks	0.26	€1,000	€500,000
Spam	0.26	€1,000	€1,600,000
DDoS	0.26	€50,000	€2,000,000
Identity theft	0.26	€1,000	€100,000
Data breach	0.26	€10,000	€4,000,000
Insider threat	0.26	€10,000	€700,000
Botnets	0.26	€50,000	€2,000,000
Physical manipulation, damage, theft and loss	0.26	€1,000	€60,000
Information leakage	0.26	€10,000	€4,000,000
Ransomware	0.26	€300	€170,000
Cyberespionage	0.26	€1,000	€70,000
Cryptojacking	0.26	€1,000	€10,000

Table 2: Risk Tolerance

Loss	Chance of Loss or Greater
€3,000,000	100%
€3,500,000	90%
€4,000,000	80%
€4,500,000	70%
€5,000,000	60%
€5,500,000	50%
€6,000,000	40%
€7,000,000	30%
€9,000,000	20%
€11,000,000	10%
€40,000,000	0%

Figure 6.2. Monte Carlo simulation input (upper table) and Risk Tolerance (lower table).

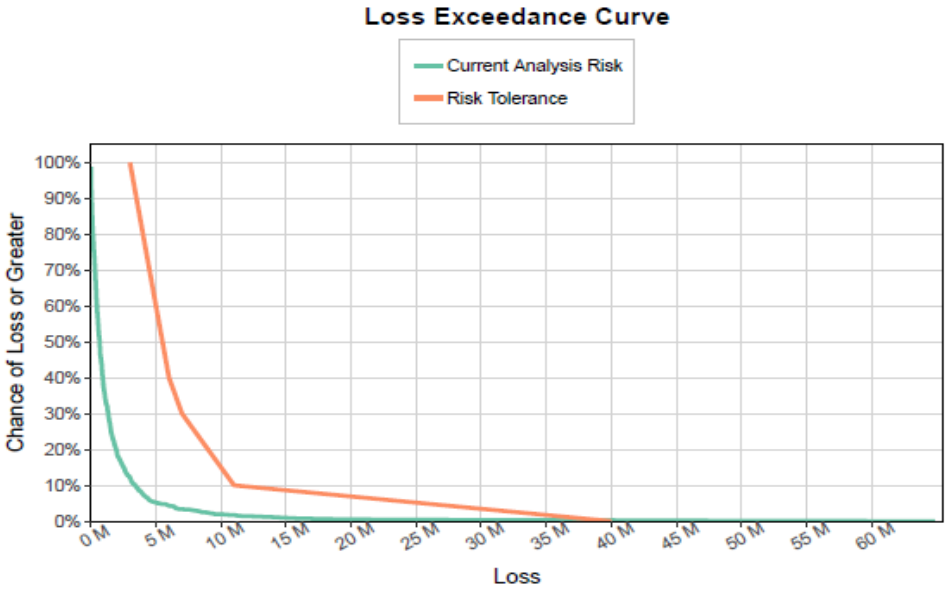
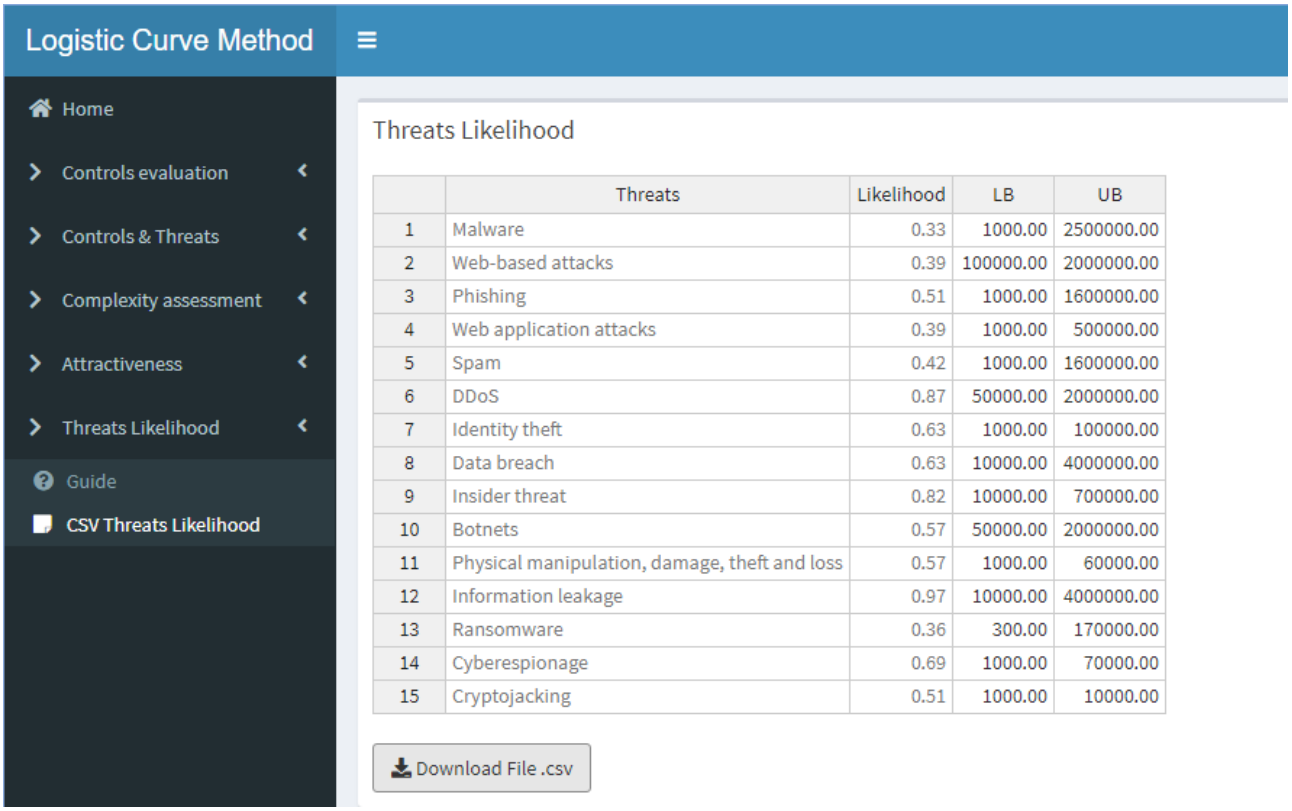


Figure 6.3. Loss Exceedance Curve (LEC) showing both the current analysis risk (green line) and the risk tolerance (orange line).

- If, on the other hand, the **maturity index decreases** (some controls may assume 0 or N/A as value, so not all the controls are implemented), it possible to notice that the likelihood assessment will show higher values, as shown in Figure 6.4.



	Threats	Likelihood	LB	UB
1	Malware	0.33	1000.00	2500000.00
2	Web-based attacks	0.39	100000.00	2000000.00
3	Phishing	0.51	1000.00	1600000.00
4	Web application attacks	0.39	1000.00	500000.00
5	Spam	0.42	1000.00	1600000.00
6	DDoS	0.87	50000.00	2000000.00
7	Identity theft	0.63	1000.00	100000.00
8	Data breach	0.63	10000.00	4000000.00
9	Insider threat	0.82	10000.00	700000.00
10	Botnets	0.57	50000.00	2000000.00
11	Physical manipulation, damage, theft and loss	0.57	1000.00	60000.00
12	Information leakage	0.97	10000.00	4000000.00
13	Ransomware	0.36	300.00	170000.00
14	Cyberespionage	0.69	1000.00	70000.00
15	Cryptojacking	0.51	1000.00	10000.00

Figure 6.4. Likelihood assessment obtained with complexity index equal to 5, "Average" attractiveness, and not all controls implemented (lower maturity index).

The report containing the results obtained from qRisk shows the input for the Monte Carlo simulation (Figure 6.5), the set Risk Tolerance (Figure 6.5) and the Loss Exceedance Curve (LEC) of both the current analysis risk and Risk Tolerance. (see Figure 6.6).

Table 1: Monte Carlo Simulation input (Risk List)

Event	Probability	LB 90% CI	UB 90% CI
Malware	0.33	€1,000	€2,500,000
Web-based attacks	0.39	€100,000	€2,000,000
Phishing	0.51	€1,000	€1,600,000
Web application attacks	0.39	€1,000	€500,000
Spam	0.42	€1,000	€1,600,000
DDoS	0.87	€50,000	€2,000,000
Identity theft	0.63	€1,000	€100,000
Data breach	0.63	€10,000	€4,000,000
Insider threat	0.82	€10,000	€700,000
Botnets	0.57	€50,000	€2,000,000
Physical manipulation, damage, theft and loss	0.57	€1,000	€60,000
Information leakage	0.97	€10,000	€4,000,000
Ransomware	0.36	€300	€170,000
Cyberespionage	0.69	€1,000	€70,000
Cryptojacking	0.51	€1,000	€10,000

Table 2: Risk Tolerance

Loss	Chance of Loss or Greater
€3,000,000	100%
€3,500,000	90%
€4,000,000	80%
€4,500,000	70%
€5,000,000	60%
€5,500,000	50%
€6,000,000	40%
€7,000,000	30%
€9,000,000	20%
€11,000,000	10%
€40,000,000	0%

Figure 6.5. Monte Carlo simulation input (top) and Risk Tolerance (bottom).

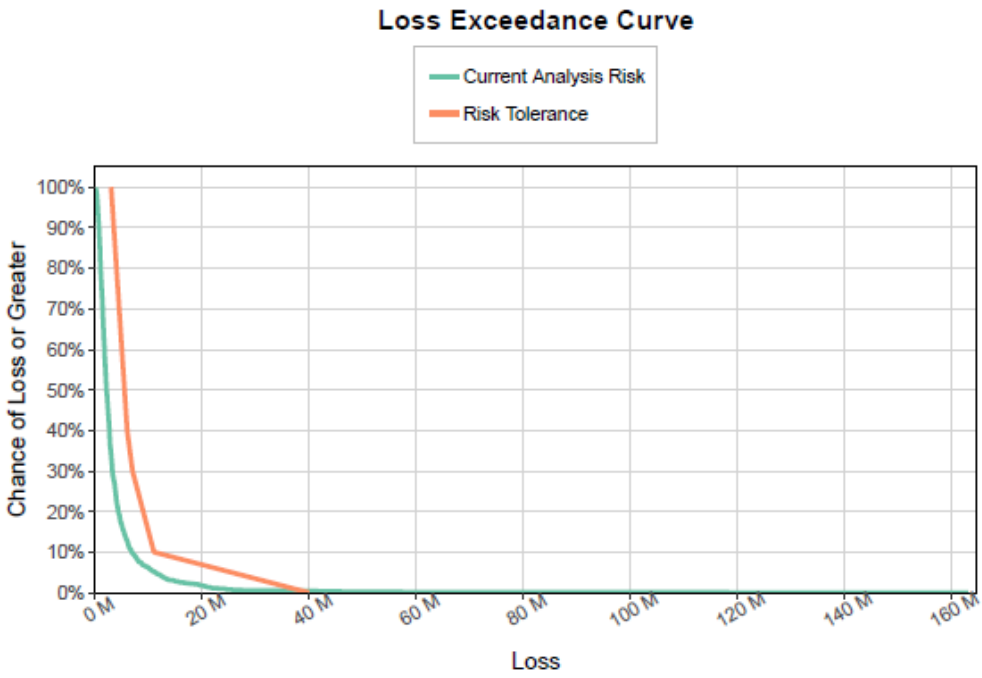


Figure 6.6. Loss Exceedance Curve (LEC) showing both the current analysis risk (green) and the risk tolerance (orange).

6.2 Constant maturity index and different complexity

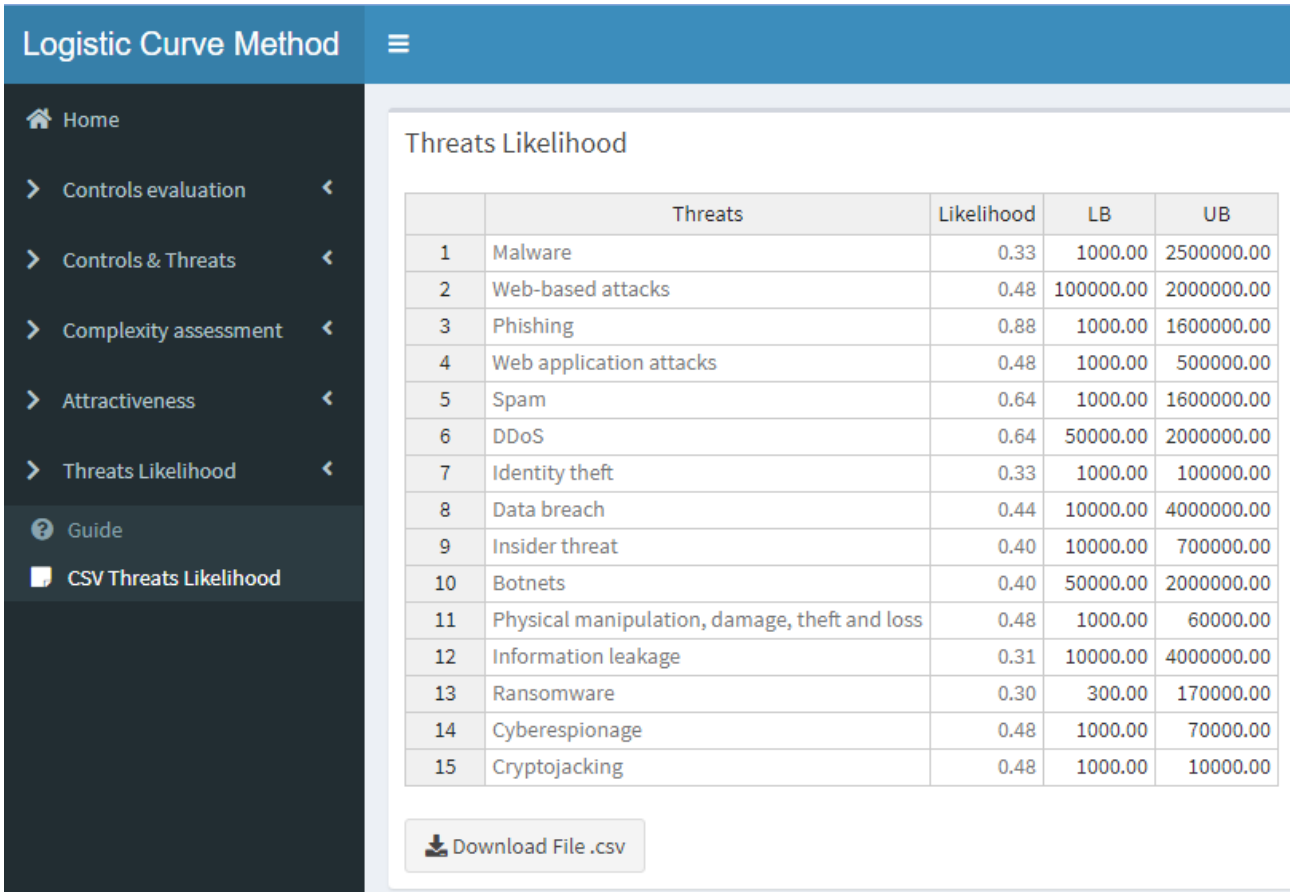
In this second example, the **maturity index is kept constant**, and the implementation of the controls used in this case is shown in Figure 6.7.

Controls Evaluation

	Controls	Evaluation
1	An inventory of systems, devices, software, services and IT applications in use within the company perimeter exists and is kept up to date	1
2	The web services (social networks, cloud computing, e-mail, web space, etc.) offered by third parties to which you have registered are those strictly necessary	
3	Critical information, data and systems for the company are identified so that they are adequately protected	1
4	It has been appointed a contact person who is responsible for coordinating the management and for the protection of information and IT systems	0
5	Laws and/or regulations with relevance in terms of cybersecurity that are applicable for the company are identified and respected	0
6	All devices that allow it are equipped with regularly updated protection software (antivirus, antimalware, etc ...)	1
7	Passwords are different for each account, of adequate complexity and the use of the most secure authentication systems offered by the service provider is evaluated (e.g. two-factor authentication)	1
8	Personnel authorized to access, remotely or locally, to the IT services have personal users that are not shared with others; access is suitably protected; old accounts that are no longer used are deactivated	1
9	Each user can only access the information and systems that he needs and/or is competent for	0
10	The staff is adequately sensitized and trained on the risks of cybersecurity and on the practices to be adopted for the safe use of company tools (eg. Recognize e-mail attachments, use only authorized software,...). The company's management takes care to prepare the necessary training for all company personnel to provide at least the basic notions of safety	1
11	The initial configuration of all systems and devices is carried out by expert personnel, responsible for their safe configuration. The default login credentials are always replaced	1
12	Backups of critical information and data for the company (identified in control 3) are periodically performed. Backups are stored securely and periodically verified	1
13	Networks and systems are protected from unauthorized access through specific tools (e.g. Firewall and other anti-intrusion devices/software)	1
14	In case of an incident (e.g. an attack or malware is detected) the security officers are informed and the systems are secured by expert personnel	1
15	All software in use (including firmware) are updated to the latest version recommended by the manufacturer. Obsolete and no longer updatable devices or software are disused	1

Figure 6.7. Control's implementation assessment used for this particular case study.

- If the **complexity index is set, for example, equal to 4**, the likelihood assessment obtained through the method implemented in the web application is shown in Figure 6.8.



	Threats	Likelihood	LB	UB
1	Malware	0.33	1000.00	2500000.00
2	Web-based attacks	0.48	100000.00	2000000.00
3	Phishing	0.88	1000.00	1600000.00
4	Web application attacks	0.48	1000.00	500000.00
5	Spam	0.64	1000.00	1600000.00
6	DDoS	0.64	50000.00	2000000.00
7	Identity theft	0.33	1000.00	100000.00
8	Data breach	0.44	10000.00	4000000.00
9	Insider threat	0.40	10000.00	700000.00
10	Botnets	0.40	50000.00	2000000.00
11	Physical manipulation, damage, theft and loss	0.48	1000.00	60000.00
12	Information leakage	0.31	10000.00	4000000.00
13	Ransomware	0.30	300.00	170000.00
14	Cyberespionage	0.48	1000.00	70000.00
15	Cryptojacking	0.48	1000.00	10000.00

Figure 6.8. Likelihood assessment obtained with complexity index equal to 4, "Average" attractiveness, and the controls implemented as shown in Figure 6.7.

The report containing the results obtained from qRisk shows the input for the Monte Carlo simulation (Figure 6.9), the set Risk Tolerance (Figure 6.9) and the Loss Exceedance Curve (LEC) of both the current analysis risk and Risk Tolerance. (Figure 6.10).

Table 1: Monte Carlo Simulation input (Risk List)

Event	Probability	LB 90% CI	UB 90% CI
Malware	0.33	€1,000	€2,500,000
Web-based attacks	0.48	€100,000	€2,000,000
Phishing	0.88	€1,000	€1,600,000
Web application attacks	0.48	€1,000	€500,000
Spam	0.64	€1,000	€1,600,000
DDoS	0.64	€50,000	€2,000,000
Identity theft	0.33	€1,000	€100,000
Data breach	0.44	€10,000	€4,000,000
Insider threat	0.40	€10,000	€700,000
Botnets	0.40	€50,000	€2,000,000
Physical manipulation, damage, theft and loss	0.48	€1,000	€60,000
Information leakage	0.31	€10,000	€4,000,000
Ransomware	0.30	€300	€170,000
Cyberespionage	0.48	€1,000	€70,000
Cryptojacking	0.48	€1,000	€10,000

Table 2: Risk Tolerance

Loss	Chance of Loss or Greater
€3,000,000	100%
€3,500,000	90%
€4,000,000	80%
€4,500,000	70%
€5,000,000	60%
€5,500,000	50%
€6,000,000	40%
€7,000,000	30%
€9,000,000	20%
€11,000,000	10%
€40,000,000	0%

Figure 6.9. Monte Carlo simulation input (top) and Risk Tolerance (bottom).

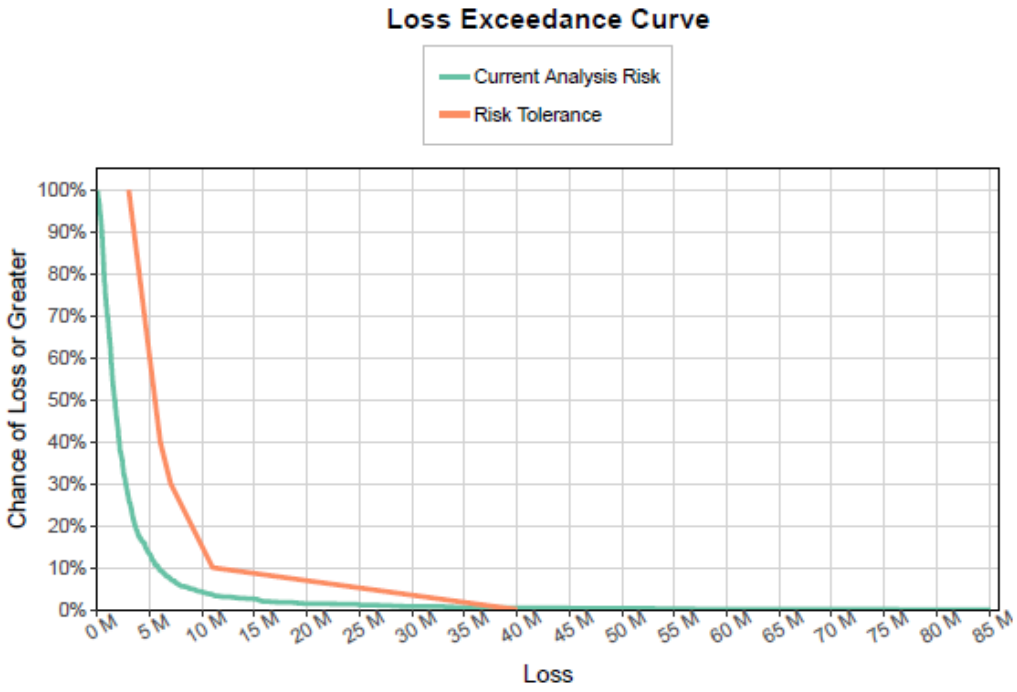
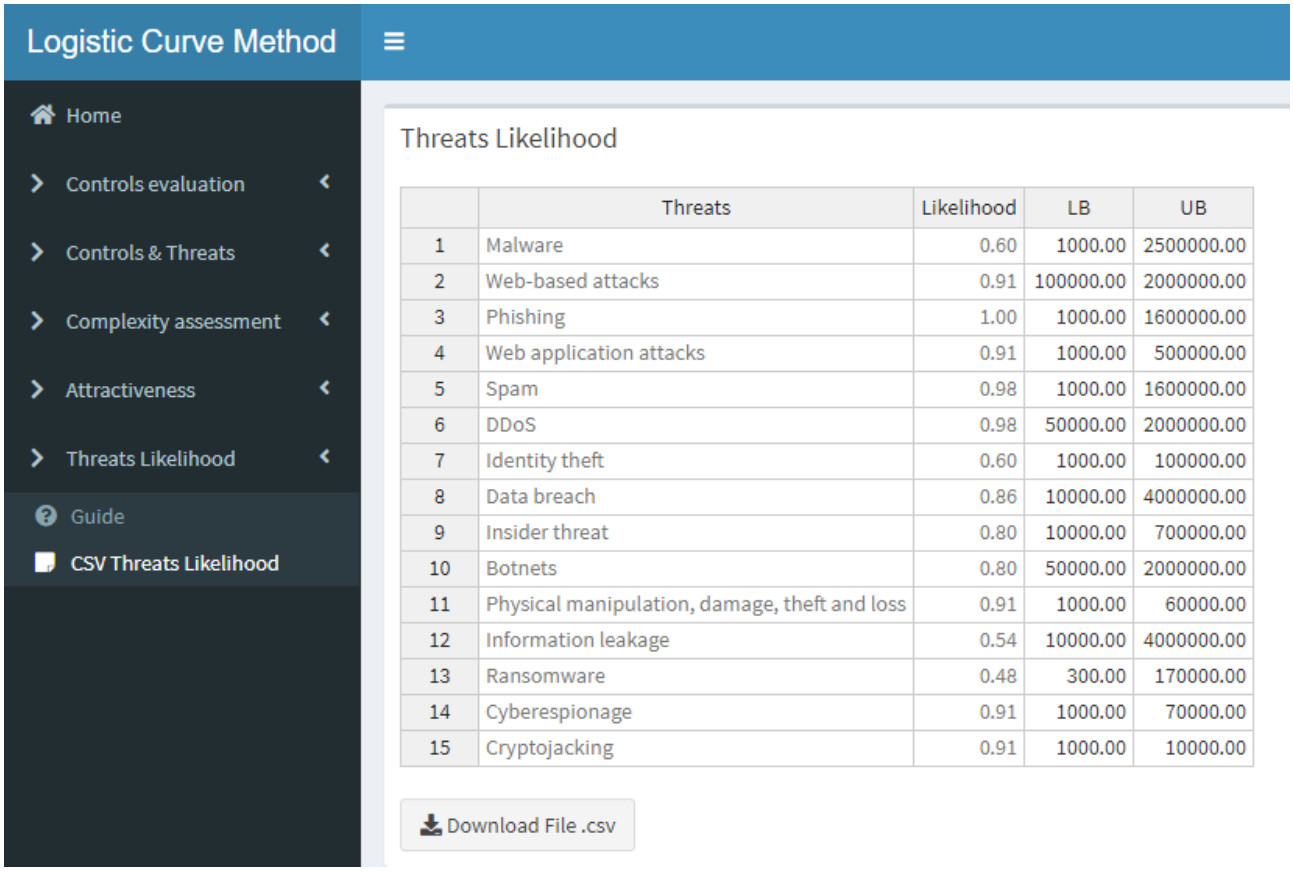


Figure 6.10. Loss Exceedance Curve (LEC) showing both the current analysis risk (green) and the risk tolerance (orange).

- If the **complexity index increases, in this case it is set equal to 6**, it is possible to notice an increase in the values shown in the likelihood assessment table (as shown in Figure 6.11).



	Threats	Likelihood	LB	UB
1	Malware	0.60	1000.00	2500000.00
2	Web-based attacks	0.91	100000.00	2000000.00
3	Phishing	1.00	1000.00	1600000.00
4	Web application attacks	0.91	1000.00	500000.00
5	Spam	0.98	1000.00	1600000.00
6	DDoS	0.98	50000.00	2000000.00
7	Identity theft	0.60	1000.00	100000.00
8	Data breach	0.86	10000.00	4000000.00
9	Insider threat	0.80	10000.00	700000.00
10	Botnets	0.80	50000.00	2000000.00
11	Physical manipulation, damage, theft and loss	0.91	1000.00	60000.00
12	Information leakage	0.54	10000.00	4000000.00
13	Ransomware	0.48	300.00	170000.00
14	Cyberespionage	0.91	1000.00	70000.00
15	Cryptojacking	0.91	1000.00	10000.00

Figure 6.11. Likelihood assessment obtained with complexity index equal to 6, "Average" attractiveness, and the controls implemented as shown in Figure 6.7.

The report containing the results obtained from qRisk shows the input for the Monte Carlo simulation (Figure 6.12), the set Risk Tolerance (Figure 6.12) and the Loss Exceedance Curve (LEC) of both the current analysis risk and Risk Tolerance. (Figure 6.13).

Table 1: Monte Carlo Simulation input (Risk List)

Event	Probability	LB 90% CI	UB 90% CI
Malware	0.60	€1,000	€2,500,000
Web-based attacks	0.91	€10,000	€2,000,000
Phishing	1.00	€1,000	€1,600,000
Web application attacks	0.91	€1,000	€500,000
Spam	0.98	€1,000	€1,600,000
DDoS	0.98	€50,000	€2,000,000
Identity theft	0.60	€1,000	€100,000
Data breach	0.86	€10,000	€4,000,000
Insider threat	0.80	€10,000	€700,000
Botnets	0.80	€50,000	€2,000,000
Physical manipulation, damage, theft and loss	0.91	€1,000	€60,000
Information leakage	0.54	€10,000	€4,000,000
Ransomware	0.48	€300	€170,000
Cyberespionage	0.91	€1,000	€70,000
Cryptojacking	0.91	€1,000	€10,000

Table 2: Risk Tolerance

Loss	Chance of Loss or Greater
€3,000,000	100%
€3,500,000	90%
€4,000,000	80%
€4,500,000	70%
€5,000,000	60%
€5,500,000	50%
€6,000,000	40%
€7,000,000	30%
€9,000,000	20%
€11,000,000	10%
€40,000,000	0%

Figure 6.12. Monte Carlo simulation input (top) and Risk Tolerance (bottom).

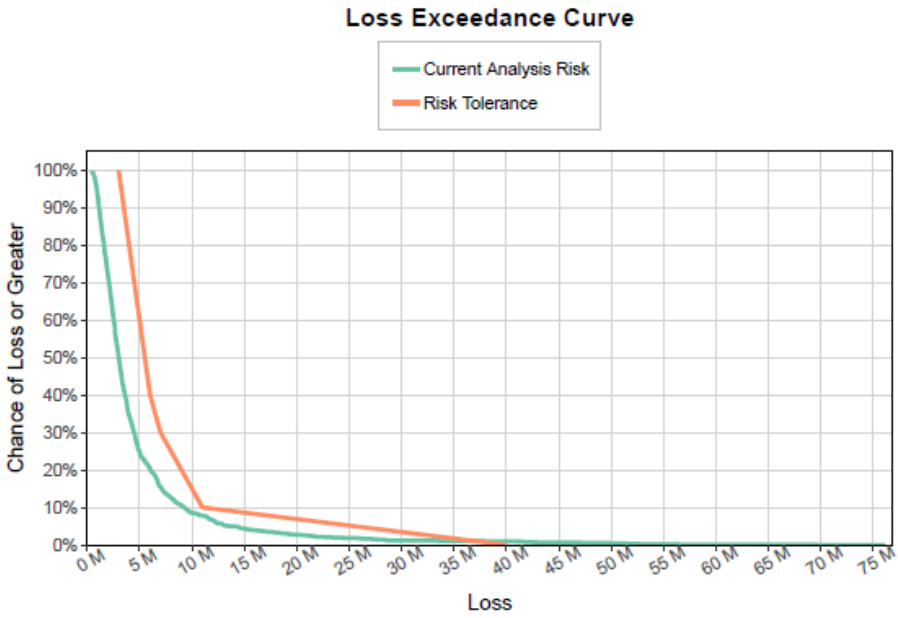


Figure 6.13. Loss Exceedance Curve (LEC) showing both the current analysis risk (green) and the risk tolerance (orange).

7. Conclusions

Some quantitative cyber risk assessment methods, as HTMA and FAIR methods, are based on past data to assess the probability of occurrence of an event, in particular the probability of a cyber-attack due to a certain threat. Even when this historic exists, it does not always consider the company's cyber posture; therefore the probability assessment is applied to a company that is potentially different from the one on which the history is based.

The model proposed in this work aims to combine the so-called scoring methods for cyber risk assessment and the so-called statistical cyber risk assessment methods, in particular the HTMA method, through the use of the Logistic Curve Method.

The model has been implemented in an interactive web application developed entirely in R; once the various sections of the application have been completed, it allows the user to obtain an objective assessment (through a scoring system) of the likelihood of occurrence for each of the 15 most frequent cyber threats.

The final result also reports the impacts, in terms of economic loss, associated with the different types of threats, but these are provided only as an example and can represent the situation for medium or large companies.

The web application also offers the possibility to download the results in the form of a CSV file; for example, this could be very useful, as shown in Chapter 6, to use the obtained data as an input for the HTMA method implemented in the qRisk application.

The case studies, reported in chapter 6, show how the application works properly: as expected, for an increase in the complexity index of the organization under exam there is also an increase in the likelihood of suffering a cyber-attack. On the other hand, when there is an increase in the maturity index, it is possible to notice a decrease in the likelihood assessment due to a higher level of security of the organization.

Bibliography

[1] S. Taubenberger, J. Jürjens, Y. Yu e B. Nuseibeh, "*Problem Analysis of Traditional IT - Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing domain*"; *Future Challenges in Security and Privacy for Academia and Industry. SEC 2011. IFIP Advances in Information and Communication Technology*; vol. 354; Camenisch J. and Fischer-Hübner S. and Murayama Y. and Portmann A. and Rieder C..

[2] National Institute of Standards and Technology (NIST); "*Special Publication 800-30 Revision 1 - Information Security".*

[3] Information System Audit and Control Association (ISACA); "*COBIT 2019* (*Control Objectives for Information and related Technology*)".

[4] D. Hubbard e R. Seiersen; "*How to Measure Anything in Cybersecurity Risk*"; Wiley; 2016.

[5] J. Freund e J. Jones; "*Measuring and Managing Information Risk: A FAIR Approach*"; Butterworth-Heinemann; 2015.

[6] CIS-Sapienza (Cyber Intelligence and Information Security); "*Controlli Essenziali di Cybersecurity"*; 2016 Italian Cybersecurity Report.

[7] Christopher Z. Mooney; "*Monte Carlo Simulation*"; 1997.

[8] ENISA (European Union Agency for Cybersecurity); "*List of top 15 threats from January 2019 to April 2020*".

[9] Center for Internet Security; "*CIS Controls";* April 2019; V7.1

[10] European Union Agency For Network and Information Security (ENISA); "*Handbook on Security of Personal Data Processing";* 2017.

[11] ISO/IEC 27001:2013; "*Information technology – Security techniques – Information security management systems – Requirements".*

[12] ISO/IEC 27001:2013; "*Information technology – Security techniques – Code of practice for information security controls".*

[13] CIS-Sapienza, Research Center of Cyber Intelligence and Information Security, Sapienza Università di Roma; CINI Cybersecurity National Lab, Consorzio Interuniversitario Nazionale per l'informatica; "*Framework Nazionale per la Cybersecurity e la Data Protection*"; February 2019; Version 2.0.

[14] P. Santini, G. Gottardi, M. Baldi, F. Chiaraluce; "*A Data-Driven Approach to Cyber Risk Assessment"*; Hindawi, Security and Communication Networks; September 2019.

[15] S. Cecchini, L. Gianvittorio, V. Sabatini; "*qRisk Assesment*"; https://cegisa.shinyapps.io/qrisk-mix/.