

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

CYBECO

Supporting Cyber-insurance from a Behavioural Choice Perspective

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Due date: M18

Abstract:

This report describes the methodology & design principles of the CYBECO Toolbox. It encompasses business requirements and constraints, integration requirements, preliminary solution specifications and planning of prototype tool development.

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Document Status

Document Title	Description Methodology & Design Principles of the CYBECO Toolbox
Version	1.0
Work Package	5
Deliverable #	5.1
Prepared by	INTRASOFT and CSIC-ICMAT
Contributors	Vassilis Chatzigiannakis, George Koutalieris, Sofia Tsekeridou, Aitor Couce Vieira, David Rios Insua
Checked by	
Approved by	
Date	
Confidentiality	PU

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
First draft (INTRASOFT)	0.1	Jan 12, 2018
Incorporated comments from WP3	0.2	Jan 30, 2018
Incorporated comments from WP4	0.3	February 27, 2018
Introduction updated, and new user journeys have been added to section 2.2	0.4	June 15, 2018
KB hierarchy table updated based on expert feedback from WP4	0.5	Sept 20, 2018
Section 2.5 has been updated with the new risk analysis input parameters	0.6	Sept 25, 2018
Added implementation details	0.7	Oct 1, 2018
Added new wireframes and Conclusions	0.8	Oct 15, 2018
Incorporated comments from WP3 and added latest version of wireframes	0.9	Oct 26, 2018

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Table of Contents

1	Introduction	7
1.1	Principle: A toolbox that handles three ways of resolving a Risk Analysis Template 9	
2	Design and Architecture of CYBECO Toolbox	11
2.1	Users - Roles	11
2.2	User journeys	11
2.3	KB Design.....	13
2.3.1	KB Entities	14
2.4	Risk Analysis Module	15
2.4.1	KB-RAT: use and elements	17
2.4.2	C-RAT.....	18
2.4.3	R-RAT.....	20
2.5	Risk Analysis Templates Input/Output	22
2.5.1	Input Description	22
2.5.2	Input options	24
2.5.2.1	Organisation profile	24
2.5.2.2	Assets	25
2.5.2.3	Other organisational features.....	27
2.5.2.4	Environmental threats	27
2.5.2.5	Non-targeted cyber attacks	28
2.5.2.6	Attackers	28
2.5.2.7	Targeted cyber attacks	29
2.5.2.8	Technical Security controls.....	30
2.5.2.9	Procedural controls.....	33
2.5.2.10	Physical controls	36
2.5.2.11	Insurance products - Coverage	37

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2.12	Security controls and insurance constraints.....	40
2.5.3	Output Description	41
2.6	Security Considerations	44
2.7	Implementation	44
2.7.1	Technologies	44
2.7.2	Risk analysis module	46
2.7.3	KB Module	49
3	Conclusions.....	50
4	Acronyms and Abbreviations.....	51
5	Appendix: CYBECO Toolbox v2 Wireframes.....	52

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

List of Figures

Figure 1: The CYBECO TOOLBOX.....	8
Figure 2: RISK ANALYSIS MODULE.....	16
Figure 3: Dataflow diagram of KB-RAT	18
Figure 4: C-RAT dataflow diagram	19
Figure 5: R-RAT dataflow diagram	21
Figure 6: R Server communication with R Workers	48
Figure 7: Home Page	52
Figure 8: Case selection	52
Figure 9: Organisation profile selection	53
Figure 10: Assets selection	53
Figure 11: Other features selection.....	54
Figure 12: Environmental/Non-targeted threats selection	54
Figure 13: Attacker/Cyber-attacks selection	55
Figure 14: Technical security controls selection	55
Figure 15: Procedural controls selection	56
Figure 16: Physical controls selection	56
Figure 17: Insurance coverage selection	57
Figure 18: Insurance constraints selection	57
Figure 19: Risk analysis results	58
Figure 20: Risk analysis results product details	58
Figure 21: Results comparison	59
Figure 22: Analysis in progress screen	59
Figure 23: Demo risk analysis modules	60
Figure 24: Risk analysis history	60

1 Introduction

Based on the outcomes of the other CYBECO work packages, the main objective and outcome of WP5 is the development of the information toolbox (CYBECO Toolbox 2.0).

The key idea here is to enable cyber insurance clients and insurance companies, research actors, policy makers and market stakeholders, not only to obtain easy access to information on relevant concepts of cyber insurance and the evaluation of the proposed models and experiments, but also to provide them with a framework of analysis and assessment of the preferred cybersecurity and cyber insurance choices regarding their specific needs and enquiries. To that end, the Toolbox will provide a set of Risk Analysis Templates, designed by WP3 and based on the use cases, scenarios, input and experience from WP4. These CYBECO “Risk Analysis Templates” (RAT) will model aspects researched by WP6 and WP7.

The CYBECO Toolbox is a web application that comprises two main modules:

- A Knowledge Base (KB) with cybersecurity and cyber insurance related content. The KB contains hierarchical taxonomies of entities such as cyber-insurance use cases and scenarios (provided by WP4), threats and security controls. All these entities in the KB are interconnected; for example, a cyber-insurance scenario may include several threats and security controls.
- A Risk Analysis System that provides users with the means to search and test and experiment with a set of Risk Analysis Templates.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

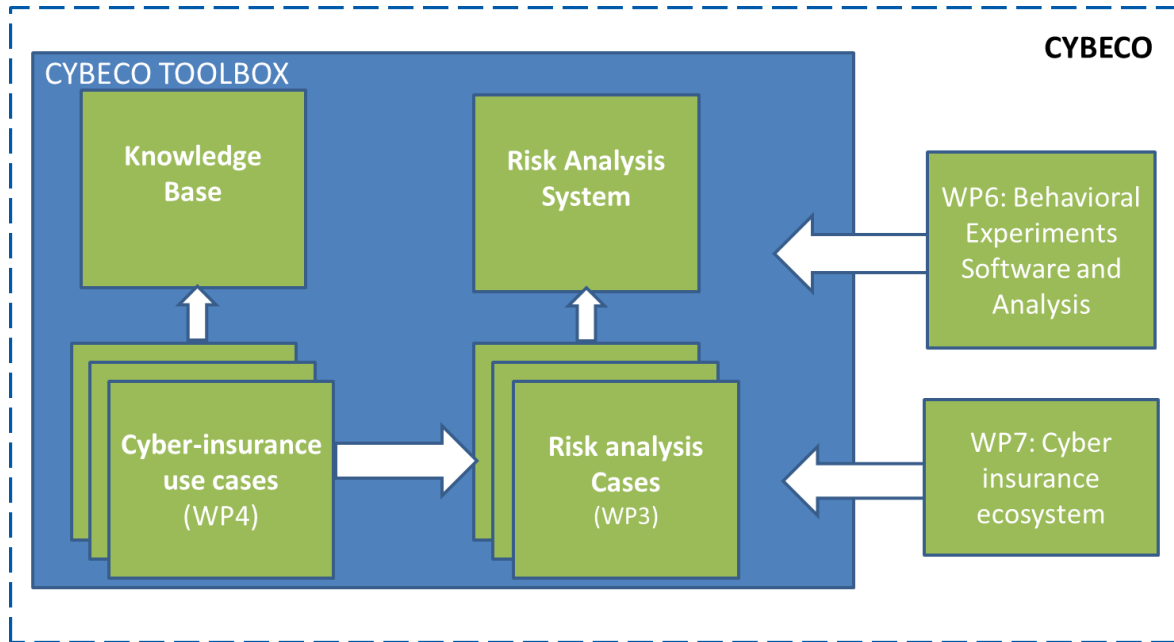


Figure 1: The CYBECO TOOLBOX

The following Risk RATs were planned for the first version of the Toolbox (CYBECO Toolbox 1.0):

- Risk Analysis for an SME: models a single SME facing cybersecurity risks. It is from the perspective of the SME decision-making, aiding it to choose the optimal cyber security portfolio and cyber insurance product. This is a simplified version of the risk analysis module that presents a specific case of an SME with predefined parameters.
- Risk analysis for an SME (insurance company perspective): The second RAT is from the perspective of the insurer; specifically, the decision on whether to insure a particular SME or not.

For the second version of the Toolbox (CYBECO Toolbox 2.0) a new RAT will be implemented.

- Generic Risk analysis: The stakeholders of this template are SMEs or large companies, and the goal is to choose the optimal cyber security portfolio and cyber insurance product. The new RAT will let the user define many parameters of the problem (such as type of company, cost of facilities, details about the market share, the threats and the security controls). The inputs are presented in detail in section 2.5.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

1.1 Principle: A toolbox that handles three ways of resolving a Risk Analysis Template

From the software implementation point of view, we have different alternatives for the processing and resolution of various Risk Analysis Templates. Specifically, we have the following three types of Risk Analysis Templates (detailed in sections 2.4.1 -2.4.3):

1. **Knowledge Base Risk Analysis Template (KB-RAT):** The Template options and results are stored in the KB. The source of the information for these templates are the use cases and scenarios provided by WP4.
2. **Calculation-based Risk Analysis Template (C-RAT):** The Template options, and some of its results, are stored in the KB, other results are calculated in a different module.
3. **R-based Risk Analysis Template (R-RAT):** The Template options are stored in the KB, but the calculation is done in a locally installed R¹ server that will run a simulation and send back the results.

The goal is to come up with (1) a verifiable scientific model but also with a model that is (2) relevant and pertinent to cyber insurance parties and (3) easy to use and interpret. The first point is mostly an outcome of the scientific WPs and use case interaction, but it also means that that outcome must be translated into the model residing in the Toolbox. The second point means that the Toolbox should be able to capture user input. The third point means (a) that user input must be something that they can infer from their knowledge and data available and (b) that the problem-solving time is acceptable regarding the complexity of the risk assessment.

The goal is to create a system that provides reliable results and that can be used by non-experts. This means translating the WP3 models into a system of algorithms to be implemented in a “*Calculation Module*” in the Toolbox that provides a faster and simpler risk assessment process. This is what we defined as the *C-RAT*. This *Template* would require storing certain simulation results in the database to be used by the *Calculation Module*.

¹ R is a programming language and environment for statistical computing and the development of data analysis applications <https://www.r-project.org/about.html>

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

However, we will also define generic RATs that do not need any calculation at all in the Toolbox. Their results are stored in the KB and, therefore, are defined as *KB-RATs*. This type will not add any complication to the Toolbox, since they do not make usage of the *Calculation Module*. Indeed, the KB-RATs may be interesting for cases in which the user input is simple but we have many users (i.e., less calculation in the *Calculation Module* and more queries in the database). Additionally, we will define RATs for performing risk analysis with the support of an R server (simulation on demand), to provide more detailed and powerful calculations. These are defined as *R-RATs* and allow users to implement a data analysis lab for risk analysis.

There are three analysis templates currently designed in the Toolbox:

- Risk Analysis for an SME: K-RAT
- Risk analysis for an SME (insurance company perspective): KB-RAT
- Generic Risk analysis: R-RAT.

2 Design and Architecture of CYBECO Toolbox

2.1 Users - Roles

Types of users:

- Anonymous users: Anonymous users have access only to a welcome page with information about the Toolbox and how to register to the Toolbox.
- Authenticated users: Registered users may use the Toolbox. Registered users may be experts, researchers, SME owners or any other type of stakeholder.
 - Editors: Role given to specific registered users with permission to edit the knowledge base.
 - Admin: Administrator of the web site.

Registration mode (there are two options):

- Free registration: Any anonymous user may register and use the Toolbox
- Registered users must be activated by admin

2.2 User journeys

A user journey is a series of steps that represent a scenario in which a user might interact with the application.

ID	Title	Description
1	New user lands on the Toolbox homepage	A new user lands on the Toolbox. The user has access only to the main/welcome page. The user is informed about the Toolbox and decides whether to register or not and use the Toolbox.
2	User registration	An anonymous user registers in order to use the Toolbox. For the registration, email verification is required. Optionally, registered users must be

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

activated by the administrator. The site also offers password recovery.

3	KB browsing	From the main page or using the main menu, the user may navigate to the KB and start browsing the taxonomy of various entities (threats, security controls, risk terms, etc.). For example, for every threat, there is a page describing the threat that also contains links to siblings, parent category and children categories/threats.
4	KB search	The user may enter a term in the search box with Autocomplete functionality. The Autocomplete provides suggestions while the user types into the search field. If the user hits the search button, they are redirected to a search results page. The search results may be divided into entity types and are sorted by relevance.
5	Risk Analysis Template selection	<p>The user navigates to the risk analysis module and selects a type of RAT. This selection may be done also in the first page.</p> <p>Because the tool is intended to be used by various stakeholders with different background (e.g. researchers, SME owners, large company security officers), a wizard will help the user select the correct RAT in an interactive way.</p>
6	RAT - Data input	The user enters inputs in a multi-step guided form. The steps are divided in categories such as Company info and assets, relevant threats, risk mitigation, etc. In case the risk analysis template requires simulation, the user is redirected to a page showing the progress of the simulation.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

7	RAT - Results	<p>When the simulation ends, the user is informed by email. The output may contain free text, tables and graphs describing parameters such as the probability of different events and economic functions.</p> <p>The results are divided in different options (selections of security measures and insurance coverages) ordered by ranking</p> <p>The user can also:</p> <ul style="list-style-type: none">• Compare results between different options• Export results to pdf
8	Risk analysis - Previous Analyses	<p>The user can view a list of previous risk analyses and select one to see the results</p>
9	Contact Form	<p>The registered user may complete a contact form for asking a question or offering a suggestion for the Toolbox</p>
10	KB editor	<p>Registered users who are given the “KB editor” role may edit the knowledge base. They may add/edit/delete entities such as threats, security controls and Risk Analysis Templates.</p>
11	User account deletion	<p>User account can be deleted upon user request by the administrator. User can also delete their account themselves.</p>

2.3 KB Design

The KB contains hierarchical taxonomies of entities such as the items of the Risk Analysis Template and a knowledge base with information about relevant cybersecurity elements such as threats or security controls. All these entities in the KB are interconnected.

More information on the KB can be found in Deliverable D5.2: CYBECO content and data collection manual which was submitted at M14.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.3.1 KB Entities

Since the submission of D5.2, the hierarchy of KB entities has been re-arranged. The new hierarchy is depicted in the following table based on expert feedback from WP4.

Category of entities	Entity	Parameters of entity
RISK	Risk term	<ul style="list-style-type: none"> Term Definition
ORGANISATION	Assets	<ul style="list-style-type: none"> Name Description
	Sector	<ul style="list-style-type: none"> Name Description
DIGITAL SYSTEM	System Assets	<ul style="list-style-type: none"> Name Description
	Vulnerabilities/Weaknesses	<ul style="list-style-type: none"> Name Description
THREAT	Threat actor	<ul style="list-style-type: none"> Threat actor type Threat actor role Threat actor sophistication Threat actor motivation Threat actor resources
	Threat action	<ul style="list-style-type: none"> Name Description
	Cyberattack pattern	<ul style="list-style-type: none"> Name Description
	Indicators of cyberattacks	<ul style="list-style-type: none"> Name Description

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

	Malware	<ul style="list-style-type: none"> • Name • Description
IMPACTS	Impacts	<ul style="list-style-type: none"> • Name • Description
RISK	Risk term	<ul style="list-style-type: none"> • Term • Definition
SECURITY ACTIONS	Security control	<ul style="list-style-type: none"> • Name • Description
	Cyber insurance	<ul style="list-style-type: none"> • Name • Description

The database with the items of the Risk Analysis Template will contain the parameters described in Section 2.6. Additionally, these parameters would be linked to their correspondent KB items of the previous table.

2.4 Risk Analysis Module

The Risk analysis module comprises two main subsystems:

- Risk Analysis System that handles the interaction with the user and the resolution of KB-RATs and C-RATs.
- R-Server for Risk Analysis that handles the simulation of R-RATs.

The *Risk Analysis Module* has the following components:

- *Graphical User Interface* to interact with the user. It has the following subcomponents:
 - Risk Analysis Template Selection View.
 - Risk Analysis Template Options Input View.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

- Risk Analysis Template Results Output View.
- Calculation Controller to perform express calculations.
- Risk Analysis Template Database that stores the data for the different RATs. This is where all options and precalculated results of the RATs are stored.
- System Risk Catalogues, i.e., risk and security catalogues stored in the KB.
- R-Input/Output Controller that exports and imports information with the R-Server for Risk Analysis. It has the following subcomponents:
 - R-Sender: Using a predefined set of R script templates, the R-sender prepares a new R script (by adding the user input to a R template).
 - R-Receiver: a parser that transforms the output produced by R scripts to html (text, tables, graphs)

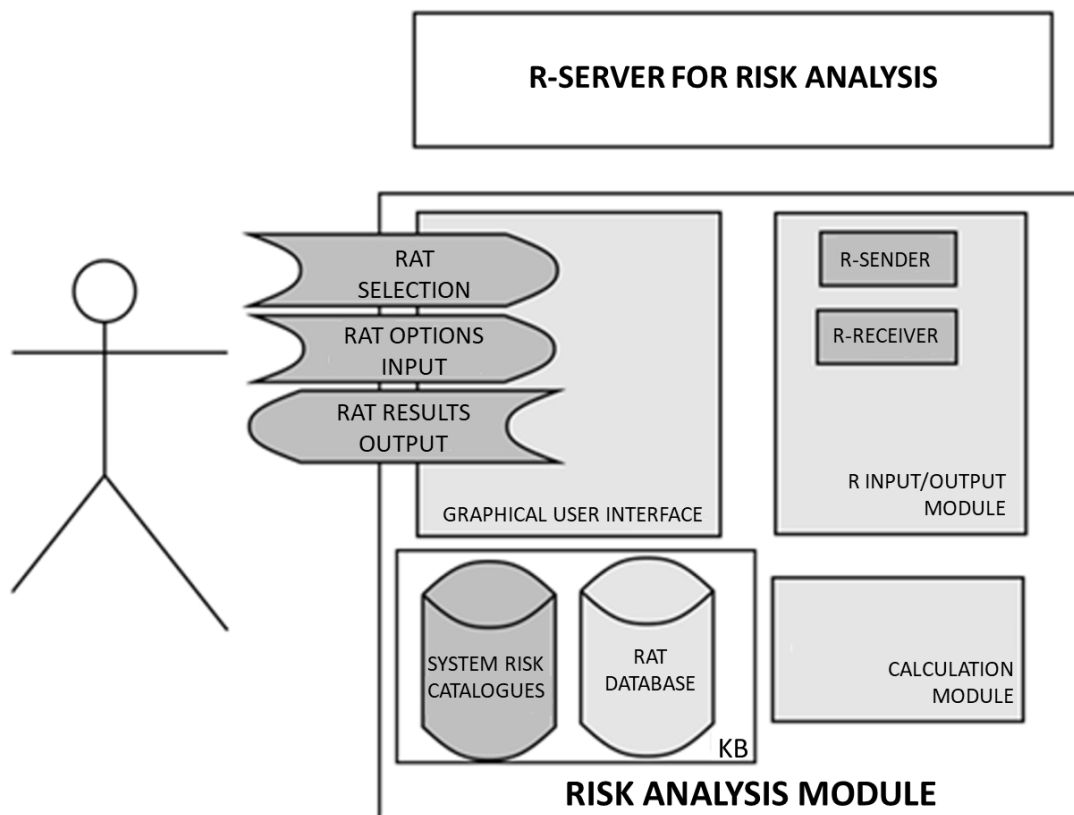


Figure 2: RISK ANALYSIS MODULE

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

We explain the different use cases (i.e., the three RAT types) in the following sections.

2.4.1 KB-RAT: use and elements

1. In the *Risk Analysis Template Selection View*, the User selects a Risk Analysis Template.
2. The *Risk Analysis Module* loads the RAT selected by the user.
3. The *Risk Analysis Module* translates the *Risk Analysis Template Options Specification* (in the KB) into a *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input View*.
 - a) For doing this, the *Risk Analysis Template Options Specification* might provide one or several *Risk Catalogues* to the User, which can be of two types: the *System Catalogues* and the *Risk Analysis Template Catalogues*.
4. The User provides their input to the *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input*.
5. Based on the User input, the *Risk Analysis Module* queries the *Risk Analysis Template Precalculation Table*, so that it provides the relevant results to a *Risk Analysis Template Dashboard* in the *Risk Analysis Template Results Output View*.
6. The User views the output of the Risk Analysis Template (applied to their input).

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

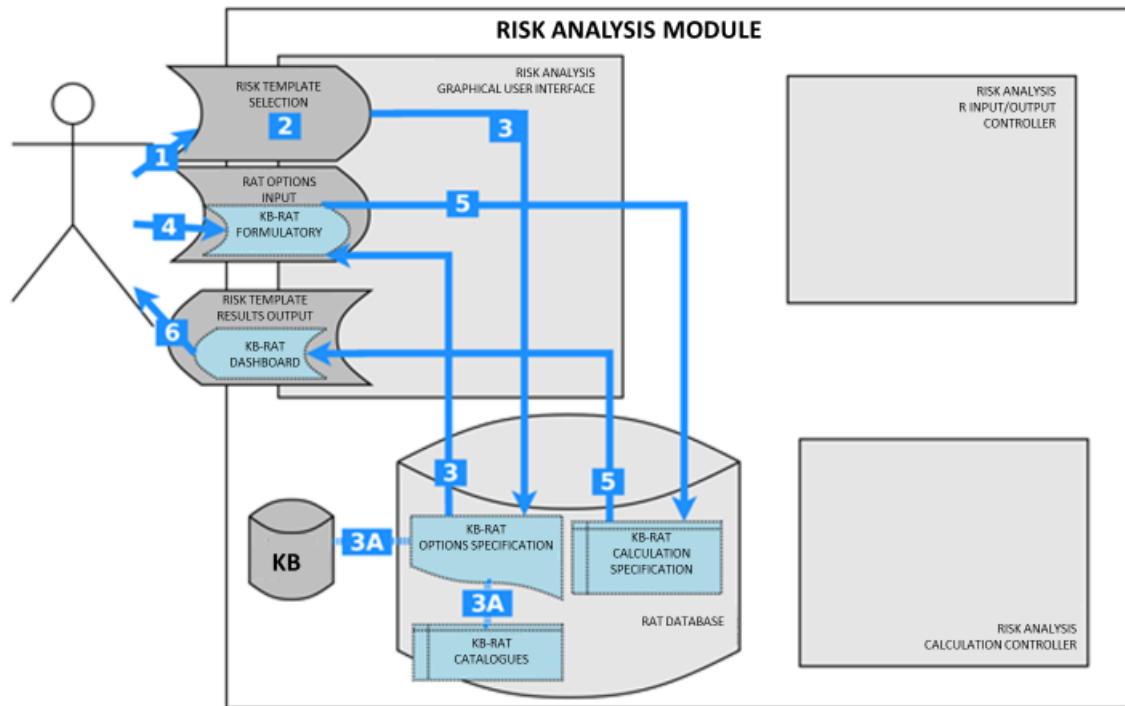


Figure 3: Dataflow diagram of KB-RAT

2.4.2 C-RAT

1. In the *Risk Analysis Template Selection View*, the User selects a RAT of the *Calculation-Based Type*.
2. The *Risk Analysis Module* activates the RAT selected by the User.
3. The *Risk Analysis Module* translates the *Risk Analysis Template Options Specifications* (in the KB) into a *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input View*.
 - a) For doing this, the *Risk Analysis Template Options Specifications* might provide one or several *Risk Catalogues* to the User, which can be of two types: the *System Catalogues* and the *Risk Analysis Template Catalogues*.
4. The User provides their input to the *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input*.
5. The *Risk Analysis Module* takes the input from the *Risk Analysis Template Formulary* into the *Calculation Module*.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

6. The *Risk Analysis Module* takes the *Risk Analysis Template Calculation Specifications* into the *Calculation Module*. The *Risk Analysis Template Calculation Specifications* must have the instructions on how to handle user input and what data is needed from the *Risk Analysis Template Simulation Results Table*.
7. Based on the instructions of the *Risk Analysis Template Calculation Specification*, the *Calculation Module* queries the *Risk Analysis Template Precalculation Tables* for obtaining relevant data to undertake the calculations.
8. The *Calculation Module* performs the calculation. It might need to do additional queries to the *Risk Analysis Template Precalculation Tables*.
9. When the calculation is finished, the *Calculation Module* provides the relevant results to a *Risk Analysis Template Dashboard* in the *Risk Analysis Template Results Output View*.
10. The User views the output of the RAT (applied to her input).

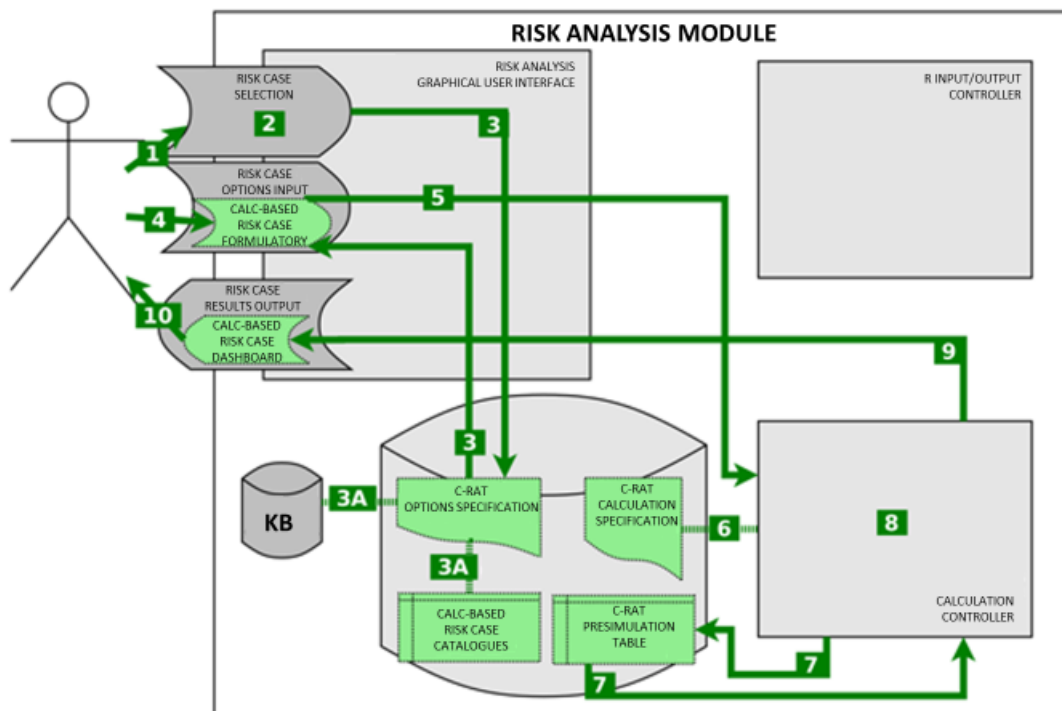


Figure 4: C-RAT dataflow diagram

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.4.3 R-RAT

1. In the *Risk Analysis Template Selection View*, the User selects a Risk Analysis Template of the *R-Based Type*.
2. The *Risk Analysis Module* activates the Risk Analysis Template selected by the User.
3. The *Risk Analysis Module* translates the *Risk Analysis Template Options Specification File* (in Risk Base Database) into a *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input View*.
4. The User provides their input to the *Risk Analysis Template Formulary* in the *Risk Analysis Template Options Input*.
5. The *Risk Analysis Module* sends the input from the *Risk Analysis Template Formulary* to the *R-Sender* of the *R Input/Output Controller*.
6. The *R-Sender* converts the User input into a format/message to be sent to the *R-Server for Risk Analysis*.
7. The *R-Sender* sends a *Simulation Request* file/message to the *R-Server for Risk Analysis*.
8. The *R-Server for Risk Analysis* performs the simulation.
9. The *R-Server for Risk Analysis* sends a *Simulation Results* file/message to the *R-Receiver*.
10. The *R-Receiver* converts the *R-Server* input into a format to be sent to the *Risk Analysis Template Results Output View*.
11. The *R-Receiver* provides the relevant results to a *Risk Analysis Template Dashboard* in the *Risk Analysis Template Results Output View*. It also stores or updates the *Simulation Results* in the *Risk Analysis Template Database*.
12. The User views the output of the RAT (applied to their input).

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

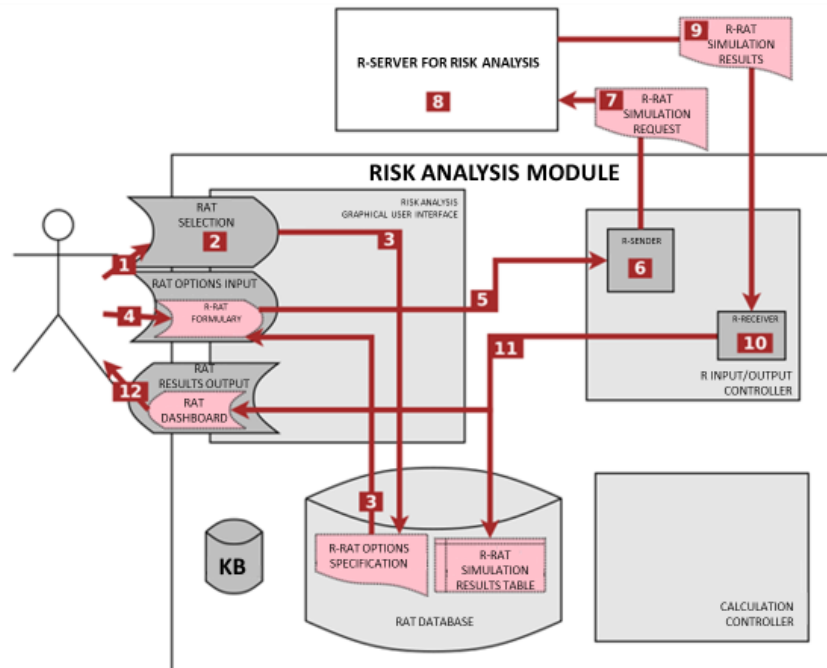


Figure 5: R-RAT dataflow diagram

2.5 Risk Analysis Templates Input / Output

2.5.1 Input Description

INPUT: The following are estimations of expected user input. This does not mean that all of these inputs are required in a Risk Analysis Template, but that this list covers all input types that might be needed in different Risk Analysis Templates.

The hierarchy of input items is the following:

Category	Subcategory
Organization profile	
Assets	
Other organizational features	
Impacts over assets or over organizational features	
Threats	Environmental threats Accidental threats

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

	Non-targeted threats Attackers Targeted cyber attack
Security controls	Technical controls Procedural controls Physical controls
Insurance products	
Security controls and insurance budget	

The tables below contain the following columns:

- **INPUT ITEM** indicates the items that shall be included in the risk analysis case in the pages where users provide their input.
- **INPUT TYPE** indicated the type of html element that is used
- **DESCRIPTION** provides information about the specific item
- **PARAMETERS** defines parameter, for a specific item, that the user of the toolbox can define.

The green rows indicate that the toolbox shall be designed with the idea of incorporating new items.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2 Input options

Upon selecting the risk analysis module, the user is guided through a series of options which are used to identify the user needs and collect the parameters for the risk analysis module. These options are each presented in single page or they are grouped together in cases where that is conceptually possible. There are a few different types of input depending on the selection required of the user. In some cases, the user has to select one of many options through radio buttons which allow the selection of only one and in other cases the user is called to select if an option should be considered or not, using a checkbox. Selecting a checkbox will sometimes enable other input as well, which becomes available once that specific option is enabled. There are also inputs which require the user to provide numeric information, usually referring to the values that will be used for the calculations. Finally, there are inputs where the user has to select using radio buttons among the options “already implemented”, “required for compliance”, “to be considered” and “not to be considered”. These inputs refer to possible options that are used while assessing the risks along also considering possible liability due to national or European laws that apply the company.

2.5.2.1 Organisation profile

These options are used to assess the size of the company.

INPUT ITEM	Input type	Parameters	Description
Type of company	Radio button	SME, Large	

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2.2 Assets

INPUT ITEM	Input type	Parameters	Description
Facilities	Checkbox	Checking this option enables the numeric input field for the value of facilities in euros.	Offices and other installations that could be affected by threats.
IT infrastructure	Checkbox	Checking this option enables the numeric fields for number of computers and number of servers	Information systems and other digital infrastructure that could be affected by threats.
Market share Customers	Radio button	Choosing market share enables the numeric fields for value of market share in euros and market share in percentage. Choosing Customers enables the numeric field for the number of customers.	Market share: Market share of the organisation. Number of current customers: Number of customers of the organisation.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Personally identifiable information (PII)	Checkbox	Choosing this option enables the numeric field for number of PII records	Information that can be used to identify, contact, or locate people.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Other organisational features

INPUT ITEM	Input type	Parameters	Description
Turnover	Checkbox	Choosing this option enables the numeric field for the turnover in euros.	Turnover of the organisation per year.
Production	Checkbox	Choosing this option enables the numeric field for the products manufactured per year	Production of the organisation per year.
Contractual and regulatory compliance	Checkbox		Include in the risk analysis the compliance requirements of the organisation regarding cybersecurity and data protection.

2.5.2.3 Environmental threats

INPUT ITEM	Input type	Description
Fire	Checkbox	A fire could affect physical assets as well as those digital assets stored, processed or transmitted through an IT infrastructure affected by fire.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2.4 Non-targeted cyber attacks

INPUT ITEM	Input type	Description
Virus, malware	Checkbox	This threat represents the most common viruses and malware that typically reduce the performance of a computer and may propagate ubiquitously through a network.

2.5.2.5 Attackers

INPUT ITEM	Input type	Parameters	Description
Hackers working for competitors	Checkbox	Choosing this option enables the dropdown input field for the skill of the hackers (options: Highly skilled / Average skilled)	Competitors aimed at disrupting the organisation through hackers that engage in targeted cyber attacks against the organisation.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Organised cyber criminals	Checkbox		Cyber criminals that operate within the framework of an organized crime entity, motivated to undertake profitable attacks. For this reasons, organisations with valuable assets or easy to attack are attractive targets.

2.5.2.6 Targeted cyber attacks

These options are enabled only after at least one of the attackers' options is selected.

INPUT ITEM	Input type	Description
Exfiltration of personally identifiable information (PII)	Checkbox	Exfiltration of personally identifiable data, resulting in a number of negative impacts for the company such as brand damage, loss of competitive advantage, regulatory fines, etc.
Manipulation of products and services	Checkbox	This type of attack involves manipulation of products or related services, compromising the production line or the quality/quantity of the product.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Description
Shutdown of website	Checkbox	An attack aimed at compromising the digital services that an organisation provides through the Internet, causing customer and reputation loss. Typically implemented through a Denial of Service attack.

2.5.2.7 Technical Security controls

INPUT ITEM	Input type	Parameters	Description
Antivirus	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Antivirus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Firewall	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Intrusion detection system	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations
Data backup solution	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	A solution of creating archive files of computer data so it may be used to restore the original after a data loss event.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Secure configuration	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Security measures and parameters defined and implemented in such a way as to reduce vulnerabilities.
Honeypots	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Security countermeasure consisting of IT assets which appear as very appealing, but with no real value, that an organization deploys in order to deflect the attack attempts from threat actors.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Cloud-based DDoS protection	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control. Additional dropdown menu allows the selection of the capacity of the control (2 Gbps, 5 Gbps, 10 Gbps, 1 Tbps).	It diverts DDoS traffic from the target to a cloud-based site absorbing malicious traffic.

2.5.2.8 Procedural controls

INPUT ITEM	Input type	Parameters	Description
Business continuity plan	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Set of processes which enable an organization to maintain operations during negative events or threat occurrences.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Security policy	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Formal document stating the plans of an organization for protecting its assets.
Awareness training	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Training methods and processes which increase the education and sensitivity level of employees on matters of security.
Incident response	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	The process, or set of processes, that defines the sequence of actions to be carried in order to detect, react, and provide response to cybersecurity incidents.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Security personnel / data protection officer	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	The set of employees whose functions consists in fulfilling the security day-to-day operations and activities, along with officers having specific key roles in a security policy.
Information sharing programs	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Specifically designed and implemented processes and enabling technology for sharing relevant information in a secure and instructive way.
Inventory of assets	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	Exhaustive database of raw materials, hardware, software, products, services, and all other assets used in maintaining business operations and client delivery of services and goods.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters	Description
Continuous vulnerability assessment and remediation	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	The process of proactive identification and correction of vulnerabilities reported through any source, including regular scans and vendor reports.

2.5.2.9 Physical controls

INPUT ITEM	Input type	Parameters	Description
Anti–fire system	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the control.	It can detect a fire facilitating early mitigation.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2.10 Insurance products - Coverage

INPUT ITEM	Input type	Parameters
Insurance covering data loss and fraud	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.
Insurance covering data loss, fraud, identity theft	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.
Insurance covering data loss	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters
Insurance covering data loss, product recall	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.
Insurance covering data loss, property damage and personal injury, media liability, theft of money and securities	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.
Insurance covering property damage	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.
Insurance covering data loss, fraud and computer reparation.	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

INPUT ITEM	Input type	Parameters
Insurance covering property damage, data loss, fraud and computer reparation.	Radio button	Choosing from already implemented, required, to be considered or not to be considered. Choosing required or to be considered enables an input field for the cost of the insurance product.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.2.11 Security controls and insurance constraints

INPUT ITEM	Input type	Parameters
Security budget	Checkbox	Choosing this option enables a numeric input field for the budget in euros.
Insurance budget	Checkbox	Choosing this option enables a numeric input field for the budget in euros.
Security and insurance budget	Checkbox	Choosing this option enables a numeric input field for the budget in euros and disables the other two.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

2.5.3 Output Description

OUTPUT: The following is a basic output for the toolbox, focusing on the output data relevant to the user. However, when it comes to the output in the GUI we also have to think in presenting a good “dashboard” of explanations and graphs that is informative and easy to the user.

Category of parameters	Output information provided to the user	Examples	Source of values																								
Event information	Probability of different events	<ul style="list-style-type: none">Probability of threatProbability of impact over asset	<p>The program will host (KB-RAT), calculate (C-RAT) or obtain from R (R-RAT) a table like the following one:</p> <table><tr><th>Sec Control selected</th><th>Security feature selected</th><th>... [other user input]</th><th>Event 1 In Impact X</th><th>Event 2 In Impact X</th><th>Event 1 in Impact Y</th></tr><tr><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td></tr><tr><td>Sec Control 1 2 and 5</td><td>Feature C E and G</td><td>...</td><td>0.70</td><td>0.30</td><td>0.55</td></tr><tr><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td></tr></table>	Sec Control selected	Security feature selected	... [other user input]	Event 1 In Impact X	Event 2 In Impact X	Event 1 in Impact Y	Sec Control 1 2 and 5	Feature C E and G	...	0.70	0.30	0.55
Sec Control selected	Security feature selected	... [other user input]	Event 1 In Impact X	Event 2 In Impact X	Event 1 in Impact Y																						
...																						
Sec Control 1 2 and 5	Feature C E and G	...	0.70	0.30	0.55																						
...																						

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

			Based on that, the GUI could produce textual output (e.g., installing the security controls 1 2 5 and the features C E G the probability of the event 1 in X is 70% and event 2 is 30%) or graphical output (e.g., histogram, boxplot).																				
	Expected events	<ul style="list-style-type: none">Expected impacts over assetsExpected total costExpected utility	<p>This represents information different from the upper one. In the upper one you have the info about different scenarios for a particular situation (eg., probability of 1 computer infected by a virus, probability of 2 computers infected, ...). In this one we have the info about what is expected in the particular situation (eg, it is expected that 10 computers are going to being infected). In some situations, this concept cannot be calculated.</p> <table><tr><th>Sec Control selected</th><th>Security feature selected</th><th>... [other user input]</th><th>Expected event In Impact X</th><th>Expected event in Impact Y</th></tr><tr><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td></tr><tr><td>Sec Control 1 2 and 5</td><td>Feature C E and G</td><td>...</td><td>Event 3</td><td>Not available</td></tr><tr><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td></tr></table> <p>Based on that, the GUI could produce textual or graphical output (e.g., histogram, boxplot).</p>	Sec Control selected	Security feature selected	... [other user input]	Expected event In Impact X	Expected event in Impact Y	Sec Control 1 2 and 5	Feature C E and G	...	Event 3	Not available
Sec Control selected	Security feature selected	... [other user input]	Expected event In Impact X	Expected event in Impact Y																			
...																			
Sec Control 1 2 and 5	Feature C E and G	...	Event 3	Not available																			
...																			
Economic information	How the expected impacts, costs or utilities vary when	<ul style="list-style-type: none">Utility/economic return on security investment	This is represented by a function. This function could be provided explicitly or with the points/data to draw its representation or that are important (e.g., “investing in																				

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

	we change the price of the insurance, security budget, or economic value of an asset	<ul style="list-style-type: none"> Utility/economic return on insurance price 	security up to €15.125 increases expected economic return but after that point it decreases it”).																
Decision outputs	Report about the decision portfolios	<ul style="list-style-type: none"> Recommended Cybersecurity controls and insurance portfolio (e.g, the one that has the biggest expected utility). Optimal security budget/investment ... 	<p>This would be calculated to obtain a table like the following one:</p> <table border="1"> <thead> <tr> <th>Sec Control selected</th><th>Security feature selected</th><th>Expected economic return</th><th>Expected utility</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td><td>...</td><td>...</td></tr> <tr> <td>Sec Control 1 2 and 5</td><td>Feature C E and G</td><td>€ 250.000</td><td>0.9</td></tr> <tr> <td>...</td><td>...</td><td>...</td><td>...</td></tr> </tbody> </table> <p>From which we can extract the best portfolio based on expected economic return, expected utility, or any additional selection criteria</p>	Sec Control selected	Security feature selected	Expected economic return	Expected utility	Sec Control 1 2 and 5	Feature C E and G	€ 250.000	0.9
Sec Control selected	Security feature selected	Expected economic return	Expected utility																
...																
Sec Control 1 2 and 5	Feature C E and G	€ 250.000	0.9																
...																

2.6 Security Considerations

The following security considerations will be taken into account:

- All communication between the user browser and the Toolbox will be encrypted, using HTTPS and a valid SSL certificate.
- The Toolbox and the R Server will be installed in a dedicated virtual machine with no local users and access restricted only to the administrators of the VM.
- User information (user profile, company data given in a simulation, etc.) will not be visible to other users.
- The users will have the option to delete their account and all their personal/company information.

2.7 Implementation

2.7.1 Technologies

In this section we make a brief introduction the technologies used in the CYBECO Toolbox.

Content management System

A content management system (CMS) is software that enables users to easily create and add content to a web application. Most of them provide much of the basic infrastructure needed for creating such an application upon installation along with the basic functionality that is required. Another important advantage of a CMS is the large variety of modules that are available in order to supplement the basic implementation and extend it to the point that is needed to achieve the desired functionality.

Drupal

The toolbox will be based on Drupal², an open-source PHP software that includes a content management platform and a development framework. Drupal is modular, highly extendable and allows for the creation of custom complex document types and entities.

² <https://www.drupal.org/about>

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Apart from the custom entity types though, one of the most important features of Drupal is the ability to create custom modules as well. These modules can be used for creating and adding new functionality and can be installed or uninstalled easily on any compatible Drupal version. Therefore, containing a new feature in such a module provides the advantage of making it easy to enable or disable it if needed or even install it on a new implementation.

MVC

Drupal 8 modules are created using MVC architecture. MVC architecture is used to separate the model which represents the part of the software where the data are stored or created, the view which represents the part that is displayed for the user or sent via a web service and the controller which is the part that changes the view upon request.

The separation of a feature into these three layers provides modularity and separation of the business logic, the front end and the necessary connection and information exchange between the two. While it increases the development complexity, its advantages make it worthwhile. The view can be redesigned easily without affecting the rest of the application, the same model can be used by multiple different modules without needing to change it and the controller can provide different views depending on the input.

R

R is a programming language and software environment primarily used for statistical computing and graphics. Its powerful computational abilities make it ideal for use in a software which provides risk analysis taking into account multiple factors, such as the toolbox.

R is available as Free Software under the terms of the Free Software Foundation's GNU General Public License in source code form. It compiles and runs on a wide variety of UNIX platforms and similar systems (including FreeBSD and Linux), Windows and MacOS.

Message Broker - RabbitMQ

RabbitMQ is an open source message broker that supports message queues³. It is easy to install and configure, it can sustain large workloads and it provides detailed tutorials for

³ <https://www.rabbitmq.com/tutorials/tutorial-two-python.html>

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

implementing producer and consumer modules in many different programming languages. It also supports features described such as durability, TTL and Ack⁴. The Message Broker is used in CYBECO Toolbox to facilitate the usage of multiple workers (nodes used for running simulations).

Server technologies

The software will be installed in a dedicated Ubuntu Linux Server⁵ in a Virtual machine. Apache⁶ and Mysql⁷ will be used for the web server and the database server, respectively.

2.7.2 Risk analysis module

The risk analysis module is created making use of the aforementioned technologies and architecture patterns as part of the toolbox. Following the MVC pattern the controller serves the input view to the user upon visiting the risk analysis page. There the user is called to provide the necessary data through the input view. These data will then be processed by the controller. There are two controllers in the module:

- The R-Input/Output Controller which is used for handling R-RATs that require simulation
- The Calculation Controller that handles the C-RATs.

Each Controller (R or Calculation) processes the user input and provides the risk analysis results. These results are presented to the user through a different view.

Therefore, the risk analysis module is separated in three parts. The views which present the user with an interface for providing the input and receiving the results, the controllers which will receive the data and provide the appropriate view and the R Server which is used to schedule the simulations.

⁴ <https://www.rabbitmq.com/>

⁵ <https://www.ubuntu.com/server>

⁶ <https://httpd.apache.org/>

⁷ <https://www.mysql.com/>

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

R Server

The R server is in essence a scheduler that receives requests for new tasks (simulations) from the R Simulation Controller. Simulations run in one or more computing nodes, called R Workers. Each new request for a simulation is entered in a message queue. The scheduler ensures that only a certain number of simulations is run on the same time at the same worker. This is a configurable option, based on the resources of each worker.

Each worker receives the input in the form of parameters and starts a new process with the Rscript command (R script execution) to perform the risk analysis. Once the analysis is complete the results are saved in a csv file. The file is returned to the R Simulation Controller to be processed so that the results are presented to the user in the form of free text, tables and charts.

The communication between the R Server and the workers is done through a message broker (RabbitMQ). More specifically the Message broker has an input and an output queue. Each worker subscribes to the input queue and the R Server subscribes to the output queue.

So for each new simulation, we have the following steps:

- The R server sends a message to the input queue with the parameters of the simulation.
- One of the workers that is not over the limit of concurrent jobs receives the message and starts a new simulation. The message becomes unavailable to the rest of the workers
- When the Rscript command terminates
 - it produces the results in the form of a file
 - acknowledges the successful termination of the task and the message containing the task/simulation definition is removed from the input queue.
 - It puts a reference to the file containing the results in the output queue. This message also references the original input message
- The R server receives the notification about the results file from the output queue.
- The results are ready to be served to the user by the R Simulation Controller. The user is also informed by email for the completion of the simulation.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

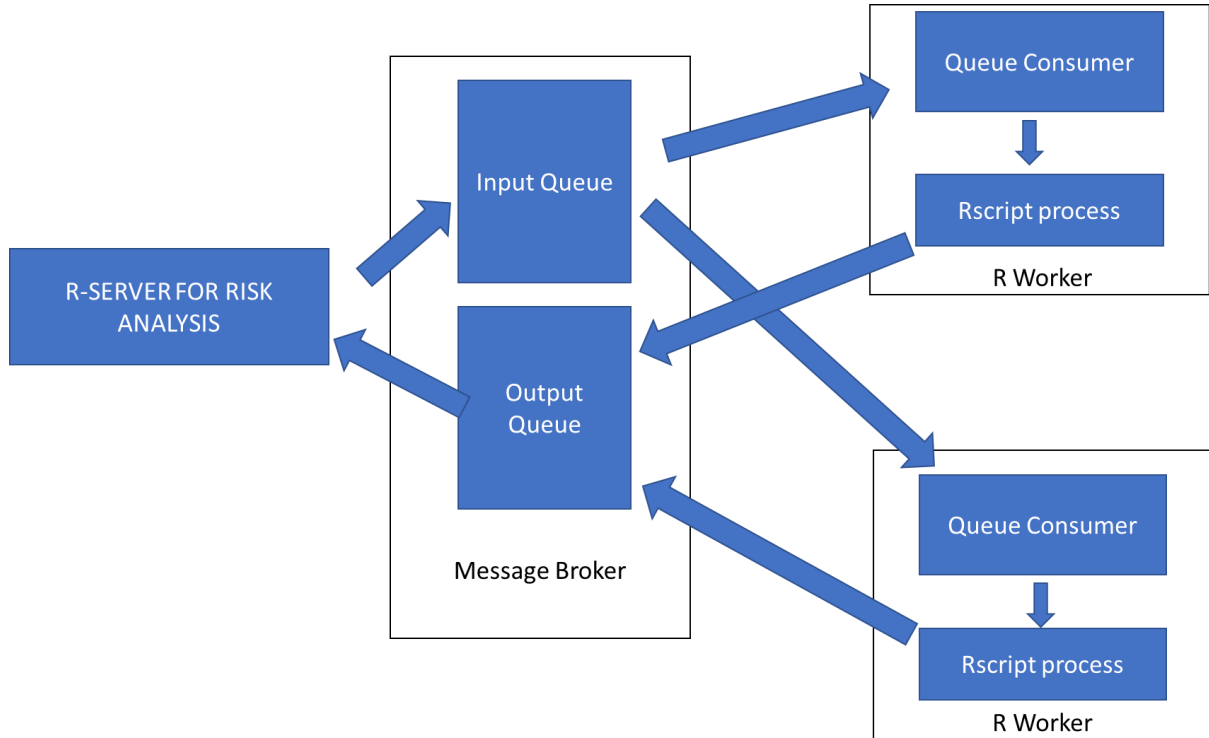


Figure 6: R Server communication with R Workers

GUI

While the R environment provides a graphical user interface, its complexity makes it unsuitable for the untrained user, and this is why the user input is collected through the toolbox application. The toolbox GUI provides a step by step guided way to receive the user input. In most cases the user is called to make selections out of the available options, which are explained through appropriate messages. Once the input collection is completed, the user is notified of the time he or she will have to wait until the calculations are complete.

To better analyze and document the functionality of the Risk Analysis Module, it was considered important to describe its functionality in the form of wireframes. An application wireframe connects the underlying conceptual structure, or information architecture, to the surface, or visual design of the application⁸. Wireframes help establish functionality and the relationships between different screen templates of an application.

⁸ Garrett, Jesse James (2010). The Elements of User Experience: User-Centered Design for the Web and Beyond. New Riders Press. ISBN 978-0321683687.

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

The produced wireframes purposefully lack typographic style, color, or graphics, since the focus lies in functionality, behavior, and priority of content. In other words, they focus on what a screen does, not what it looks like.

The wireframes are available in the Appendix of the Deliverable.

2.7.3 KB Module

The KB entities are designed as custom Drupal content types⁹. The content of the KB is organized using the built-in taxonomy module that can be used to connect, relate and classify the various KB entities.

More information about the KB module can be found in D5.2: CYBECO content and data collection manual, submitted at M14.

⁹ <https://www.drupal.org/docs/7/understanding-drupal/content-types>

3 Conclusions

This deliverable presented the work carried out as part of T5.1 Development of methodology for building CYBECO Toolbox. The main outcomes of the task, presented in this report, were the:

- The definition of the concepts behind the tool in terms of functional characteristics, design approach and expected outputs.
- The design of the Toolbox, in form of wireframes that were based on user journeys provided and validated by the project consortium.
- The provision of a system architecture that can support the required functionality in a scalable way.

4 Acronyms and Abbreviations

CMS	Content Management System
KB	Knowledge Base
RAT	Risk Analysis Template
C-RAT	Calculation-bases Risk Analysis Template
KB-RAT	KB-based Risk Analysis Template
R-RAT	R-based Risk Analysis Template
MVC	Model View Controller

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

5 Appendix: CYBECO Toolbox v2 Wireframes

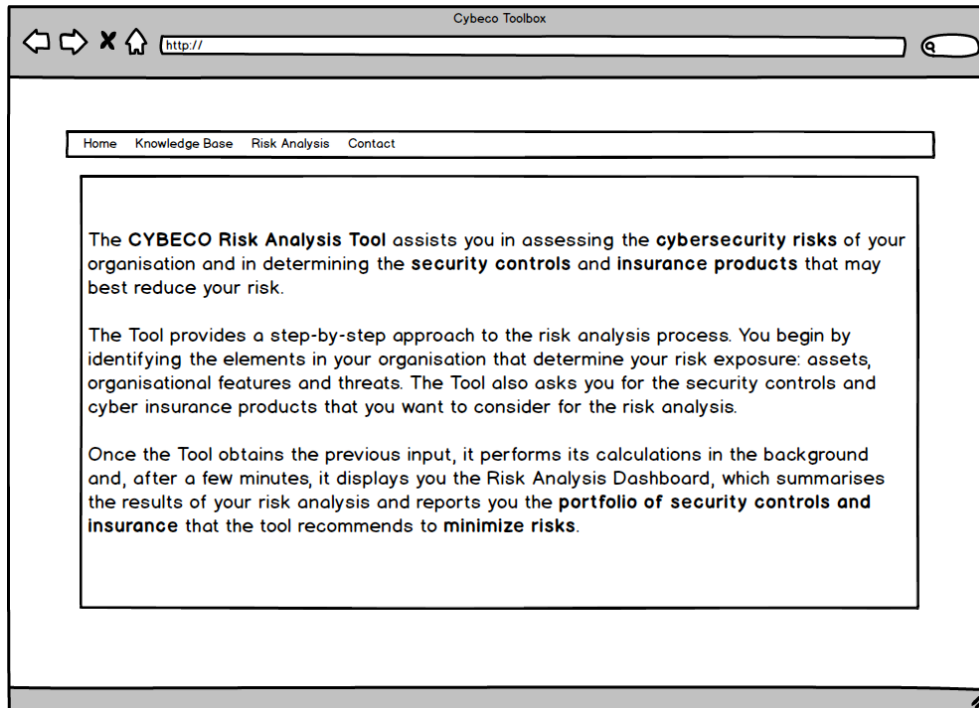


Figure 7: Home Page

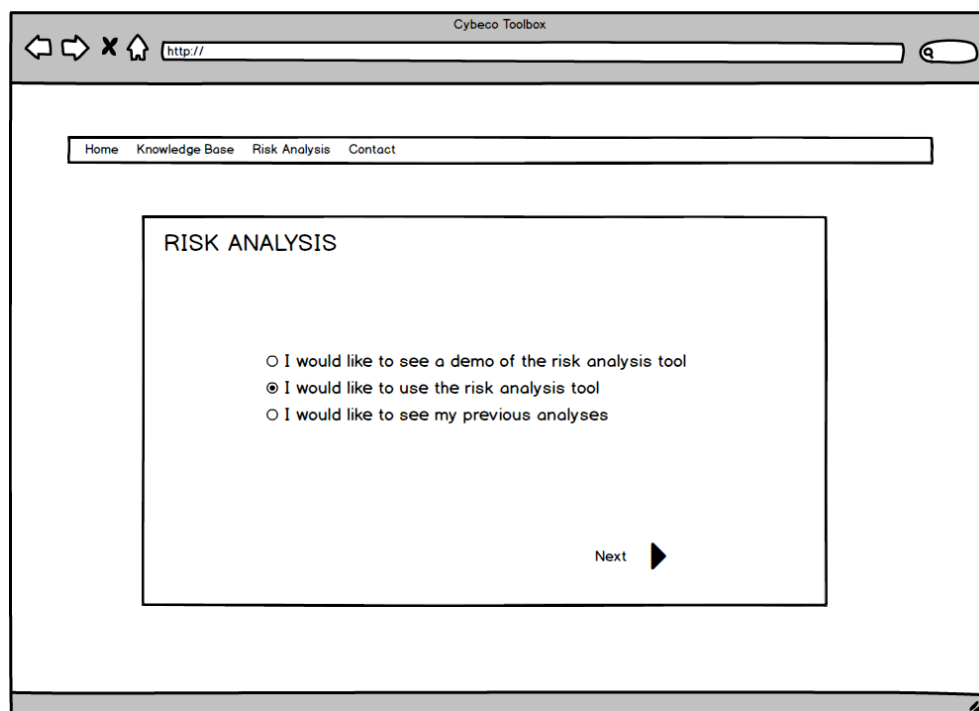
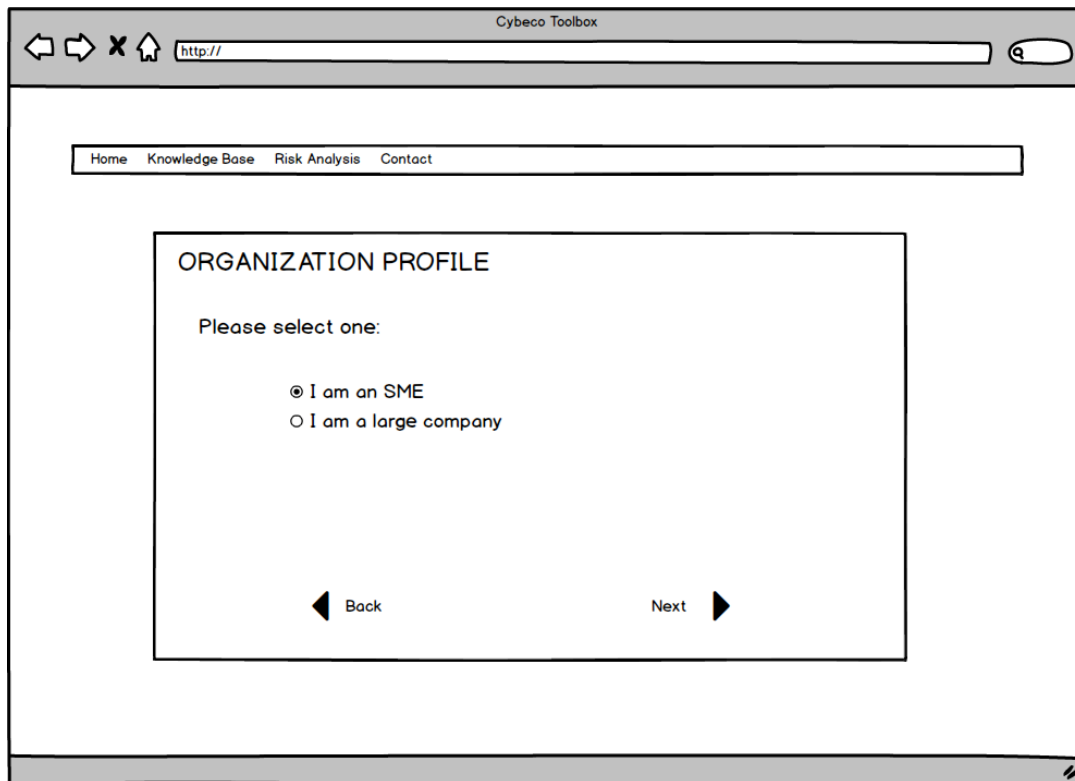


Figure 8: Case selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox



Cybeco Toolbox

http://

Home Knowledge Base Risk Analysis Contact

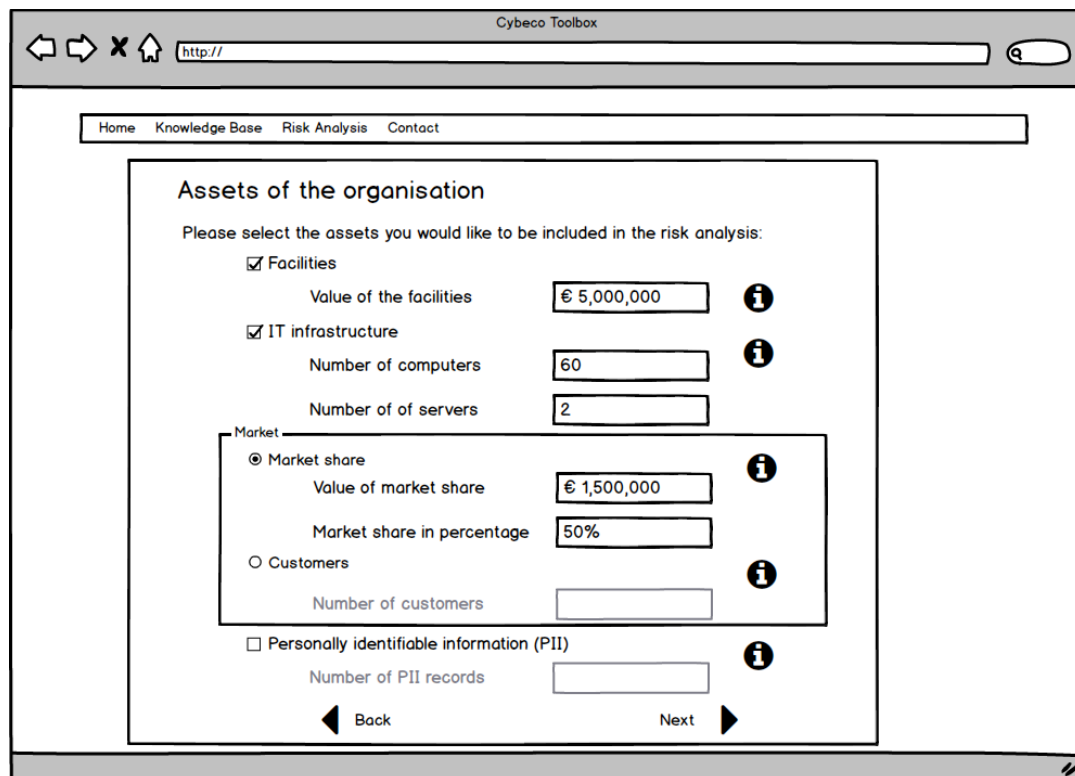
ORGANIZATION PROFILE

Please select one:

☒ I am an SME
☐ I am a large company

Back Next

Figure 9: Organisation profile selection



Cybeco Toolbox

http://

Home Knowledge Base Risk Analysis Contact

Assets of the organisation

Please select the assets you would like to be included in the risk analysis:

☒ Facilities
Value of the facilities € 5,000,000 ⓘ

☒ IT infrastructure
Number of computers 60 ⓘ
Number of of servers 2 ⓘ

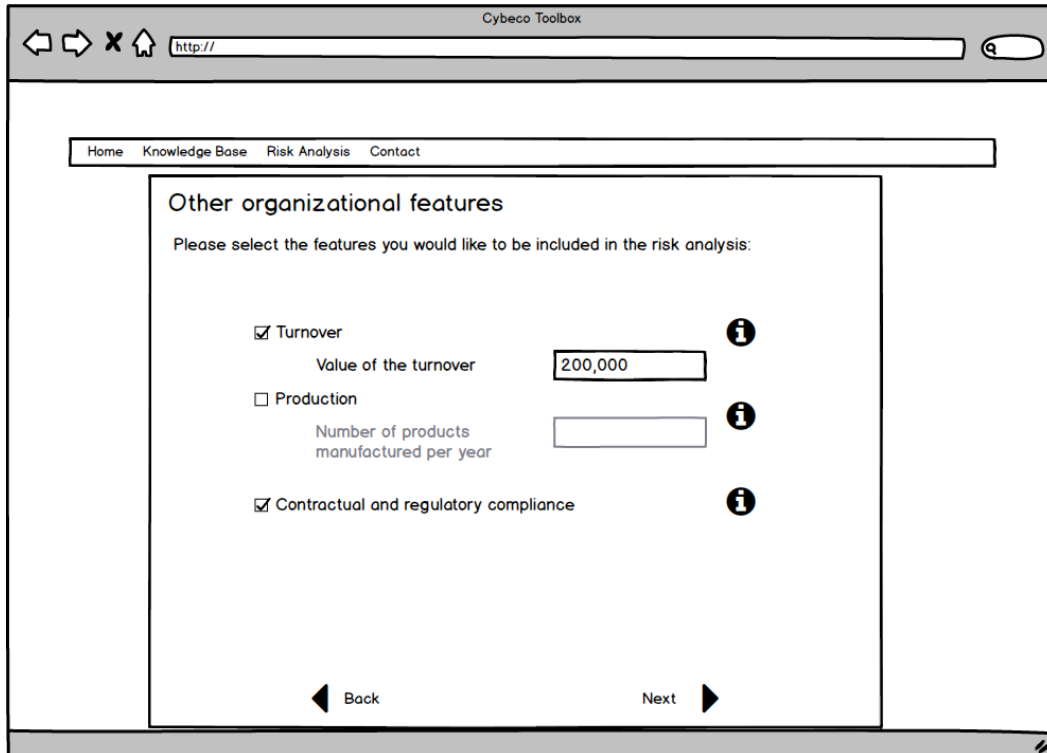
Market
☒ Market share
Value of market share € 1,500,000 ⓘ
Market share in percentage 50% ⓘ
☐ Customers
Number of customers ⓘ

☐ Personally identifiable information (PII)
Number of PII records ⓘ

Back Next

Figure 10: Assets selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

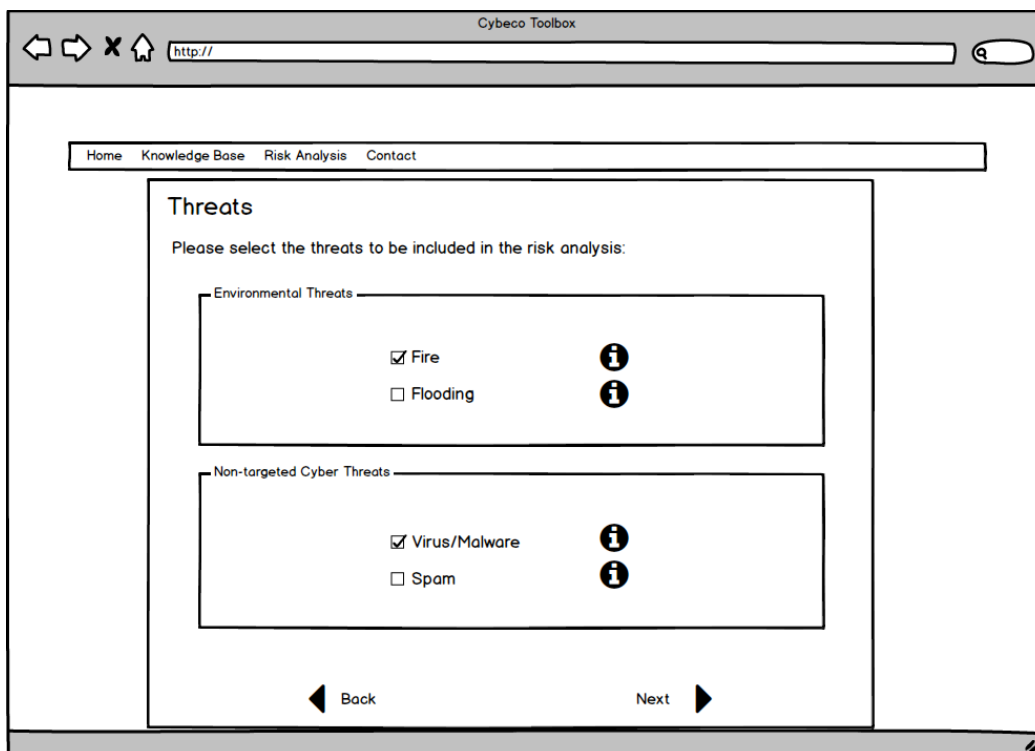


The screenshot shows a web browser window titled "Cybeco Toolbox". The address bar contains "http://". The navigation menu includes "Home", "Knowledge Base", "Risk Analysis", and "Contact". The main content area is titled "Other organizational features" and contains the instruction "Please select the features you would like to be included in the risk analysis:". There are three sections of features:

- ☒ Turnover (with an information icon *i*)
 - Value of the turnover:
- ☐ Production (with an information icon *i*)
 - Number of products manufactured per year:
- ☒ Contractual and regulatory compliance (with an information icon *i*)

At the bottom, there are "Back" and "Next" navigation buttons.

Figure 11: Other features selection



The screenshot shows the same web browser window, now displaying the "Threats" selection screen. The instruction is "Please select the threats to be included in the risk analysis:". There are two sections of threats:

- Environmental Threats** (with an information icon *i*):
 - ☒ Fire (with an information icon *i*)
 - ☐ Flooding (with an information icon *i*)
- Non-targeted Cyber Threats** (with an information icon *i*):
 - ☒ Virus/Malware (with an information icon *i*)
 - ☐ Spam (with an information icon *i*)

At the bottom, there are "Back" and "Next" navigation buttons.

Figure 12: Environmental/Non-targeted threats selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

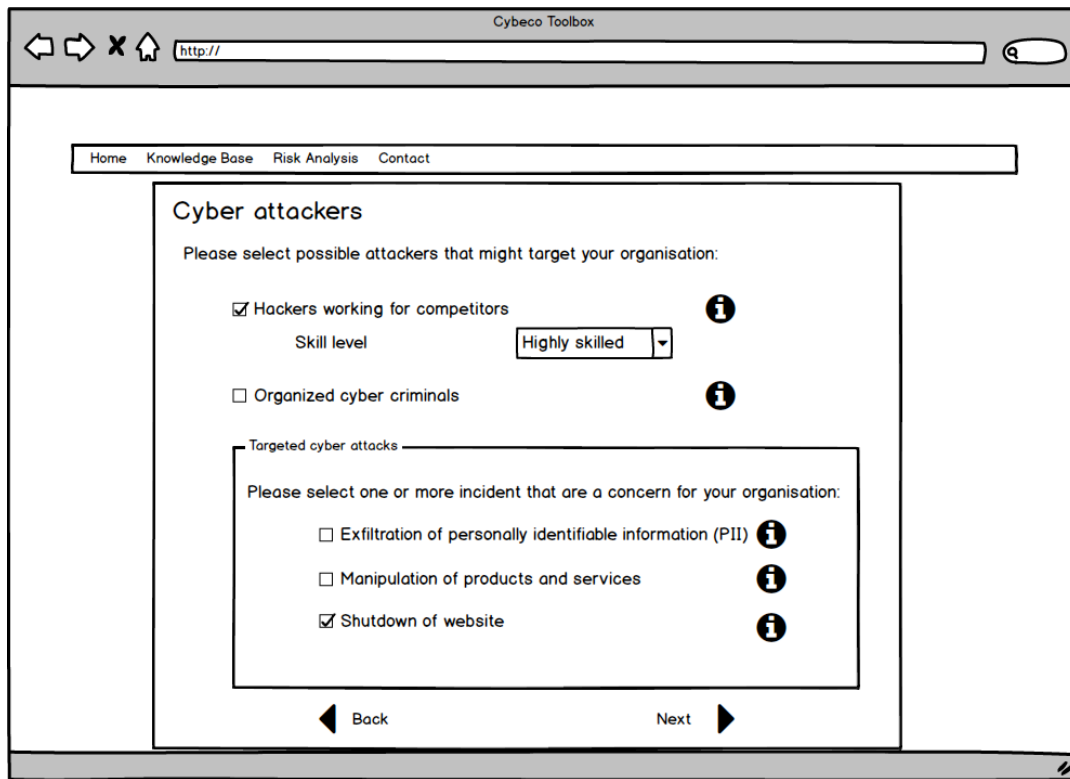
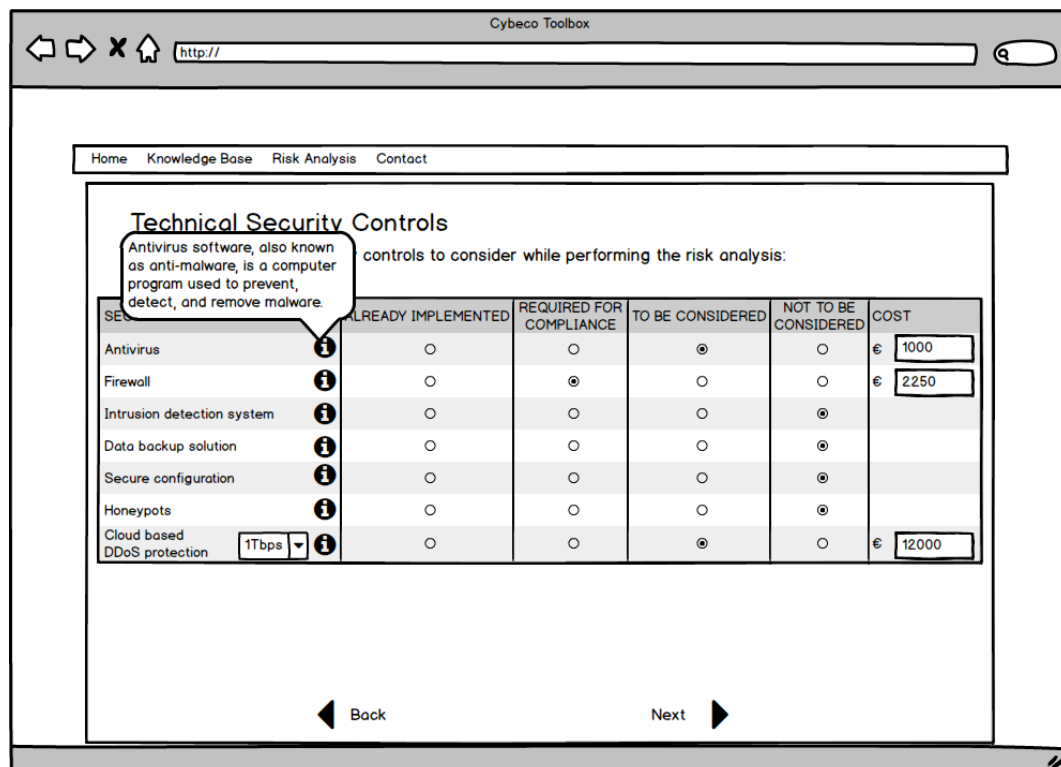


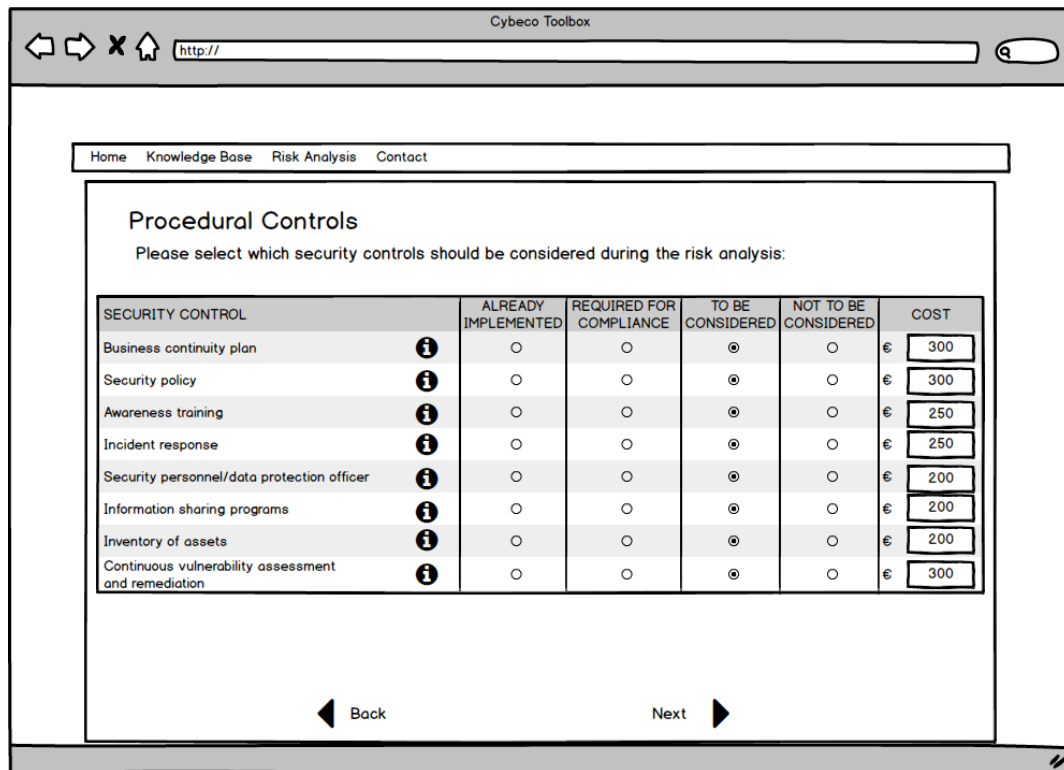
Figure 13: Attacker/Cyber-attacks selection



SELECTION	ALREADY IMPLEMENTED	REQUIRED FOR COMPLIANCE	TO BE CONSIDERED	NOT TO BE CONSIDERED	COST
Antivirus	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 1000
Firewall	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	€ 2250
Intrusion detection system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Data backup solution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Secure configuration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Honeypots	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Cloud based DDoS protection	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 12000

Figure 14: Technical security controls selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox



Home Knowledge Base Risk Analysis Contact

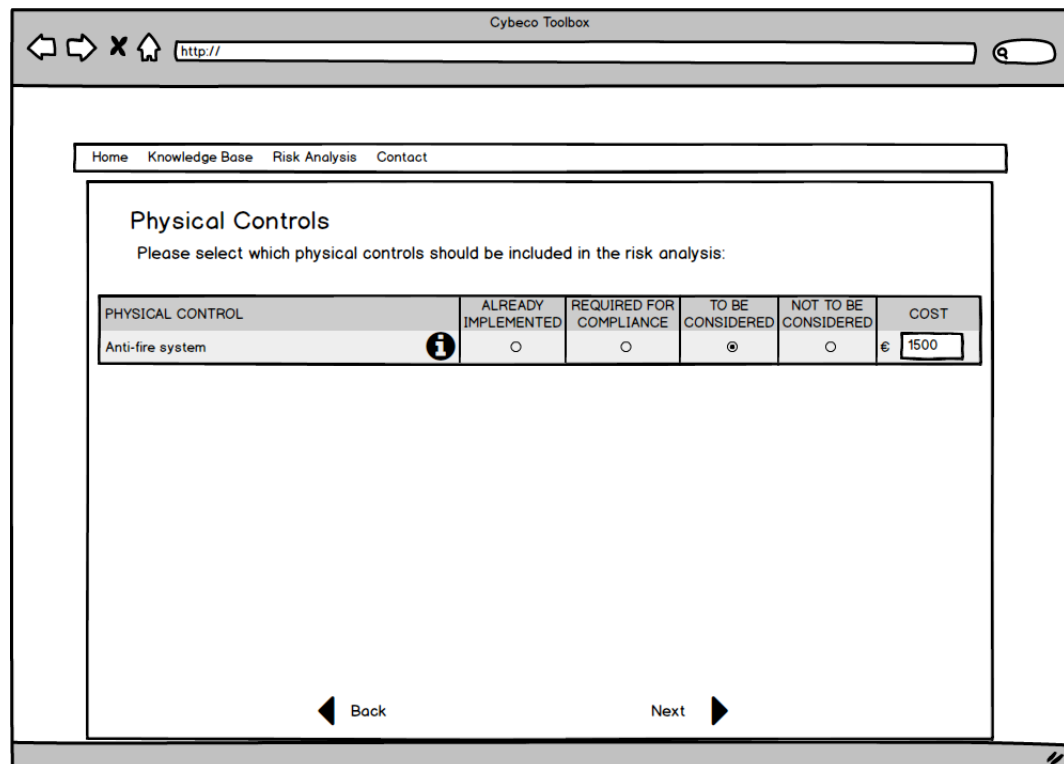
Procedural Controls

Please select which security controls should be considered during the risk analysis:

SECURITY CONTROL	ALREADY IMPLEMENTED	REQUIRED FOR COMPLIANCE	TO BE CONSIDERED	NOT TO BE CONSIDERED	COST
Business continuity plan	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 300
Security policy	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 300
Awareness training	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 250
Incident response	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 250
Security personnel/data protection officer	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 200
Information sharing programs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 200
Inventory of assets	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 200
Continuous vulnerability assessment and remediation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 300

Back Next

Figure 15: Procedural controls selection



Home Knowledge Base Risk Analysis Contact

Physical Controls

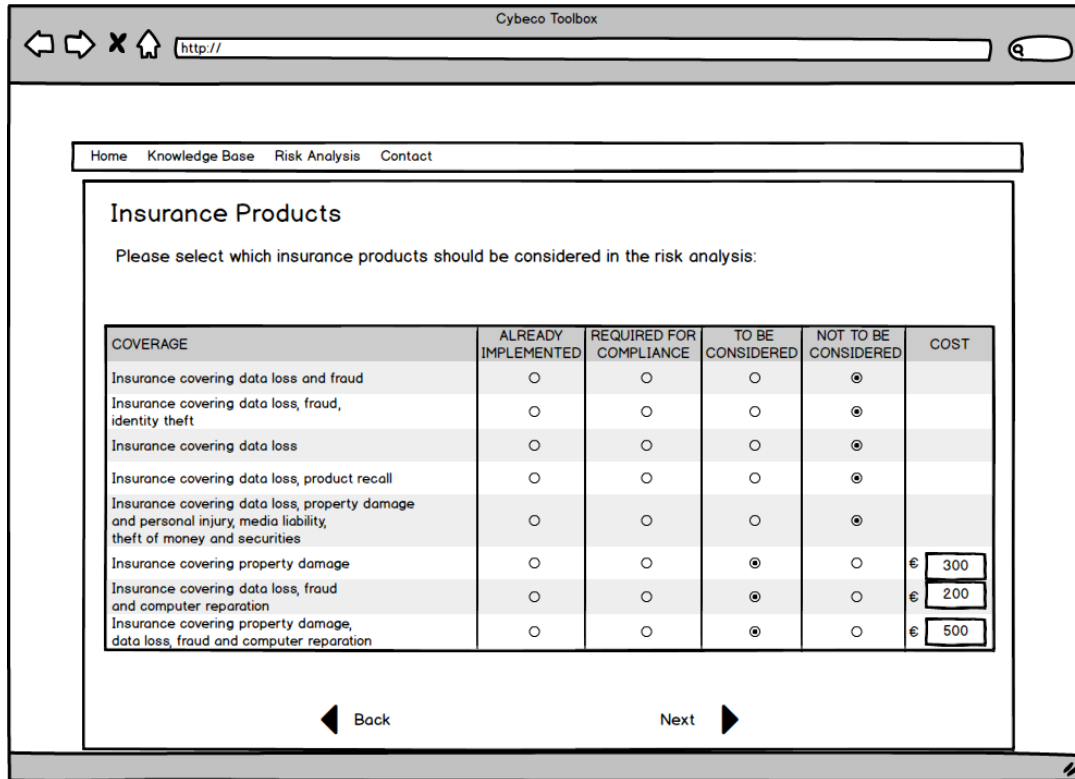
Please select which physical controls should be included in the risk analysis:

PHYSICAL CONTROL	ALREADY IMPLEMENTED	REQUIRED FOR COMPLIANCE	TO BE CONSIDERED	NOT TO BE CONSIDERED	COST
Anti-fire system	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 1500

Back Next

Figure 16: Physical controls selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox



Home Knowledge Base Risk Analysis Contact

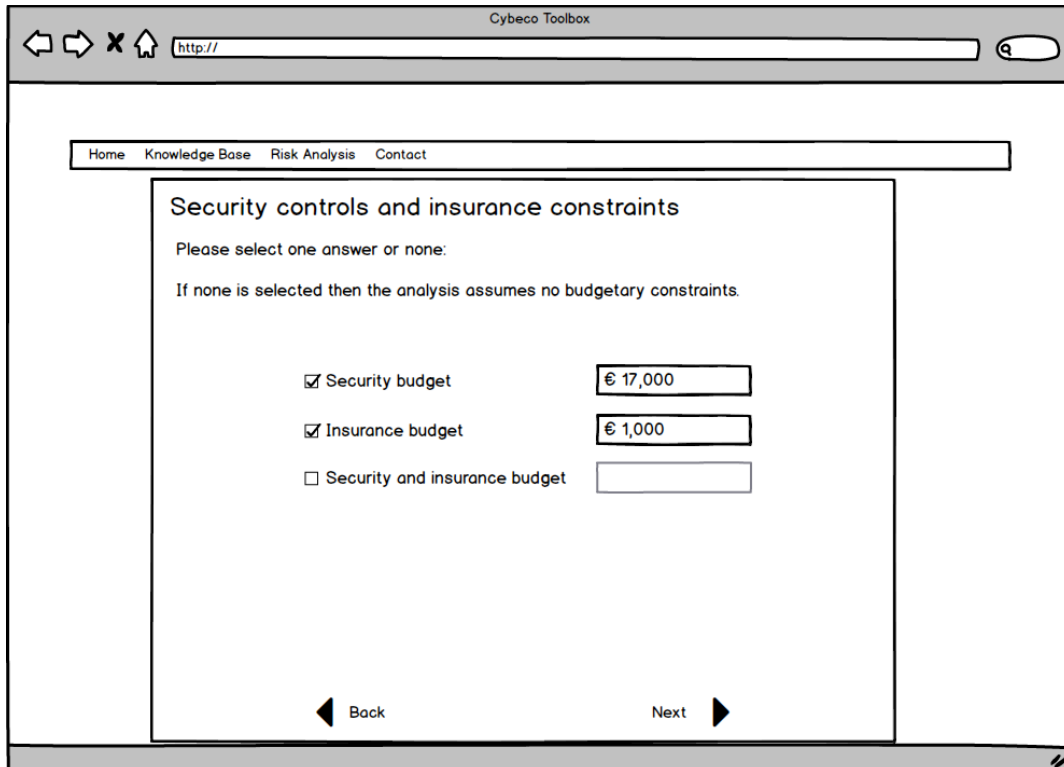
Insurance Products

Please select which insurance products should be considered in the risk analysis:

COVERAGE	ALREADY IMPLEMENTED	REQUIRED FOR COMPLIANCE	TO BE CONSIDERED	NOT TO BE CONSIDERED	COST
Insurance covering data loss and fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Insurance covering data loss, fraud, identity theft	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Insurance covering data loss	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Insurance covering data loss, product recall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Insurance covering data loss, property damage and personal injury, media liability, theft of money and securities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Insurance covering property damage	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 300
Insurance covering data loss, fraud and computer repairation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 200
Insurance covering property damage, data loss, fraud and computer repairation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	€ 500

Back Next

Figure 17: Insurance coverage selection



Home Knowledge Base Risk Analysis Contact

Security controls and insurance constraints

Please select one answer or none:

If none is selected then the analysis assumes no budgetary constraints.

☒ Security budget € 17,000

☒ Insurance budget € 1,000

☐ Security and insurance budget

Back Next

Figure 18: Insurance constraints selection

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

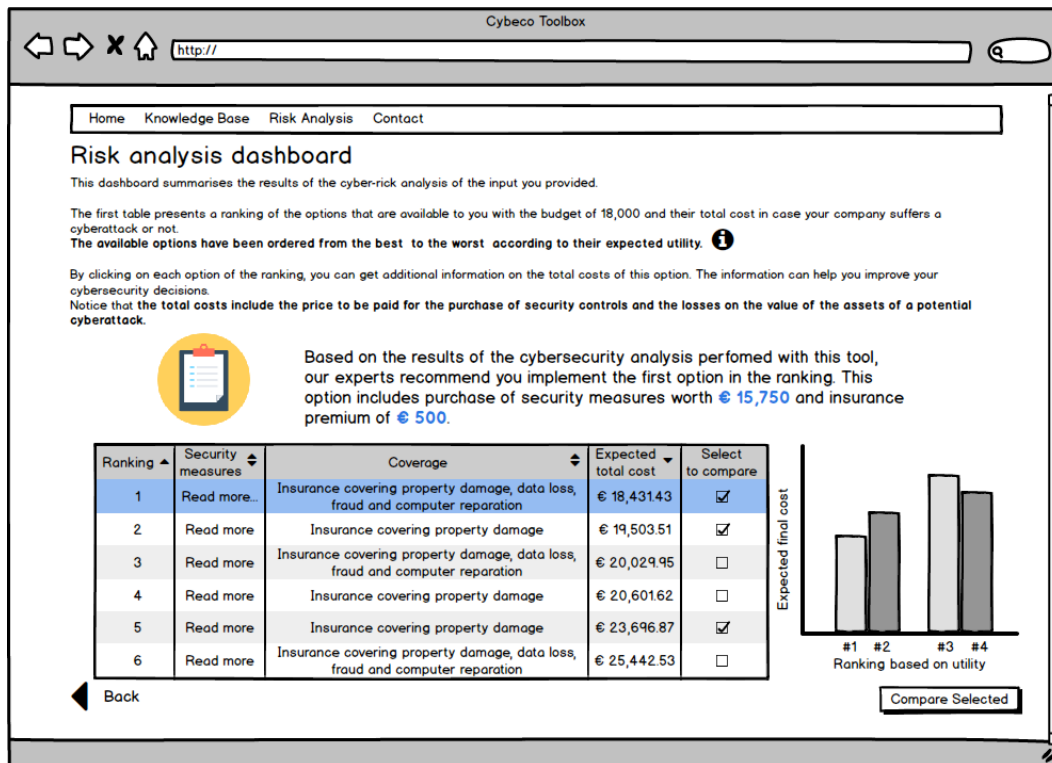


Figure 19: Risk analysis results

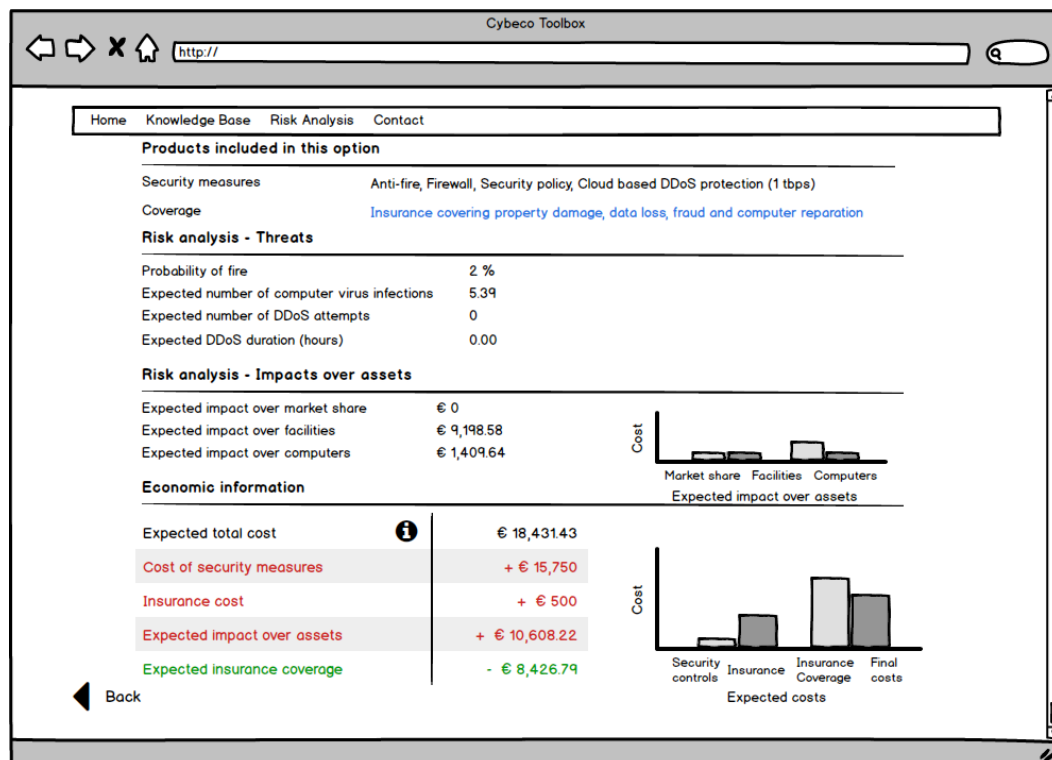


Figure 20: Risk analysis results product details

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

Cybeco Toolbox

Home Knowledge Base Risk Analysis Contact

Detailed options comparison

Portfolio	1	2	5
Coverage	Insurance covering property damage, data loss, fraud and computer reparation	Insurance covering property damage	Insurance covering property damage
Anti-Fire system	Yes	Yes	No
Firewall	Yes	Yes	Yes
Risk mitigating procedures	No	No	No
Cloud-based DDoS protection system	1 tbps	1tbps	1tbps
Probability of Fire	2%	2%	2%
Expected number of computer virus infections	5.39	5.43	5.36
Expected number of DDoS attempts	0	0	0
Expected DDoS duration	0.00	0.00	0.00
Expected impact over market share	0	0	0
Expected impact over facilities	€ 9,198.58	€ 10,859.71	€ 36,273.79
Expected impact over computers	€ 1,409.64	€ 1,281.56	€ 1,692.11
Cost of security controls	€ 15,750	€ 15,750	€ 14,250
Cost of insurance	€ 500	€ 300	€ 500
Expected insurance coverage	€ 8,426.79	€ 8,687.77	€ 29,019.03
Expected final costs	€ 18,431.43	€ 19,503.51	€ 23,696.87

Back

Export Print

Figure 21: Results comparison

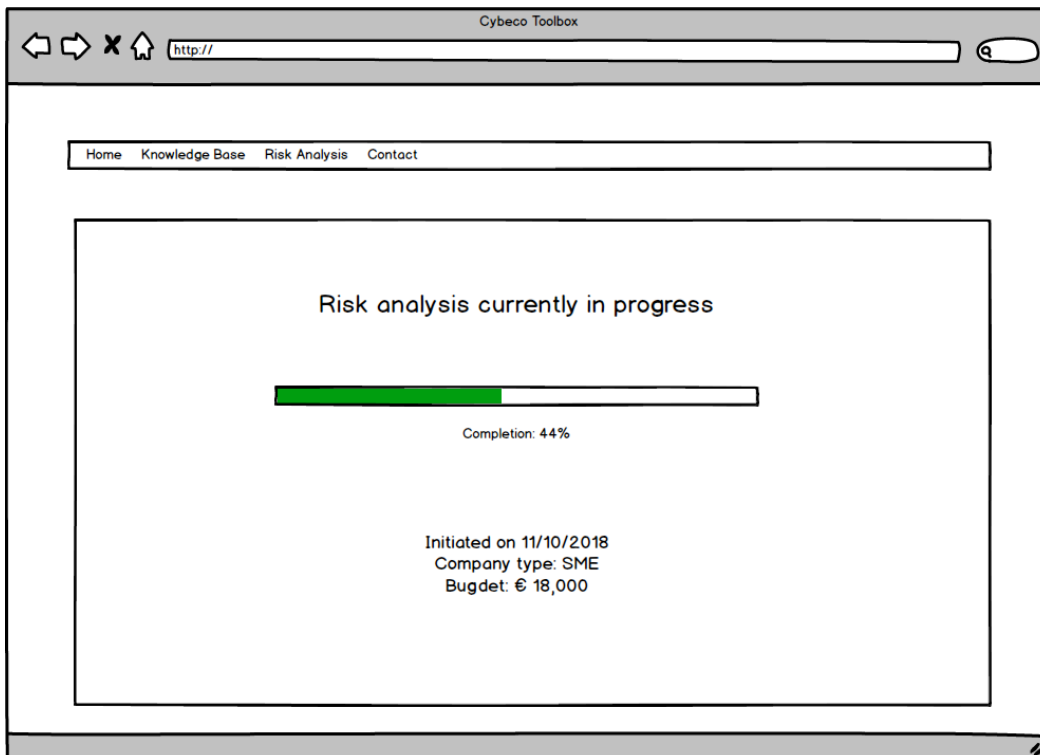


Figure 22: Analysis in progress screen

D5.1: Description Methodology & Design Principles of the CYBECO Toolbox

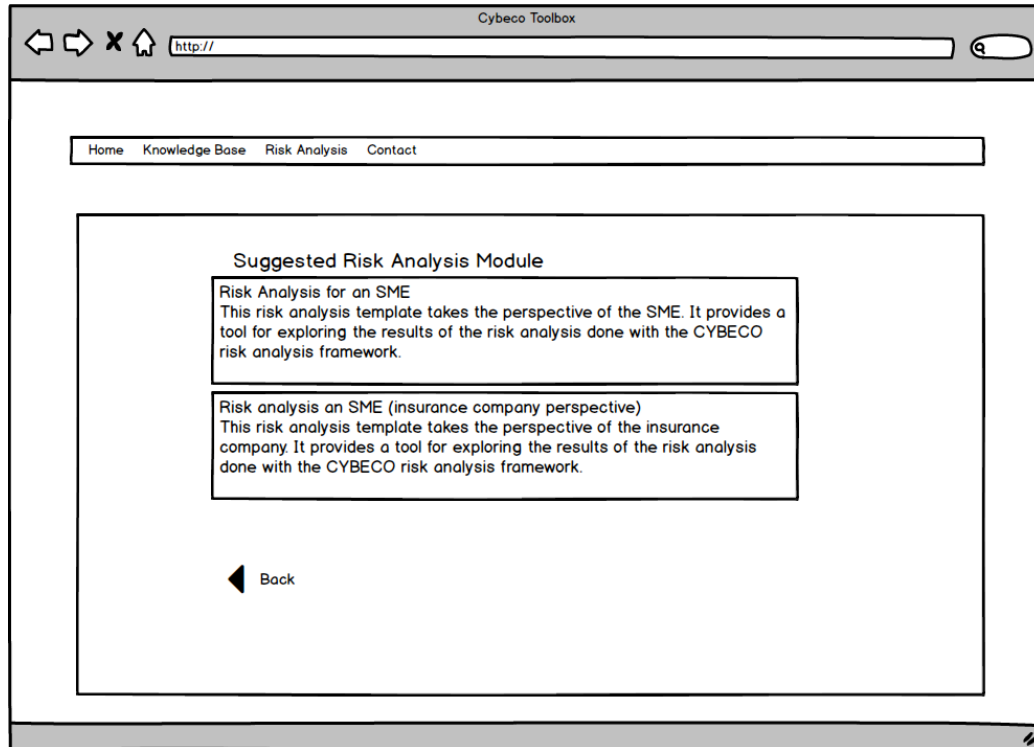


Figure 23: Demo risk analysis modules

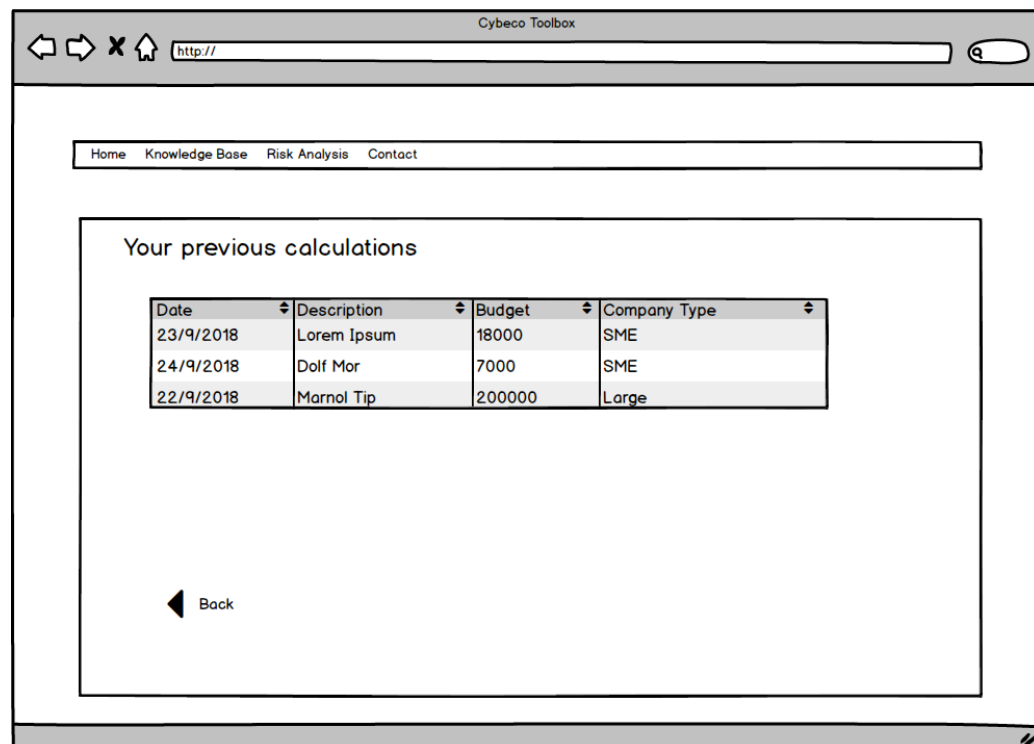


Figure 24: Risk analysis history