Deliverable	**D4.4.2 – CYSPA Risk Tool – final release**
Work package	WP4
Due date	30/03/2015
Submission date	03/04/2015
Revision	V2.00
Status of revision	Final
Responsible partner:	Engineering Ingegneria Informatica S.p.A (ENG)
Contributors:	Visionware ATOS Fraunhofer Corte EOS
Project Number	FP7-ICT-2011-8 / 318355
Project Acronym	CYSPA
Project Title	European Cyber Security Protection Alliance
Start Date of Project	01/10/2012

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

Version history

Rev.	***Date***	***Author***	***Notes***
V1.00	16/03/2015	Engineering	Table of content
V1.01	31/03/2015	Engineering	First draft
V1.02	01/04/2015	Engineering	Overall content review
V1.03	02/04/2015	Engineering	Final review
V2.00	3/04/2015	EOS	Final review and submission

Glossary

Acronym	*Description*
CERTS	Computer Emergency Response Team
CIWIN	Critical Infrastructure Warning Information Network
CRISK	Community-Interaction Risk Self-assessment Tool
CYSPA	European Cyber Security Protection Alliance
DG	Directorate-general of the European Commission
EC	European Commission
ENISA	European Network and Information Security Agency
EOS	European Organisation for Security
EU	European Union
ISP	Internet Service Provider
TLP	Traffic Light Protocol (TLP) (refer to Annex I for more information)
WP	Work Package

Table of contents

Table of figures

Table of tables

Executive summary

CYSPA is an initiative created by 17 partners aiming to create a European Alliance to protect cyberspace for industry [1]. The initiative is currently evolving to become a self-sustained Alliance of organisations interested to reduce the impact that cybercrime has on industry sectors. As an online community, CYSPA launched a campaign called "Understanding Risk". The campaign deals with the importance of cyber risks and possible solutions that may be used to reduce those risks, for organisations running IT assets.

CRISK (the **C**ommunity–Interaction **Risk** Self–assessment Tool) created in the context of the CYSPA initiative is a tool born to support the "Understanding Risk" campaign. With this regard, the tool allows members of the CYSPA community to self-evaluate their risk exposure to the most common cyber threats, as has been identified in the CYSPA impact reports [2][3][4][5]. By filling a questionnaire, specifically tailored to the industry sector organisations operate in, users obtain an assessment of the exposure to cyber risks that their organisation is currently facing. This may improve the respective organisation's awareness of cyber security, while giving the user a holistic overview on threats that may have a major impact on their organisation.

Moreover, in a context where cyber threats and solutions to address them are constantly changing, no organisation has the ability to build and maintain its knowledge across the entire landscape. Therefore, the only possibility for facing issues that constantly arise, is to leverage (by sharing) the collective knowledge of community participants. CRISK has also been conceived to give the CYSPA community participants the possibility to introduce new cyber threats in order to include them in the self-assessment process and provide new input with the aim of improving the questionnaires; they can also report available solutions.

The community interaction is one of the main added values of CRISK. In addition to other considerations introduced in section 2, it is one of the reasons that led to the decision to create a new tool, instead of reusing what is already available in the market…

The risk tool implementation has been scheduled in two phases: the first one ended in November 2014 with a first release that was open to CYSPA partners only while the second one was completed at the end of March and will be made available to the whole CYSPA Alliance via the Community Portal.

This document, as part of the second release of the tool, integrates the content of the first release from D4.4.1 – which presents the CRISK tool logical design and behaviour - including the description of the extensions and improvements applied in the second release of the tool.

1. Introduction

CRISK is an online self-assessment tool that allows users to:

1. Identify threats that may be affecting their organisations;
2. Obtain a risk analysis to self-evaluate their level of exposure;
3. Navigate through a tree of threats collected in D2.4;
4. Interact with the rest of the community and enrich the tool by providing questions, information and references about the threats, solutions that can prevent or mitigate them and reporting new threats by using the community interaction feature.

In order to identify the threats affecting their organisations, users have to answer a series of questions related to the value of their assets to the business and their exposure to known threats. The initial questions are fairly general and answers are not considered as revealing sensitive information; as the questions become more precise in terms of the details of the critical assets to the organisation and which countermeasures are in place, answers can become more sensitive. The decision to answer or to skip a question in more detailed questionnaires is always optional for the user. However, the actual precision of the results provided by CRISK will be linked to the extensiveness with which the user has answered questions.

Once the user has completed and submitted the answers, a qualitative analysis is displayed revealing the relative risk for each threat related to the business in terms of impact and probability of occurrence. This analysis allows the user to identify the threats he should be more concerned about (those with a higher impact or probability) as opposed to those which are not likely to occur or have no serious consequences (low probability or low impact).

This analysis is complemented with information and references about each threat to raise awareness of its impact and explain how important is to prevent or monitor them. One or more solutions, or relevant technologies, may also be proposed for each of the identified threats. Regarding the solutions proposed, the tool will not delve into details of the proposed solutions, but will point to experts in the field and / or tools on the market that can be used in order to mitigate these threats. Solutions are linked to the solutions section in the CYSPA community portal since the 2nd release of this tool.

The community interaction will allow users to share information, including threats, solutions and recommendations that will make the process of mitigating and preventing threats much easier. It will also be an important source of information exchange where users can share questions, and experts within the alliance can provide solutions and suggestions in order to make the tool more complete and accurate. Users will also be able to send feedback to improve the functionality of the tool.

The community interaction of the CRISK tool will also allow users to comment and understand better the results obtained in the analysis, and even skip the risk identification process and find a solution to a specific threat.

This second release of the tool widened its usage to all members of the CYSPA Alliance through its community portal. This way, a larger group of experts rather than only a restricted project partner group, can work together against cyber-attacks and share relevant information and knowledge about cyber security. This document is divided in four main sections:

1. **Introduction**: Short description that briefly explains the main functionalities and provides an overview of the entire process of the tool;
2. **CRISK positioning**: This section explains the stronger points of CRISK and the reason why it was decided to proceed with the development of CRISK and not adopt another tool available in the market;
3. **CRISK design:** Detailed description of the tool's design and all the functionalities available. This section provides a better understanding of all the processes carried out within the tool: behaviour, interface and internal logic. Screenshots have been incorporated in order to help describe all these processes and sections of the tool;
4. **Conclusions:** Description of the benefits of having CRISK as a service in an Alliance such as CYSPA and next steps to follow.

2. CRISK Positioning

This section contains an overview of the risk tools already available on the market and their main features. It also introduces the motivations for the creation of the CRISK tool.

2.1. Existing Risk Tools

Risk management is a process that goes back to the beginning of the computer era (1970s). Modern risk assessment methodologies define risk as "the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation." [11]. To this effect, a process of risk assessment identifies the assets (information resources) that are critical to the organisation, and for each asset what vulnerabilities exist and which threats may use these vulnerabilities to affect the integrity, confidentiality and availability of the asset.

There are many tools available in the market to assist in the risk assessment process, some more sophisticated than others, more efficient, or even more able to carry out the risk analysis processes. The number of tools available is rapidly increasing nowadays, mainly because organisations are now working in a hyper connected world that makes the exposure of risks more difficult to understand and mitigate.

The CYSPA project carried out extensive research in identifying and analysing a number of existing tools for risk analysis. The most interesting ones (in relation to CYSPA purposes and activities) are briefly introduced in the list below.

- "**Enterprise Risk Management**" developed by the University of California.

  This tool will help to consider the factors affecting the risks faced by an organisation. The factors considered are:
  - Event likelihood;
  - Time to impact;
  - Financial severity;
  - Injury severity;
  - Reputational impact severity.

The tool will prompt organisations to list potential risk events which may impact them and describe the controls the organisation has put in place in order to manage or mitigate those risks.

The purpose of this tool is not to ensure all risks are rated as "Adequately Controlled" but rather to help departments assess their control structure for sufficiency given their environment, resources, and bandwidth. This tool will help organise organisations thinking while considering the organisation's risk profile and related enterprise risk management implications.

For further information about this tool please refer to:

- http://www.ucop.edu/enterprise-risk-management/tools-templates/risk-assessment-toolbox-content/risk-ranking-tool.html

- The company MITRE developed three tools:

    1. "**RiskNav**" is a tool to facilitate the risk process and help program managers handle their risk information in a collaborative manner. This tool provides three dimensions of information graphically: risk priority, probability and mitigation/management status.
       RiskNav, originally produced for the U.S. government, is designed to capture, analyse, and display risks at a project or enterprise level.

       For further information about this tool please refer to:
        - http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools

    2. "**RiskMatrix**" is a software application that can help identify, prioritize, and manage key risks on a program. MITRE created this applicationt a few years ago, with the aim of supporting risk assessment processes developed by a MITRE DoD client. MITRE and the client have expanded and improved the original process, creating the Baseline Risk Assessment Process. Although the process and application were developed for use by a specific client, these principles can be applied to most government acquisition projects.

       For further information about this tool please refer to:
        - http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools

    3. "**RiskRadar**" is a risk management database to help project managers identify, prioritise, and communicate project risks in a flexible and easy-to-use form. Risk Radar provides standard database functions to add and delete risks, as well as specialised functions for prioritizing and retiring project risks. Each risk can have a user-defined risk management plan and a log of historical events.

       A set of standard short- and long-form reports can be easily generated to share project risk information with all members of the development team. The number of risks in each probability/impact category by time frame can be displayed, which allows the user to drill down through the data to uncover increasing levels of detail.
       Risk Radar allows the user with the flexibility of automatically sorting in addition to manually moving risks up and down in setting priority rank.

       For further information about this tool please refer to:
        - http://www2.mitre.org/work/sepo/toolkits/risk/ToolsTechniques/RiskRadar.html

- "**OpenPages software**" developed by IBM enable customers to manage risk and compliance initiatives across the enterprise, helping businesses to reduce loss, improve decision-making in regards to resource allocation and optimises business performance.
  The IBM OpenPages GRC Platform allows organisation to:

  - Integrate risk management processes across the enterprise;
  - Manage risk and compliance across multiple regulations, including Basel II, Solvency II, SOX and SOX-like requirements, financial reporting, data privacy, industry regulations, and more;
  - Leverage GRC information to make better business decisions;
  - Empower decision makers with fully scalable and interactive reporting and trending tools.

  For further information about this tool please refer to:
  - http://www-01.ibm.com/software/analytics/openpages/

- "**RM Studio**" RM Studio software is the dynamic solution combining risk management and business continuity management into one, easy to use software application. You can use RM Studio to simplify operational risk management or implement a strategic ISMS governed through a framework for implementing risk management procedures and outlining business continuity recovery planning.

  RM Studio is a turnkey application with time saving technology features, built in and many customisation options that will meet the unique needs of an organisation. RM Studio is used by organisations of all types on a global scale to implement effective ERM strategies.
  Features:

  - Risk assessment;
  - Risk treatment;
  - Gap analysis;
  - Business continuity management.

  For further information about this tool please refer to:
  - http://www.riskmanagementstudio.com/features

- "**BSI Entropy Software**" BSI Entropy Software provides a management solution that significantly reduces the cost and effort needed to proactively manage risk, performance and sustainability activities.

  Entropy Software provides a number of powerful features that drive continual business improvement throughout an organisation.
  Entropy Software is composed of five key modules, which function independently or as a whole to help organisations effectively manage business challenges around the areas of:

  - Audit & Compliance Management;

- Incident Management;
- Performance Management;
- Risk Management;
- Knowledge Management.

For further information about this tool please refer to:

- http://www.bsi-entropy.com/
- http://www.bsi-entropy.com/explore-entropy/modules/risk-management/

- "**AlienVault Unified Security Management™**" developed by Alien Vault is an all-in-one platform that provides:

  - Unified, Coordinated Security Monitoring;
  - Simple Security Event Management and Reporting;
  - Continuous Threat Intelligence;
  - Fast Deployment;
  - Multiple Security Functions without Multiple Consoles.

  This tool also provides a threat reporting system similar to the Community Interaction but it does not improve the tool in any case.

  With AlienVault USM for threat management, you can:

  - Identify, isolate, and investigate indicators of exposure (IOEs) and indicators of compromise (IOCs);
  - Correlate asset information with built-in vulnerability scan data and AlienVault Labs Threat Intelligence to better prioritise response efforts;
  - Respond to emerging threats with detailed, customized "how to" guidance for each alert;
  - Validate that existing security controls are functioning as expected;
  - Demonstrate to auditors and management that your incident response program is robust and reliable.

  For further information about this tool please refer to:

  - https://www.alienvault.com/products
  - https://www.alienvault.com/open-threat-exchange

- "**The Cyber Security Evaluation Tool** (CSET®)" developed by The Department of Homeland Security's is a desktop software tool that provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system networks. CSET guides users through a step-by-step process to assess their control system and information technology network security practices against recognised industry standards. CSET helps asset owners to assess their information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architecture,

as well as operational policies and procedures. These questions are derived from accepted industry cybersecurity standards. Once the self-assessment questionnaire is complete, CSET provides a prioritized list of recommendations for increasing cybersecurity posture, including solutions, common practices, compensating actions, and component enhancements or additions. The tool also identifies what is needed to achieve a desired level of cybersecurity within a system's specific configurations.

Key Benefits:

- CSET contributes to an organisation's risk management and decision-making process;
- Raises awareness and facilitates discussion on cybersecurity within the organisation;
- Highlights vulnerabilities in the organisation's systems and provides recommendations on ways to address the vulnerability;
- Identifies areas of strength and best practices being followed in the organisation;
- Provides a method to systematically compare and monitor improvement in the cyber systems;
- Provides a common industry-wide tool for assessing cyber systems.

For further information about this tool please refer to:

- https://ics-cert.us-cert.gov/Assessments

- "v**sRisk**" developed by Standalone – Basic. The vsRisk version 2:

  - Automates and delivers an ISO/IEC 27001-compliant information security risk assessment;
  - Simplifies and accelerates the risk assessment with an intuitive risk assessment process;
  - Provides a set of 3 different pre-populated controls: ISO/IEC 27001:2005, ISO/IEC 27001:2013 and ISO/IEC 27032:2012;
  - Assess confidentiality, integrity and availability (CIA) for business, legal and contractual requirements.
  - Produces a set of exportable, reusable and audit-ready ISO 27001-compliant documents;
  - Link and track controls back to specific documents to record implementation details;
  - Customisable assessment scales and risk assessment criteria;
  - Features a backup and restore functionality;
  - Includes a detailed user manual to take you step-by-step through the process.

  The vsRisk version 2.3 has new additions:

  - Fully compatible with ISO/IEC 27001:2013;
  - Offers the choice of applying either a scenario-based or asset-based assessment methodology;
  - Includes an integrated, searchable ISO 27005-compliant threat and vulnerability database as well as a database of common risk scenarios;
  - Supports the option to add additional, customised risks and controls;

- Create views and categories based on risks, owners, assets or customised company groups, in addition to sub-groups;
- Includes the option to conduct assessments on multiple, different information security management systems (ISMSs), i.e. across different companies and geographic locations;
- Additional ISMSs are available to purchase;
- Easily switch between multiple ISMSs from a single tool;
- Offers suggestions intuitively about relevant controls for specific threats and vulnerabilities.

Includes a conversion tool for current vsRisk users, which helps to quickly map existing controls based on ISO27001:2005 to ISO27001:2013 controls.

For further information about this tool please refer to:
http://www.itgovernance.co.uk/shop/p-1228-vsrisk-standalone-basic.aspx#.VLAN2iuG-aq

- **"CoAble"** developed by CoBlue, is a benchmark tool, and related platform, for assessment of the compliance of your organisation with a number of ISO security-related standards.

"Cybersecurity is a challenge in all sorts of industries. A collective effort can truly improve cybersecurity on an organisation, national and international level. Coblue has developed Coable to facilitate this collaboration: Coable is a benchmark and collaboration platform which helps organisations to assess and improve their cybersecurity by facilitating inter-organizsational benchmarks and knowledge exchange. Information is kept confidential throughout this process." [9]. Main features of the CoAble tool include:

- Assess your whole organisation in detail;
- See your progress over time;
- Benchmark with peers anonymously;
- Learn from the knowledge base;
- Create flexible reporting;
- Collaborate with or delegate to colleagues - increase user awareness.

For further information about this tool please refer to:
- http://www.coable.eu/

2.2. Motivations for the CRISK Tool

The analysis of the tools listed in the previous section shows that most of them are not targeting a specific sector and are in fact general enough to apply to any kind of organisation. While this is good from a marketing point of view because it benefits tool creators (or vendors); it is not ideal for the tool users that need to customise (or setup) the tool for a specific sector or use cases.

Furthermore, the analysis of existing tools reveals that in many of them it is necessary to know the threats affecting an organisation and input the information in order to get an analysis and further evaluate the level of exposure. This is a common limitation in the usage of such tools; the

tool itself should identify the threats the organisation could be exposed to. This is also connected to the fact that the settings needed to get the tool working properly and the findings with regards to improving tool accuracy, usually remains within the boundaries of each organisation as internal knowledge. This furthers duplicating of efforts related to discovery of threats, and calculation of exposure.

Starting from the abovementioned considerations, the CYSPA consortium decided to elaborate a different risk self-assessment tool aiming at addressing the issues identified from the analysis.

Essentially, the CRISK tool should provide organisations – especially SMEs that typically do not have a Security Manager or a Risk Expert on board – with a tool to conduct a first cybersecurity self-assessment and get a rough estimation about the exposure of the organisation to most common threats. The CRISK tool should:

- Suggest the threats an organisation could be exposed to, based on high-level information about its processes and sector;
- Allow members of the CYSPA community to exchange information about common threats thus enriching the knowledge base of each participant, and refine the behavior of the CRISK tool. This is called “Community Interaction”, in the context of CRISK.

To start this process, we can rely on the support of four sector leaders (for eGovernment, Energy, Finance and Transport sectors) that have provided initial knowledge and content so users can obtain a first evaluation without having to know or input the existing threats that could affect organisations’ operations in those sectors.

3. CRISK Design

3.1. Tool Behaviour

CRISK is built upon three main sections as we can see in the functional navigation map represented below:

1. Tree of Threats;
2. Questionnaires and Risk Assessment;
3. Community interaction:
    a. Propose question
    b. Report Threat

Each of these sections is necessary to help CRISK achieve its primary goal: allow members of the Alliance to self-evaluate their organisations and increase the level of awareness about existing threats that may be affecting them.

Threats

All the existing and identified threats that can be displayed in the analysis are gathered in this section, so users can have an overview of the actual cyber threat situation. Furthermore, they are able to navigate through the tree in order to learn more about these threats, even if those have not been identified as potentially impacting user's organisation during the analysis. For each threat, a list of available solutions is displayed based on the suggestions of the community of experts. Furthermore, users can easily interact, as explained more in details in the next section, through 'OPENNESS' [13] social bar. This toolbar is located the bottom of each threat description allowing users to comment and rate the threat as well as subscribe to the specific threat in order to be promptly updated whenever important changes are applied to it .

Questionnaires

CYSPA operates mainly in four different sectors: transport, energy, e-Government and finance. The CYSPA alliance has the opportunity to count with members from organisations that play an important role in each of these sectors and that can support the rest of the community by providing knowledge, while reporting new threats appearing in their sectors. Based on their expertise and knowledge CRISK has been populated with different types of questionnaires, targeting each of the sectors above, so all expert and non-expert members of the alliance can self-evaluate their organisations. Each of the questionnaires is composed by a certain number of (multiple choice) questions to address existing threats (among those included in the Tree of Threats, see below) and evaluate likelihood and impact of these threats on organisations of a given sector. Questionnaires have been developed by using the impacts reports (D2.1.1-D2.1.4) [2][3][4][5] delivered in the context of work package 2 of the CYSPA project.

A mapping that links each question with corresponding threats and each answer with a value that is used in the risk analysis has been also developed (for more detailed info please refer to section 4.3 Logic of the tool). Once the user has answered and submitted the questionnaire, the risk analysis is displayed, containing all the identified threats represented in a two dimensional graph. Impact and likelihood are represented on graph axis, both within the same range -zero to five- zero being the minimal impact and likelihood and five the maximum. For each of the identified

threat, a threat detail is also presented. The detail contains relevant information and references to increase the awareness and knowledge of the user about the related threat.

Community interaction

This section allows members of the Alliance that are using the tool to share information about new and existing threats as well as related solutions (considering an initial solutions and threats collection performed in *D3.6.2 – Solutions and Threats dataset* [10]). Also suggestions on new questions can be included in the tool, thus increasing awareness and knowledge that community participants have with respect to cybersecurity topics.

The following figure introduces the functional navigation map of the CRISK tool. Boxes in the different sections represent the different views of the tool's interface, while the arrows represent the user actions navigate among different views. Back paths (paths that allow the user to go back from one section to the previous one) are enabled in the tool but they have not been presented in the diagram as arrows in order to make it more readable. Main elements of the map are available and will be explained (with relevant screenshots) in the following sections.

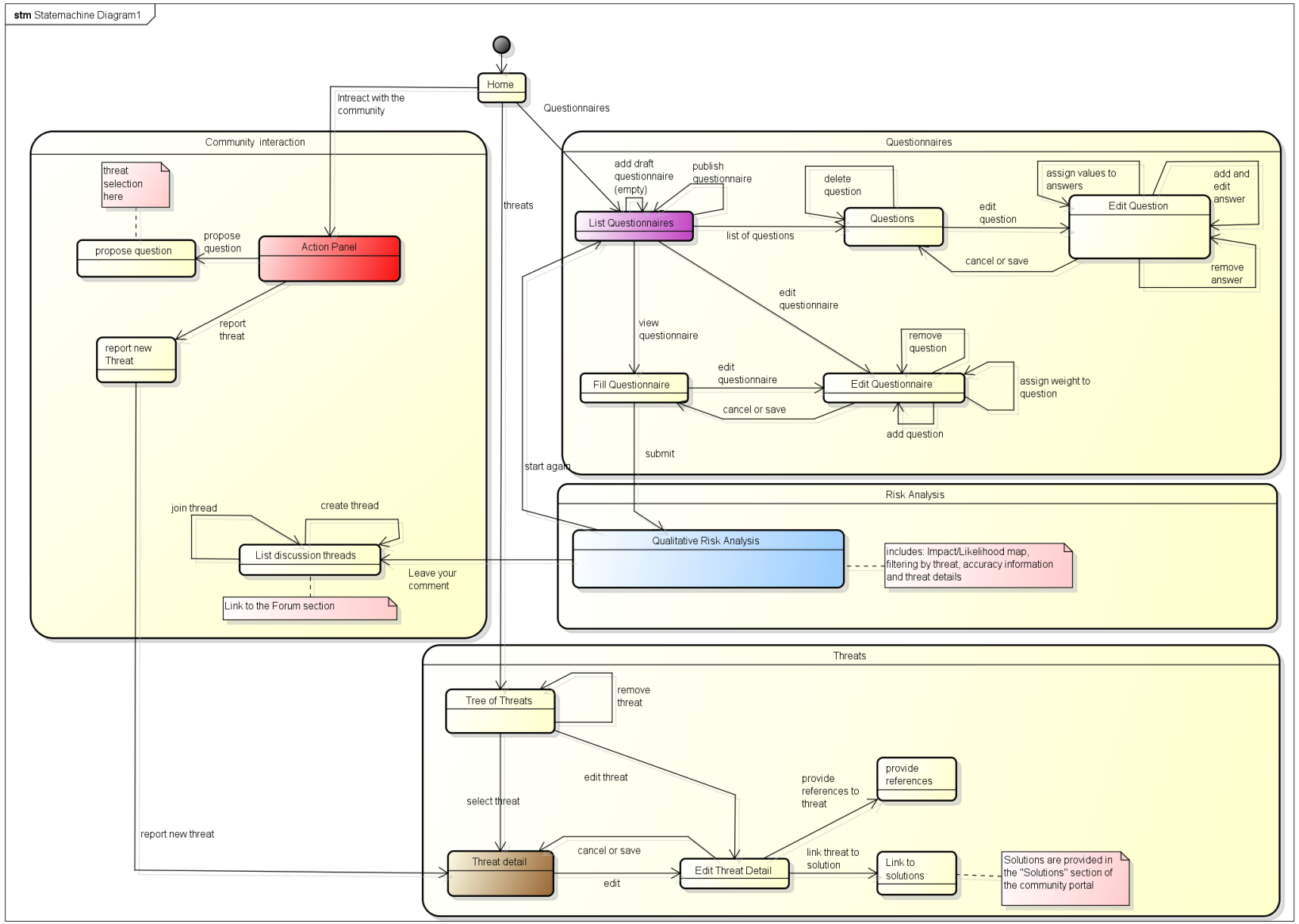

Figure 1 – Functional Navigation Map

3.2. Tool Interface

In this section some screenshots are presented, showing each of the sections of the tool.

Home

As mentioned (in section 3.1), the tool is built upon three main sections and those are exactly the three options that a user has in the welcome page:

- **Tree of Threats;**
- **Questionnaires (and Risk Assessment);**
- **Community interaction.**

Furthermore, since CRISK is integrated with the CYSPA community portal, it can benefits and add value to its functionalities with links to and from portal sections such as the "**Cyber Reference**" section, and the "**Solutions**" section. In particular, "Cyber Reference" can help to raise knowledge and thus awareness about cyber threats, as shown in the screenshots below. On the other hand, in the "Solutions" section, specific solutions to cyber threats, also related to a defined sector, a particular threat, or to a specific purpose, can be consulted and/or proposed. Thereby, CRISK can suggest to users, for each completed risk analysis, appropriate solutions to mitigate the identified threats (as they are linked to solutions), taking advantage of the solutions collected, categorised, and approved, through the community portal.

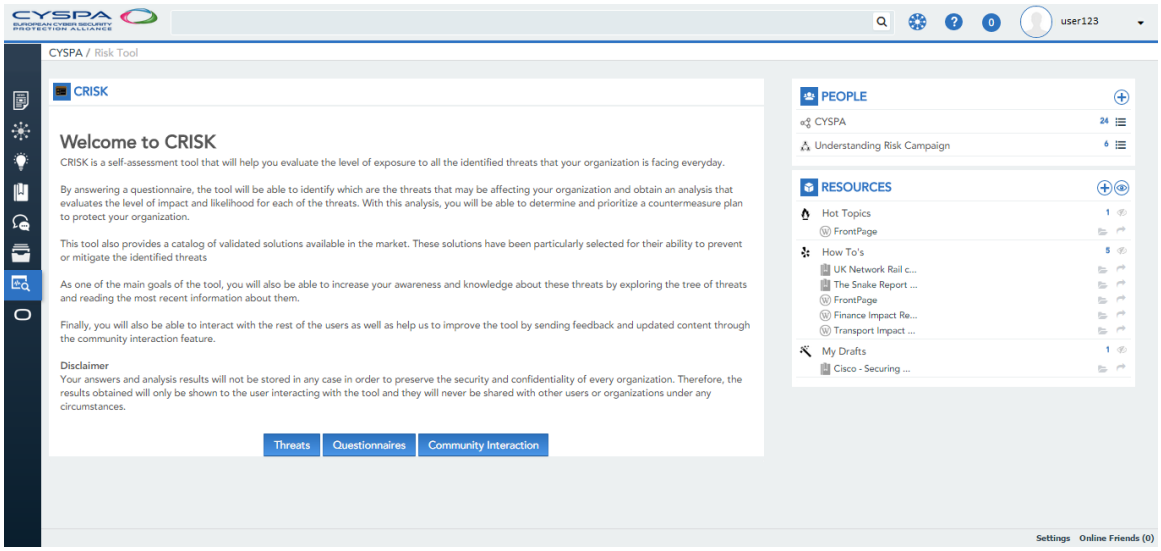

Figure 2 – CRISK home

Threats

The following screenshot represents the tree that gathers and structures all identified threats reported in D2.4. This layout displays all the threats in a hierarchy, also allowing to incorporate new reported threats as sub-threats that could be the topic of a more specific analysis (with dedicated questionnaires):

On the right of the threats tree, a detailed description is depicted contextually for each selected threat, as well as the related solutions that have been previously validated from the community of experts.

The bottom part of the following screenshot also shows the OPENNESS [13] social bar, enabling users to keep track of a threat by following it; it also allows addition of personal comments and notifies other members of the community in regards to the threat.

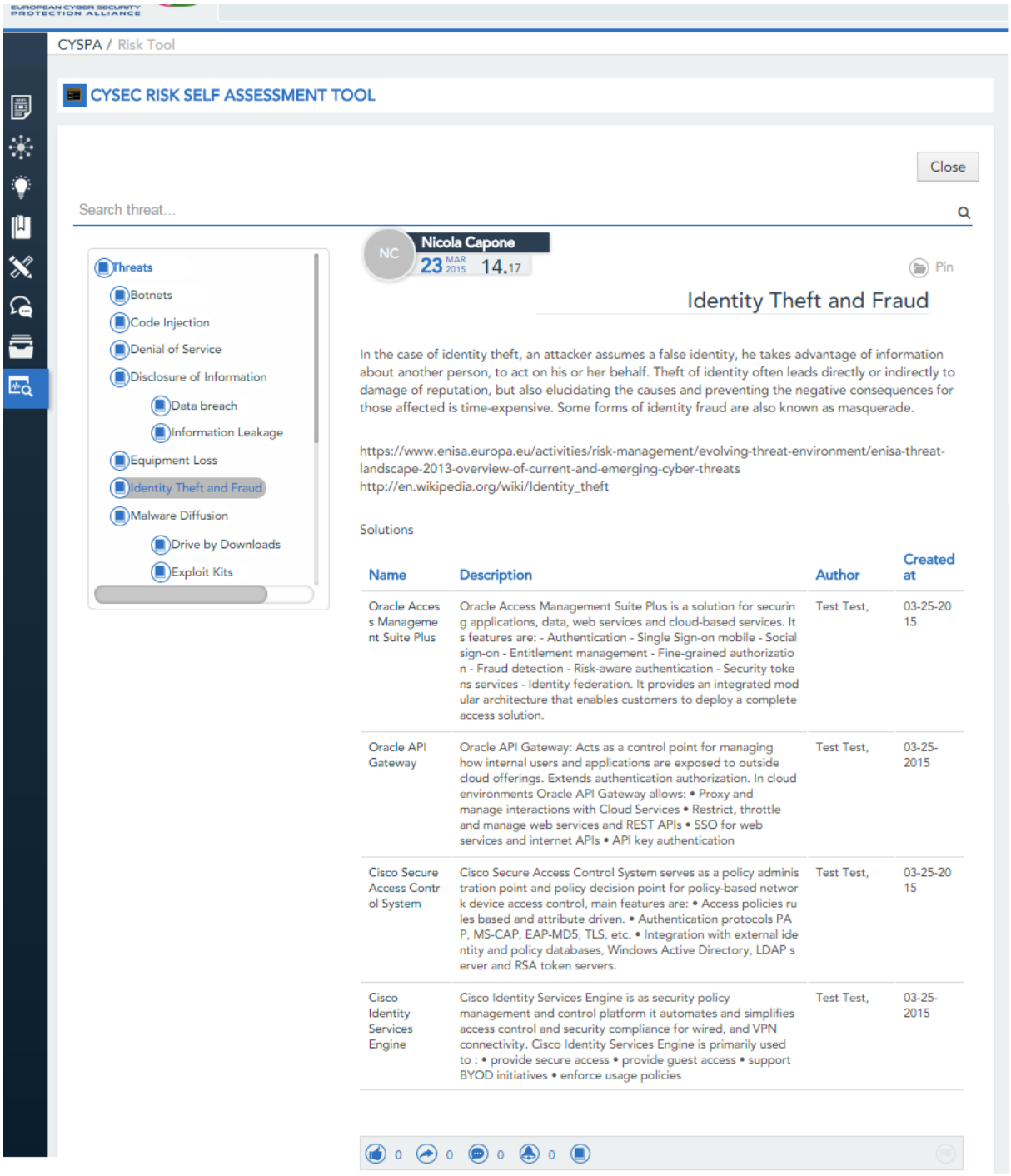

Figure 3 – Tree of threats

Questionnaires and Risk Assessment

In this section, a list of questionnaires is presented to the users so they can choose the most suitable one depending on the sector or type of self-evaluation process they would like to conduct.

Since this second release of CRISK, all the sector related questionnaires have been completed with the support of each specific expert partner of the project. In the following screenshots there are excerpts from four different questionnaires that represent each of the mentioned sectors that CYSPA has been involved with.

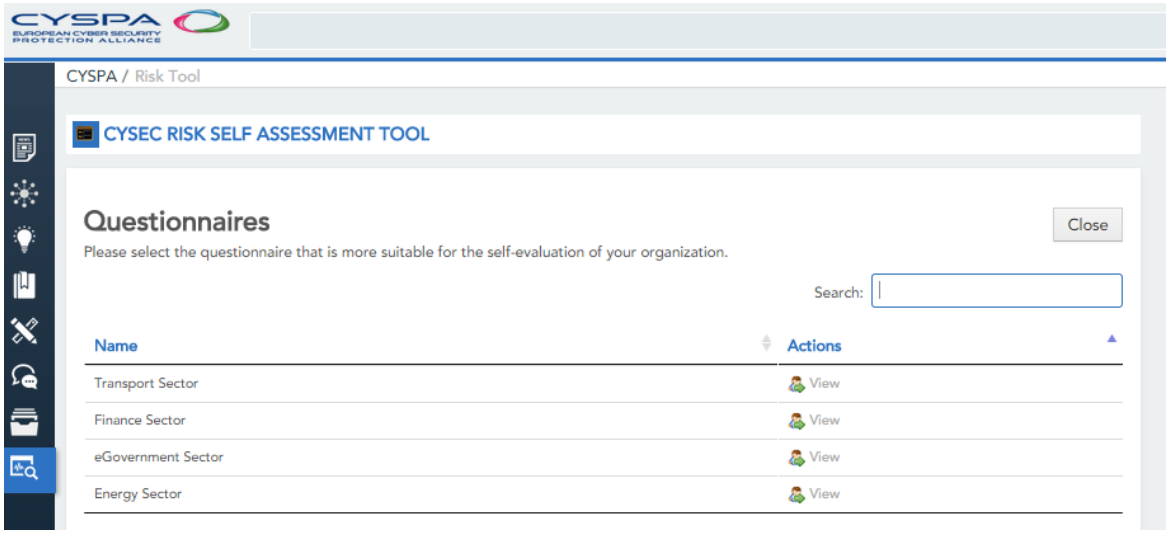

Figure 4 – Set of questionnaires

After choosing one, all the (multiple choice) questions are displayed, as shown in the next screenshots for each sector respectively:

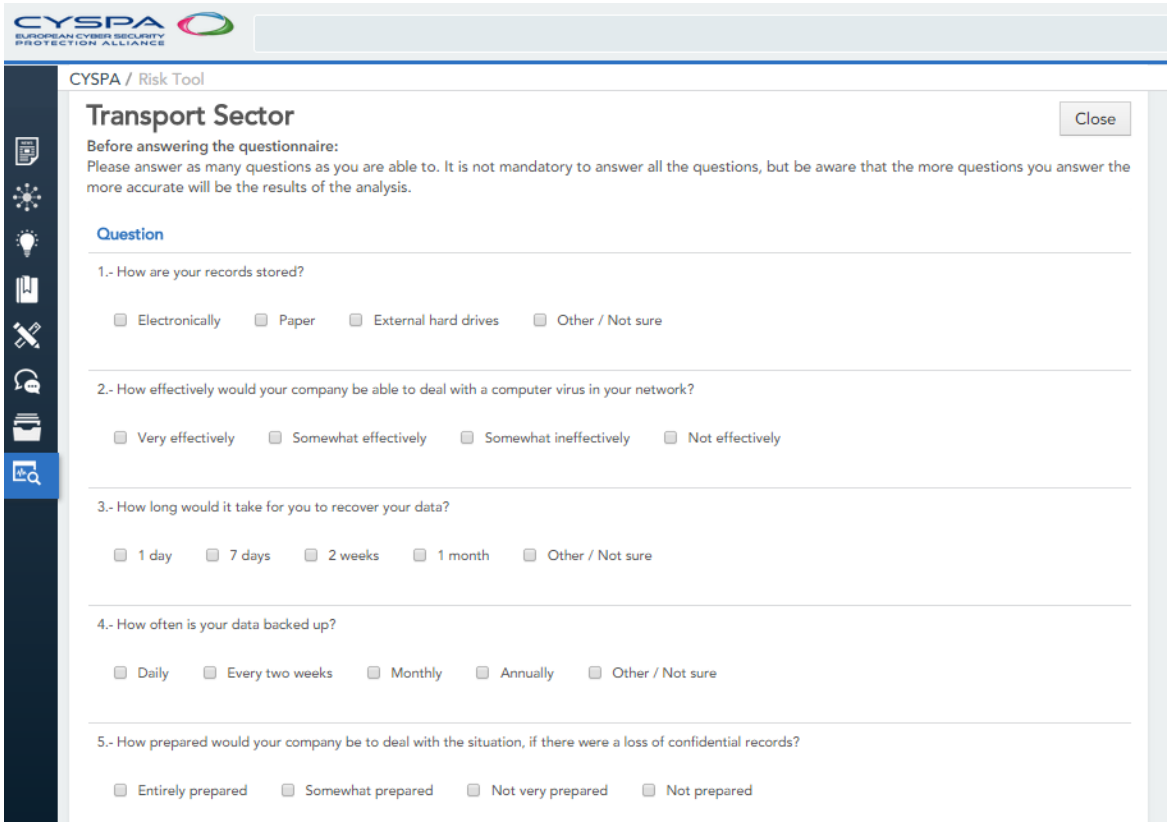

Figure 5 –Transport sector questionnaire

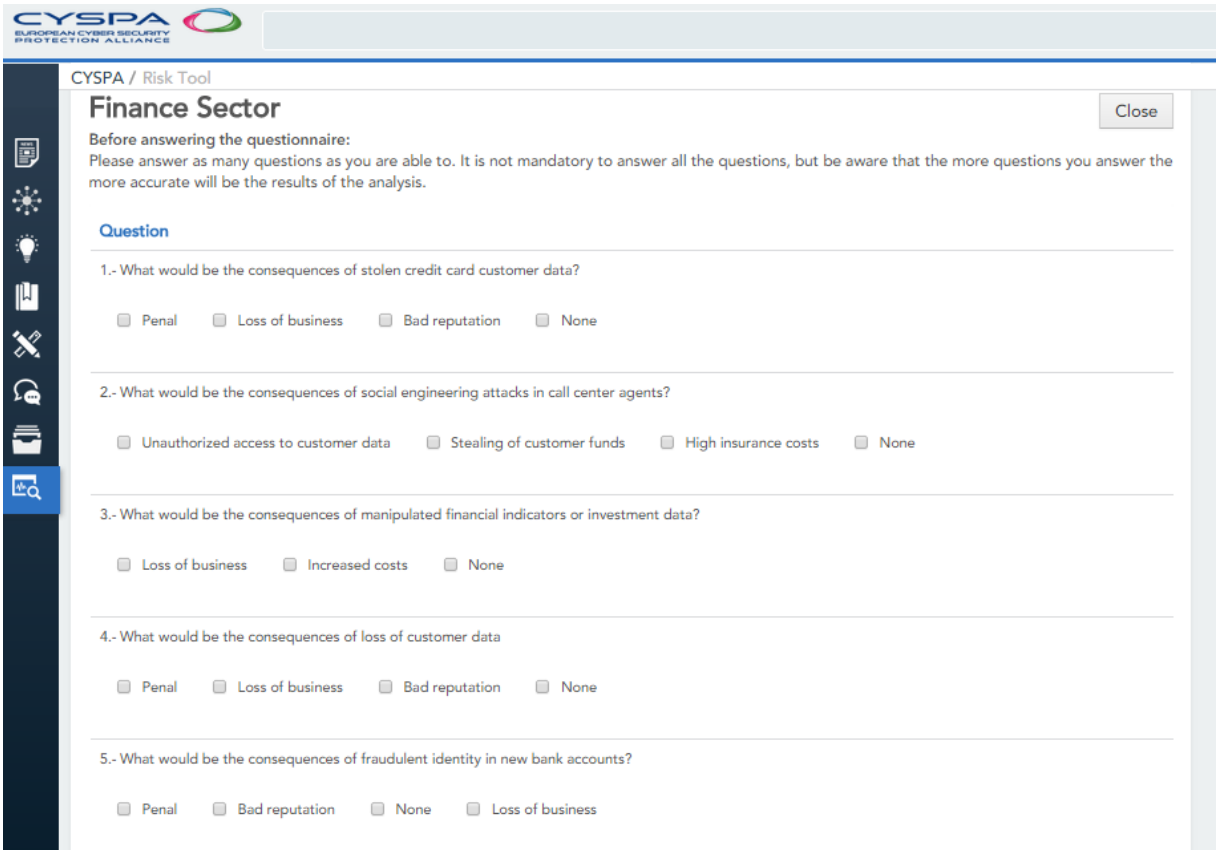

Figure 6 – Finance sector questionnaire

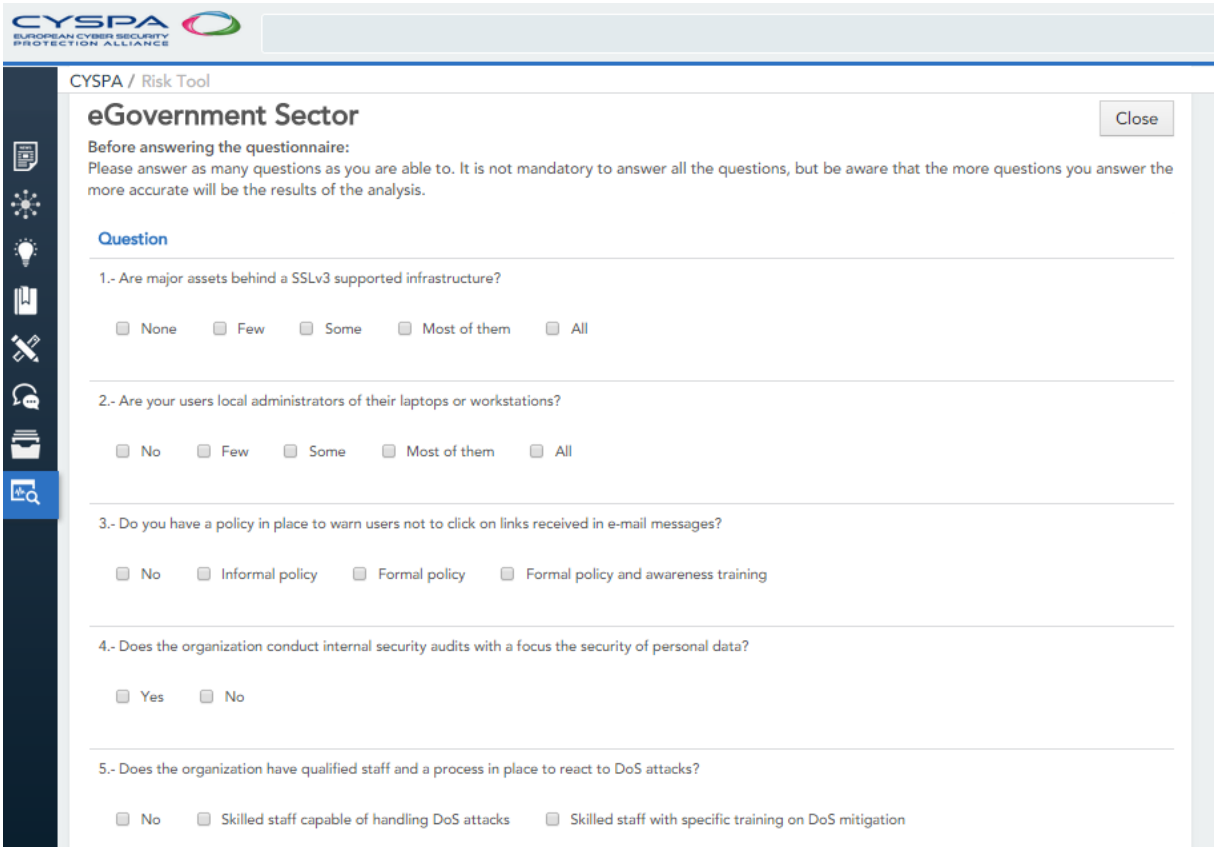

Figure 7 –e-Government sector questionnaire

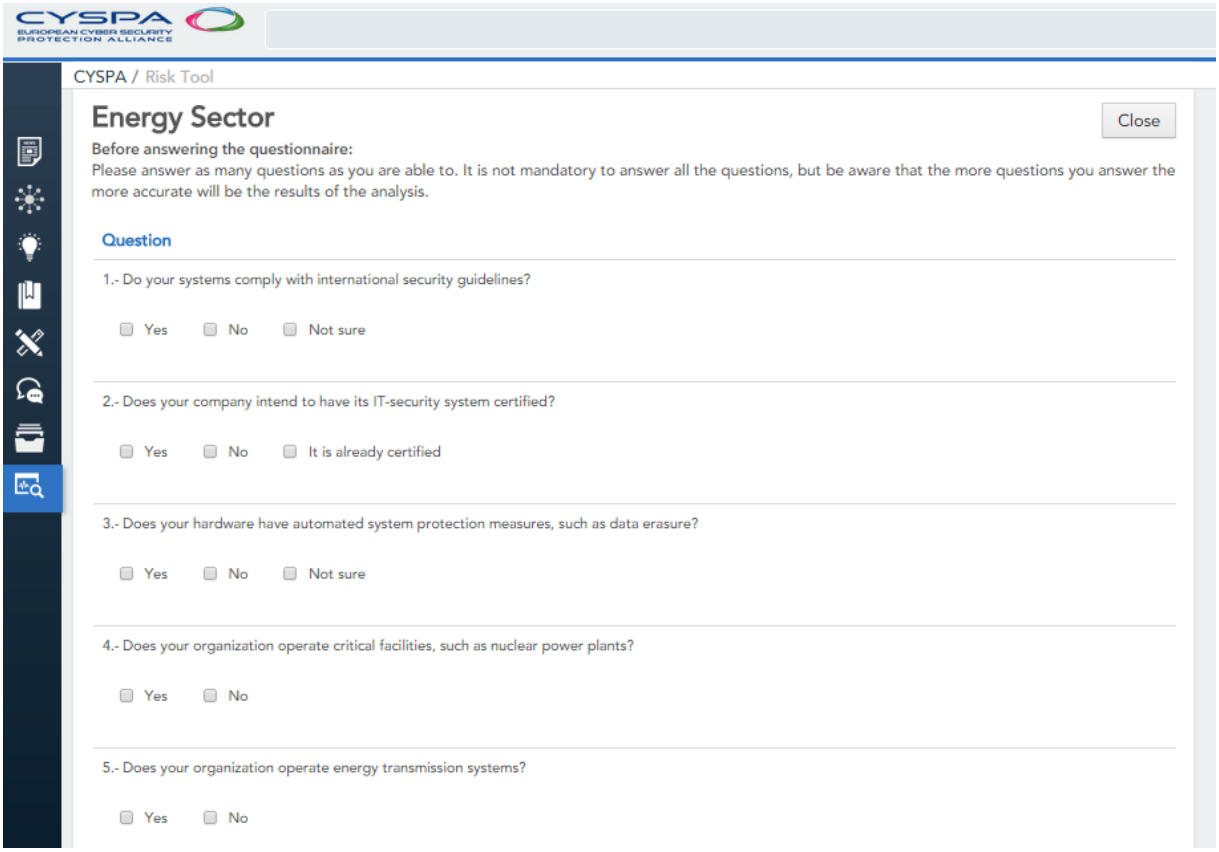

Figure 8 – Energy sector questionnaire

At the end of each questionnaire, as shown in the next screenshot, participants can 'Submit' their answers; thereafter, the risk analysis processing begins:

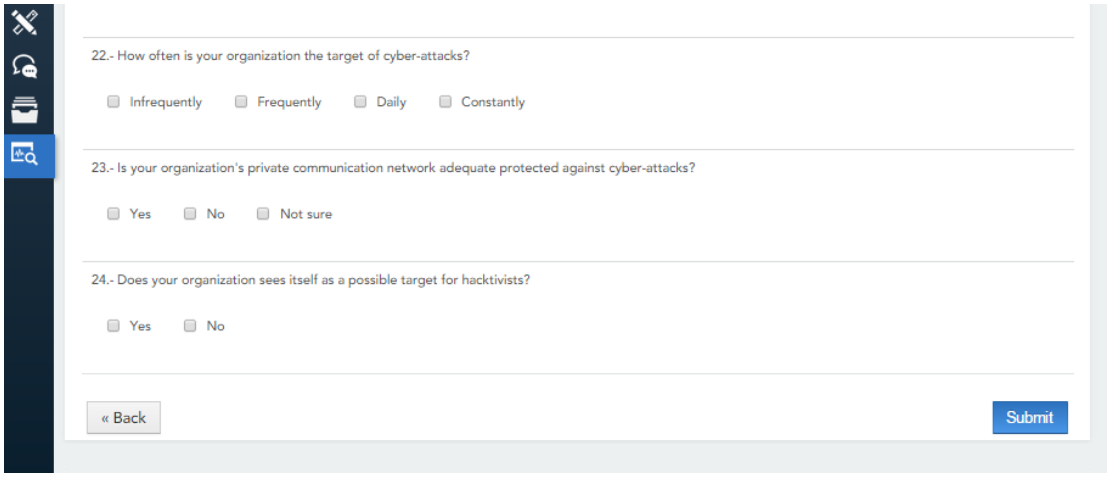

Figure 9 – Submit a questionnaire

Once all the answers have been processed and evaluated according to the internal logic of the tool (see section 0) the analysis is presented to the user as follows:

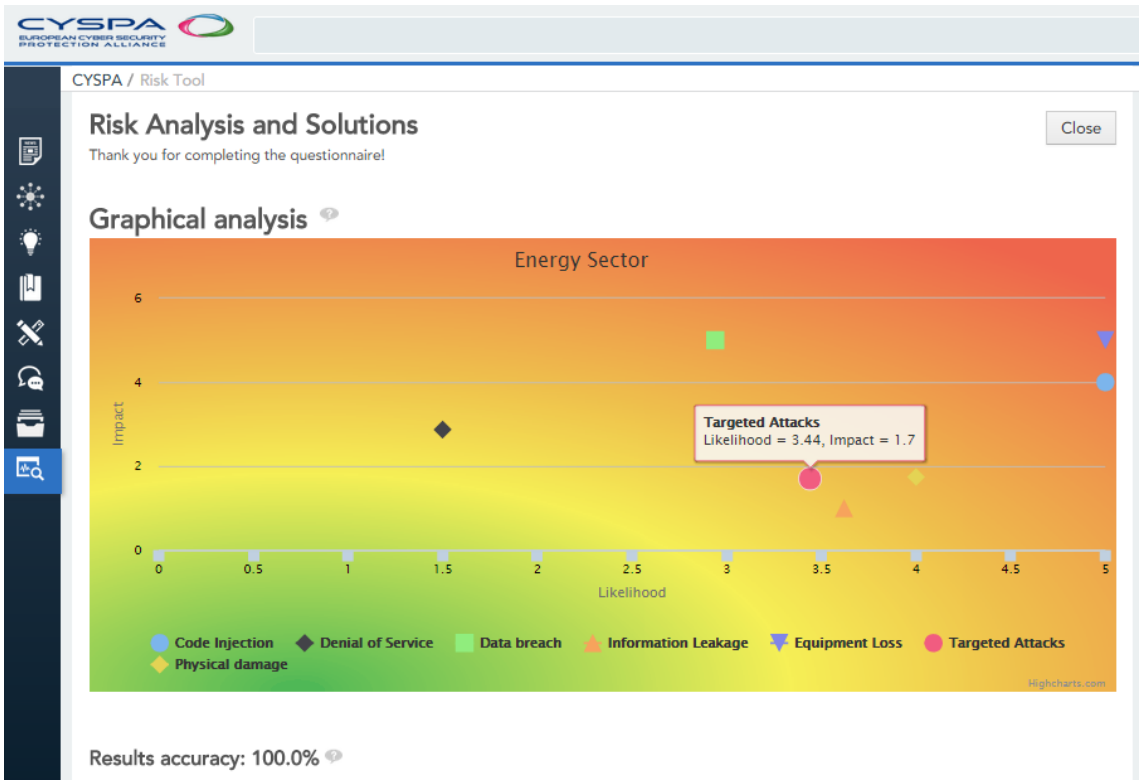

Figure 10 – Graphical analysis

The vertical axis corresponds to impact and the horizontal to likelihood. As we can see the maximum values are five and the minimum is zero for both dimensions. Just below the chart the info and references for each of the threats identified in the analysis is displayed:

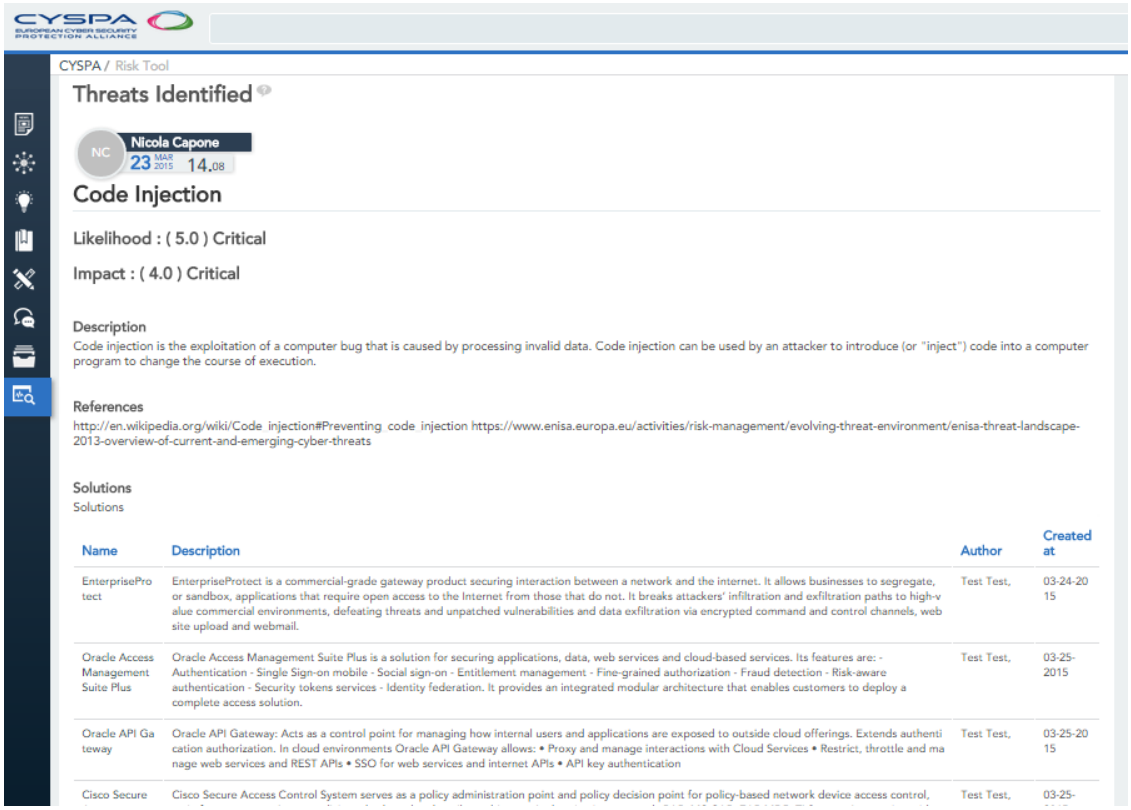

Figure 11 – Information and references of the risk analysis

Community interaction

This section allows, as in the previous version of the tool, to propose new questions or report new threats.

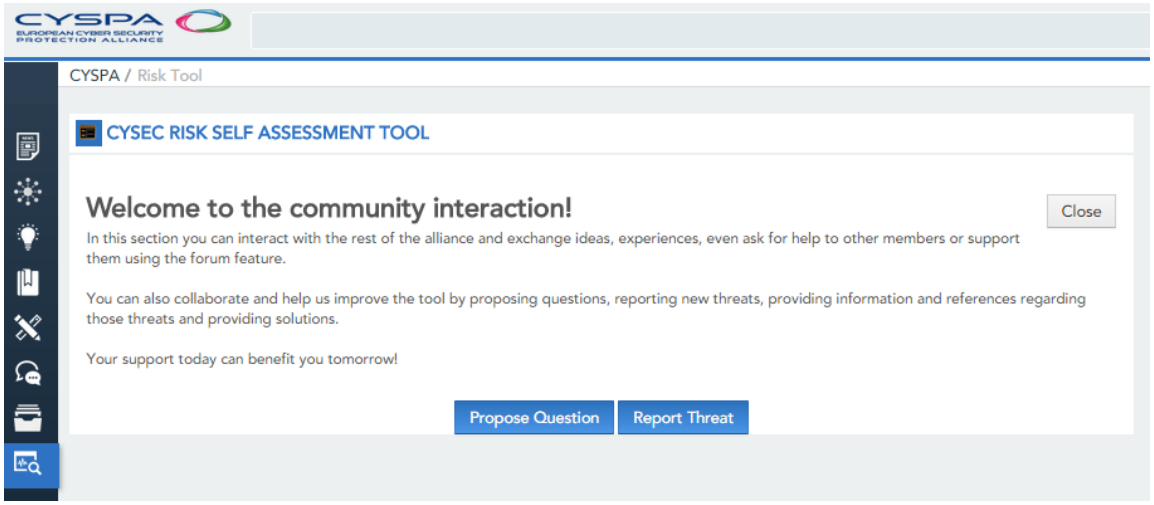

Figure 12 – Community Interaction home

In the following screenshots we can see how the process of reporting new threats and proposing new questions works. In order to propose a new question it is necessary to select whether the questions refers to impact or likelihood, write the actual question, add the relevant answers and select the threats that this questions is related to:

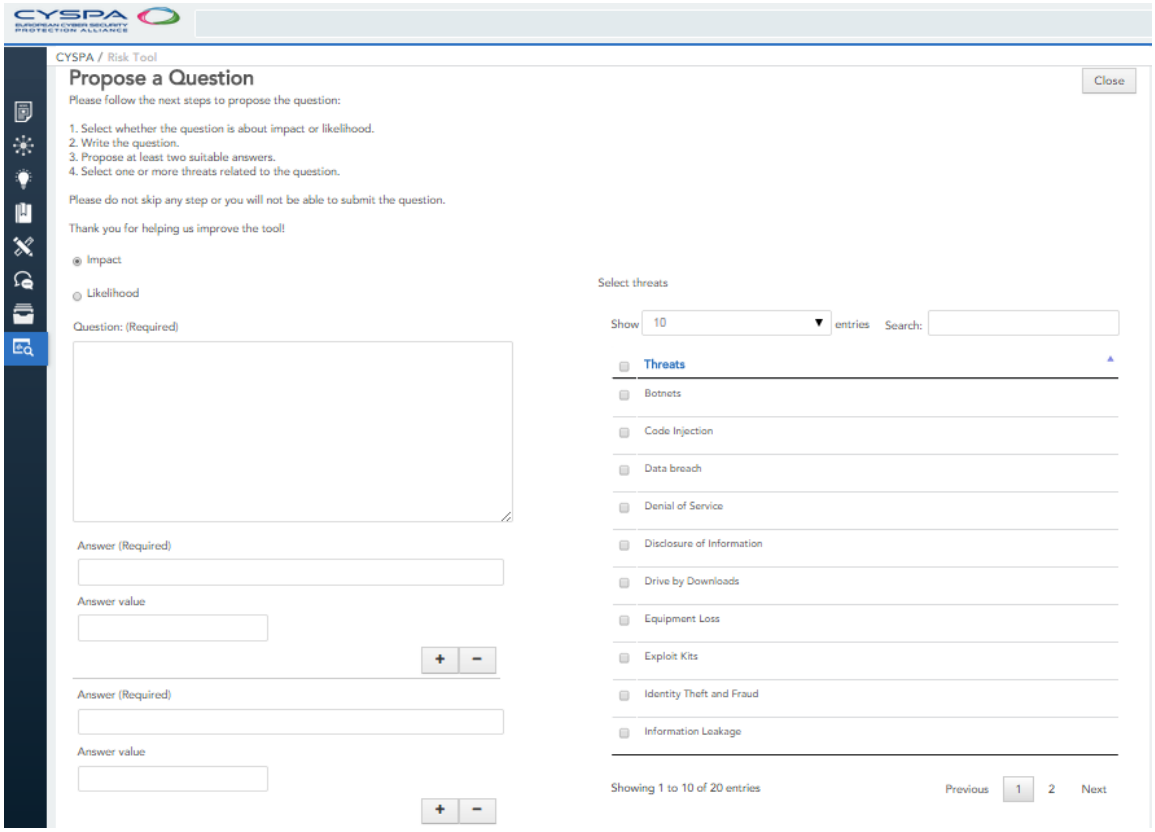

Figure 13 – Propose questions

Reporting new threats is also easy, it is only necessary to perform the following five steps:

1. To write the actual threat name;
2. To include a short description of the threat;
3. To add some working references;
4. To select possible existing solutions by choosing the most suitable ones from a prefilled list;
5. To select whether it is a sub-threat of another threat.

The mask to report a new threat is displayed in the following screenshot:

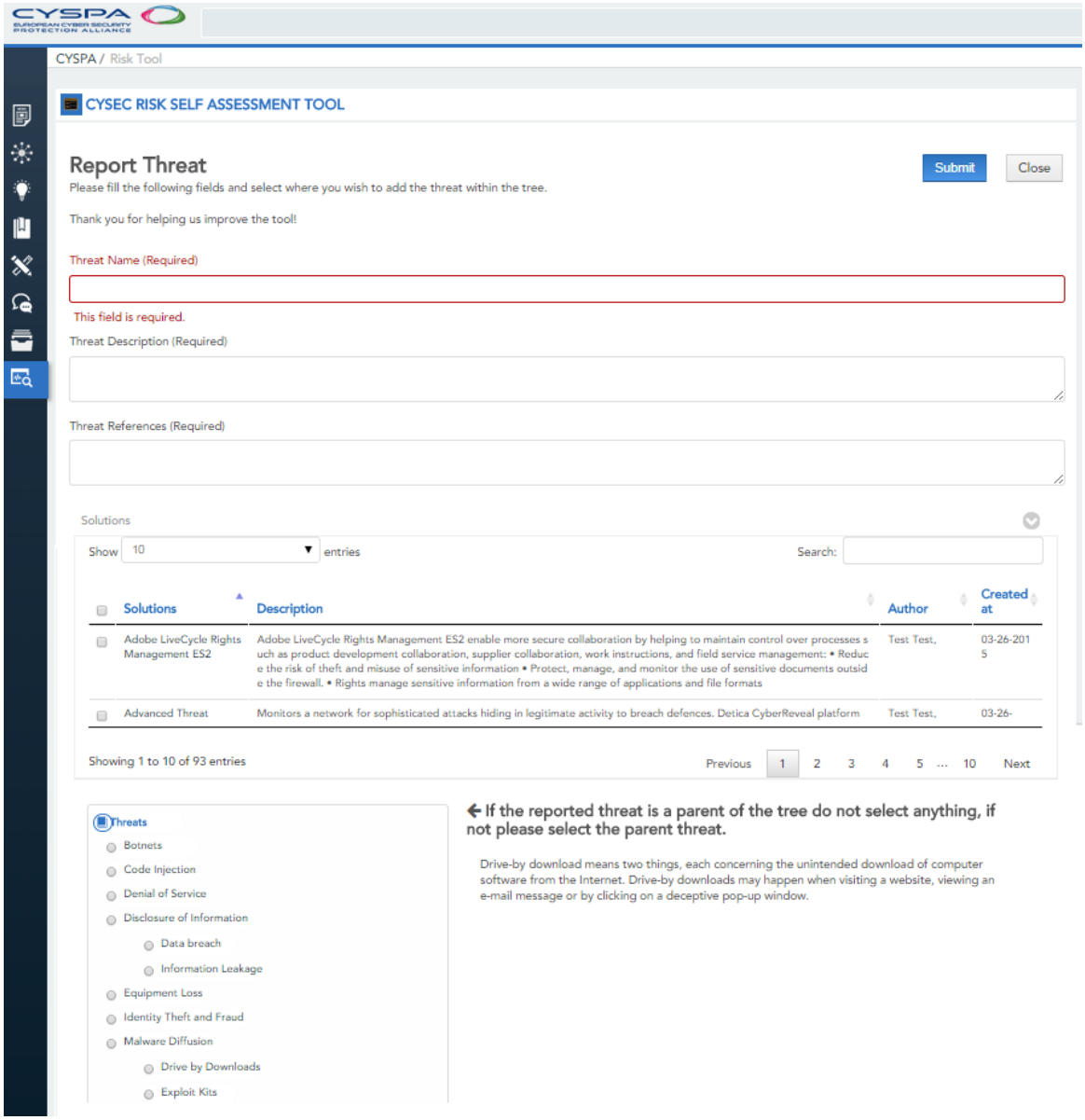

Figure 14 – Report new threats

As previously introduced, solutions to specific threats can be proposed and submitted by any member of the community and then approved from the experts of the same community through the approval process implemented in the portal itself. Once a request for the inclusion of a new solution is received (or a request for modification of an existing one), the experts in the portal are notified by email. Experts can then review the request, approve, reject or apply modifications to information about existing solutions.

The following screenshot (taken from the solutions section) shows how they can be searched for by using filtering criteria or text search (yellow circles). In the same screenshot, the create button (red circle) is also shown, with which users can propose new solutions and associate them to any specific threats. Further details about the "Solutions" submission process and behaviour are available in deliverable 3.6.2.

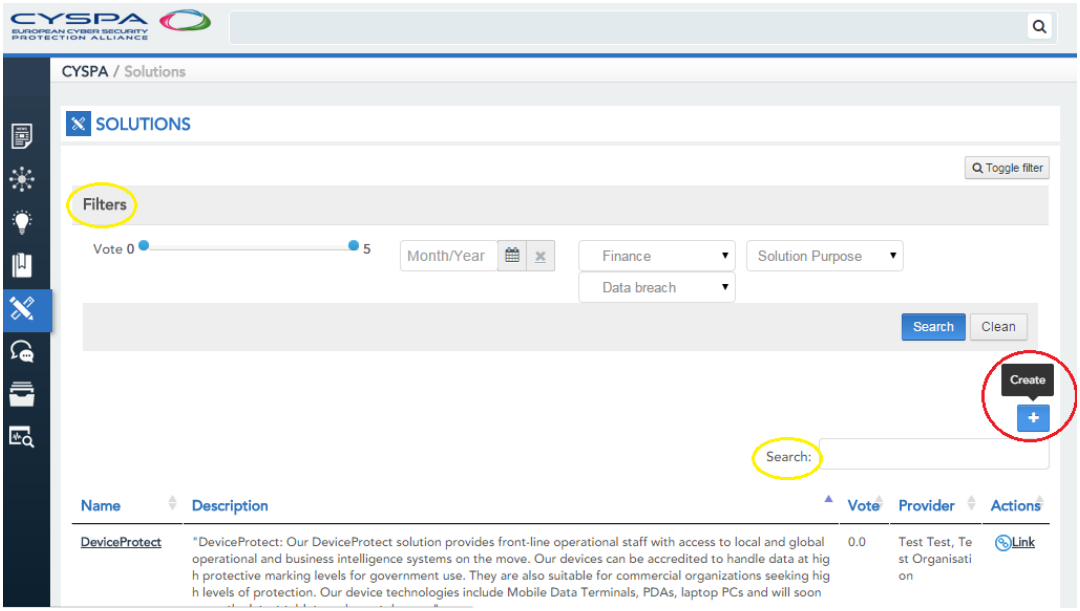

Figure 15 – Solutions search & create

3.3. Tool Internal Logic

The PMBOK [12] defines qualitative risk analysis as "the process of prioritising risks for further analysis or action by assessing and combining their probability of occurrence and impact". CRISK helps in carrying out this process using answers provided by users through the questionnaires. In order to convert these answers into final values of impact and likelihood for each of the identified threats, the tool must follow a specific process with several stages.

The seven main stages of each risk analysis are:

1. Answer the questionnaire and save the answers;
2. Classify questions per threat;
3. Classify questions by impact or likelihood;
4. Assign values to answers;
5. Assign weights to answers;
6. Apply the expressions/indicators;
7. Represent the obtained values on the graph.

Answer the questionnaire and save the answers

As mentioned before, users may select the most suitable questionnaire according to their sector or area of interest among those provided in the tool. Users must answer all the multiple choice questions in order to submit the questionnaire by selecting only one of the answers in each of the questions. These answers are saved and stored temporarily with the aim of using them in the following stages.

Classify questions per threat

One important characteristic of the tool is that it provides questionnaires for all the different sectors that CYSPA is involved with; these questionnaires gather the most relevant threats

affecting each of them. Questions have been carefully developed by taking into consideration a majority of threats within the same questionnaire. They also allow the tool to understand if it's important to prevent or mitigate the related threat.

Being clear that questionnaires contain and explore many different threats, it thus becomes essential that all questions referring to a same threat are classified together in order to reach a final quantitative analysis for that threat.

Classify questions by impact or likelihood

A similar process is necessary at this stage, once questions have been classified per threat, now they have to be separated into two different groups, impact and likelihood. This separation is necessary because in the analysis, each threat has two different values that represent the axis of the graph, one value for impact (vertical axis) and the other one for likelihood (horizontal axis).

Assign fixed values to answers

A prior mapping determines the value assigned to a specific answer depending on the question and the number of available answers. This value is always within the same range: 0 as minimum and 5 as maximum, values are arranged and distributed taking into account the number of available answers.

Assign weights to answers

Some questions are more important than others within the same questionnaire, since all answers are evaluated within the same range, equally and independently from the question and the related threat, it is absolutely necessary to have a differentiating factor that determine the importance of that specific question related to a specific threat within a specific questionnaire, that factor is the weight and it is assigned to every question.

The reason why this approach was adopted is because of the following advantages:

- Values assigned to answers are always assigned within the range [0,....,5] (this simplifies the administrators' tasks);
- If the importance of a question changes with time (because certain technologies have evolved and gained higher relevance within a specific sector, and so related threats have become more dangerous) the questionnaires would be updated by just modifying the weight and not every value of every answer;
- Having the same values assigned to answers allows the tool to compare them whenever necessary, and elaborate evolutional reports if requested;
- User perceives that questions and answers are homogeneous, making the task of answering a questionnaire much easier, especially for non-experts on security, and also improving the UX (User eXperience);
- The model captures the sectorial analysis done in D2.4.2.

Apply the expressions/indicators

The adopted process is the weighting process and works as follows:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i w_i}{\sum_{i=1}^{n} w_i} = \frac{x_1 w_1 + x_2 w_2 + x_3 w_3 + ... + x_n w_n}{w_1 + w_2 + w_3 + ... + w_n}$$

Where: X are fixed values assigned to answers and W are the weights

$$X = \{x_1, x_2, x_3..., x_n\}$$

$$W = \{w_1, w_2, ..., w_n\}$$

Represent the obtained values on the graph.

After obtaining the values for impact and likelihood for each of the threats the only step left is to represent them in a graph, as mentioned before this graph represents the impact and likelihood scale of a threat. The graph respects the range of the values from 0 to 5 for both dimensions and all the identified threats are represented within this area. Questions are focused to identify the most common threats that may affect the organisations operating in each of the sectors, taking into account: technologies used, available IT infrastructure, different activities and processes deployed etc.

Below is a working example of the entire process of answering questions and obtaining the quantitative analysis, this example concretely has been developed to identify the threat of information leakage in each of the sectors, evaluating the impact and likelihood.

It is important to clarify that in CRISK threats are evaluated separately for each of the sectors.

The graph below (figure 13) represents the values for one threat in each of the four sectors, this is just an example to explain the process of evaluation and it does not represent the risk analysis explained before (figure 6)

	Questions	Answers	Answer value
Impact	What would be the impact of an information leakage incident?	Critical	5
	What would be the impact of a confidential business information leakage on your organisation?	Moderate	2
Likelihood	Do you know which computer systems in your company are used to process or store critical or private data?	Yes	1
	Are there systems or procedures in place to protect confidential information flow within your organisation?	No	4

Table 1 – Example: Information leakage questions

Replies & Values [0,…,5]							
Reply 1	Value 1	Reply 2	Value 2	Reply 3	Value 3	Reply 4	Value 4
Critical	5	High	4	Moderate	2	Residual	0
Critical	5	High	4	Moderate	2	Residual	0
Yes	1	No	4				
Yes	1	No	4				

Table 2 – Example: Values assigned to answers for evaluation

Weights [0,…,5]			
Q1 - Transport	Q2 - Energy	Q3 - eGov	Q4 - Finance
4	2	3	5
4	4	3	3
4	2	3	5
4	4	3	3

Table 3 – Example: Weights assigned to sectors for evaluation

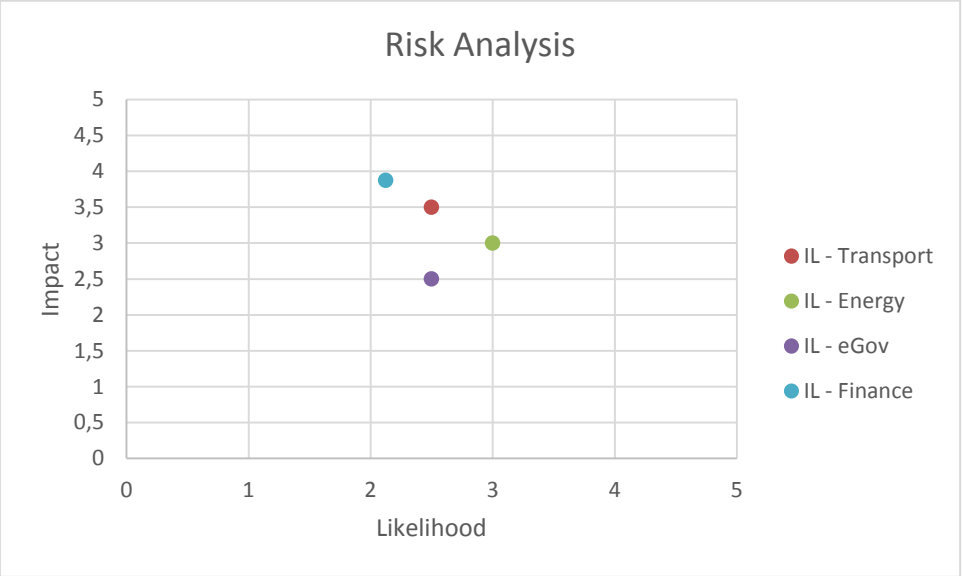

Figure 16 – Example: Graphical analaysis

4. Questionnaires

4.1. Transport sector questions

Question Text	Impact/ Likelihood	Associated threat	Question Weight	Answer 1		Answer 2		Answer 3		Answer 4		Answer 5	
				Text	Value	Text	Value	Text	Value	Text	Value	Text	Value
Do you have a centralised or decentralised wireless network?	Likelihood	[ENISA.13.a] Information leakage	34	Centralised	4	Decentralised	2						
Are all your portable devices encrypted? (laptops, mobile devices, wireless connections)	Likelihood	[ENISA.6.c] Equipment Loss	14	YES	2	NO	4						
Is the data on portable devices encrypted?	Likelihood	[ENISA.13.a] Information leakage	15	YES	2	NO	4						
How would you rate the safety of the encryption service you use?	Impact	[ENISA.12] Data Breaches	16	High	1	Mediocre	3	Low	4	Not sure	2		
Are portable devices equipped with tracking software?	Likelihood	[ENISA.6.c] Equipment Loss	17	YES	2	NO	4						
How would you rate the safety of the tracking software?	Impact	[ENISA.6.c] Equipment Loss	18	High	1	Mediocre	3	Low	4	Not sure	2		
Is data storage on USB drives allowed?	Likelihood	[ENISA.2] Worms / trojans	36	YES	4	NO	2						
What technology do you use to keep track of the location of trailers, trucks, shipments?	Likelihood	[ENISA.13.a] Information leakage	35	Radio Frequency Tag (RF)	4	GNSS applications	3	E-sensors	3	Other (please specify)	3	None	5
Is an Anti-Phishing mechanism or	Likelihood	[ENISA.9] Phishing	19	YES	2	NO	4						

software in place?													
How effectively would your company be able to deal with a computer virus in your network?	Impact	[ENISA.2] Worms / trojans	3	Very effectively	1	Somewhat effectively	2	Somewhat ineffectively	4	Not effectively	5		
How securely is private data stored and processed in your company?	Impact	[ENISA.12] Data Breaches	4	Very securely	1	Somewhat securely	2	Somewhat insecurely	4	Insecurely	5		
Is your network linked to other wireless networks that are not under your control?	Likelihood	[ENISA.13.a] Information leakage	21	YES	4	NO	2						
If you are connected to other networks, how susceptible to cyber-attacks do you think they could be?	Impact	[ENISA.13.a] Information leakage	22	Very susceptible	5	Somewhat susceptible	4	Not very susceptible	2	Not susceptible	1		
Are you confident that your company always sends data only through secure networks?	Likelihood	[ENISA.10] Spam	20	YES	2	NO	4						
Are you in possession of any confidential data of any of your employees, customers, clients?	Likelihood	[ENISA.12] Data Breaches	28	YES	4	NO	2						
Do you or your employees have access to any corporate information or trade secrets, either for	Likelihood	[ENISA.13.a] Information leakage	29	YES	4	NO	2						

your company or for those of your clients?													
How prepared would your company be to deal with the situation, if there were a loss of confidential records?	Impact	[ENISA.13.a] Information leakage	1	Entirely prepared	1	Somewhat prepared	2	Not very prepared	4	Not prepared	5		
Have you ever had problems with your mobile and / or Internet service provider? (failure, interruption, outage of Internet access)	Likelihood	[ENISA.8] Denial of service	30	YES	4	NO	2						
Is there a messaging protocol in place for e-mail communications?	Likelihood	[ENISA.10] Spam	23	YES	2	NO	4						
Has any malfunction or defect of any hardware, component, or equipment, been noted?	Likelihood	[ENISA.6.a] Physical damage	24	YES	4	NO	2						
Do you regularly update the antivirus software on your devices?	Likelihood	[ENISA.2] Worms / trojans	2	YES	2	NO	4						
Could software be performing inadequately due to the expiration or withdrawal of technical support?	Likelihood	[ENISA.2] Worms / trojans	31	YES	4	NO	2						
Do you have a data	Likelihood	[ENISA.12]	6	YES	2	NO	4						

management plan in place?		Data Breaches											
Does your company compile identity theft risk assessment reports?	Likelihood	[ENISA.7] Identity theft / fraud	7	YES	2	NO	4						
Is a data privacy policy in place in your company?	Likelihood	[ENISA.12] Data Breaches	8	YES	2	NO	4						
Is there a policy in place regarding data breaches and/or cyber-attacks?	Likelihood	[ENISA.12] Data Breaches	9	YES	2	NO	4						
Are your policies and security systems regularly updated and tested?	Likelihood	[ENISA.13.a] Information leakage	5	YES	2	NO	4						
Is your IT infrastructure and data insured against theft?	Likelihood	[ENISA.6.b] Theft	10	YES	2	NO	4						
How are your records stored?	Impact	[ENISA.12] Data Breaches	25	Electronically	3	Paper	2	External hard drives	3	Other / Not sure	4		
Who in your company has access to private client records?	Impact	[ENISA.12] Data Breaches	26	Data owner only	2	Employees	3	Clients	3	Other/ Not sure	4		
Who is able to add/modify the data on the hard drive?	Impact	[ENISA.12] Data Breaches	27	Data owner only	2	Employees	3	Clients	3	Other / Not sure	4		
Who is in charge of the notification process, if any private client records are lost?	Impact	[ENISA.12] Data Breaches	32	Company	3	Client	3	Other / Not sure	4				
Is this stipulated in a written agreement?	Impact	[ENISA.12] Data	33	YES	2	NO	4						

		Breaches											
Do you have a backup system for your wireless network?	Likelihood	[ENISA.13.a] Information leakage	11	YES	2	NO	4						
How often is your data backed up?	Impact	[ENISA.13.a] Information leakage	13	Daily	1	Every two weeks	2	Monthly	3	Annually	4	Other / Not sure	5
How long would it take for you to recover your data?	Impact	[ENISA.13.a] Information leakage	12	1 day	1	7 days	2	2 weeks	3	1 month	4	Other / Not sure	4

4.2. Finance sector questions

Question Text	Impact/ Likelihood	Associated threat	Question Weight	Answer 1		Answer 2		Answer 3		Answer 4	
				Text	Value	Text	Value	Text	Value	Text	Value
Are access control mechanisms in place to control internal access to customer financial and personal data?	Likelihood	[ENISA.12] Data Breaches	90	Yes	2	No	5				
Are security mechanisms (access control, integrity, monitoring, identity services, etc) duly tested and their proper functioning audited?	Likelihood	[ENISA.13.b] Information leakage	80	Yes	1	Partially	3	No	5		
Are there security mechanisms in place in customer mobile channels?	Likelihood	[ENISA.2] Worms / trojans	70	Yes	2	No	4				
Is data integrity ensured in insurance customer databases?	Likelihood	[ENISA.7] Identity theft / fraud	90	Yes	2	No	4				
Are there multiple security layers in place?	Likelihood	[ENISA.4] Exploit kits	50	Yes	2	No	4				
Consequences of fraudulent identity in new bank accounts?	Impact	[ENISA.7] Identity theft / fraud	70	Penal	5	Bad reputation	4	None	0	Loss of business	3
Consequences of loss of customer data	Impact	[ENISA.5] Botnets	60	Loss of business	4	Bad reputation	4	Penal	5	None	0
Consequences of manipulated financial indicators or investment data	Impact	[ENISA.12] Data Breaches	70	Loss of business	5	Increased costs	4	None	0		
Consequences of stolen credit card customer data	Impact	[ENISA.4] Exploit kits	90	Loss of business	5	Bad reputation	4	Penal	5	None	0
Consequences of social engineering attacks in call center agents	Impact	[ENISA.14] Targeted attacks	90	Unauthorized access to customer data	5	Stealing of customer funds	5	High insurance costs	4	None	0
Consequences of faulty or compromised 3rd party software in mission-critical systems	Impact	[ENISA.4] Exploit kits	90	Access to org and customer	5	Stealing of funds	5	None	0		

				data							
Consequences of faulty or compromised teller machines	Impact	[ENISA.4] Exploit kits	80	Stealing of funds	5	High insurance costs	4	None	0		
Consequences of phishing on bank customers	Impact	[ENISA.14] Targeted attacks	60	Stealing of funds	5	Loss of reputation	4	None	0		
Consequences of security failures in 3rd party systems in non-mission related systems (air conditioning, etc..)	Impact	[ENISA.4] Exploit kits	80	Access to core systems	5	Higher security controls costs	4	None	0		
Consequences of BYOD-induced failures	Impact	[ENISA.4] Exploit kits	40	Loss of business	5	Access to core systems	5	None	0		
Consequences of online POS fraud	Impact	[ENISA.6.b] Theft	70	Loss of business	5	High insurance costs	4	None	0		

4.3. e-Government sector questions

Question Text	Impact/ Likelihood	Associated threat	QW	Answer 1		Answer 2		Answer 3		Answer 4		Answer 5	
				Text	Value	Text	Value	Text	Value	Text	Value	Text	Value
Does the organisation have exposed systems with High avaibility requirements ?	Impact	[ENISA.8] Denial of service	50	None	0	Few	1	Some	2	Most of them	4	All	5
Does the organisation use Denial of Service mitigation?	Impact	[ENISA.8] Denial of service	10	No	5	Redundant large throughput Internet links	3	Redundant sites hosted in different providers	2	Contracted external DoS mitigation infrastructures and services	1		
Does the organisation have qualified staff and a process in place to react to DoS attacks?	Impact	[ENISA.8] Denial of service	40	No	5	Skilled staff capable of handling DoS attacks	3	Skilled staff with specific training on DoS mitigation	2	Skilled staff, policies and procedures to handle DoS attacks	1		
Do you see the organisation as a desirable target for cyber hacktivism? What would be in your opinion the probability of such an attack in the next year?	Likelihood	[ENISA.8] Denial of service	20	Not likely	0	Low	1	Medium	2	High	4	Very likely	5
What is the history of DoS, defacements or other types of successful hacktivism attacks on your organisation in the last three years?	Likelihood	[ENISA.8] Denial of service	50	No perceived attacks	0	At least one attack	3	Between 2 and 5 attacks	4	More than 5 attacks	5		
Does the organisation conduct frequent external security audits and penetration tests?	Likelihood	[ENISA.8] Denial of service	30	No	5	At least every two years	3	Every year	2	Every 6 months	1	More than twice a year	0
In the event of a defacement attack, would the organisation:	Impact	[ENISA.14] Targeted attacks	40	Recover the systems as soon as possible, using	5	Use automated recovery processes to restore the	3	Use business continuity or disaster recovery processes to	2	Use the professional services of a specialized	1		

				internal resources		affected systems		restore the affected systems		partner to recover the systems and gather any evidence needed			
The organisation's publicly exposed systems are located:	Impact	[ENISA.14] Targeted attacks	30	In an external hosting provider	0	In a segregated network (DMZ) behind a firewall	2	In the internal network, published through the perimeter firewall	4	Outside the internal network, with no firewall	5		
Does your organisation have a dedicated incident response staff and intrusion analyst staff to monitor and secure major assets exposed on the internet ?	Impact	[ENISA.14] Targeted attacks	30	No	5	Skilled staff capable of conducting incident response and analysis	3	Skilled staff with specific training in incident response and analysis	2	Skilled staff, policies and procedures for incident response and analysis	1		
Regarding the security maintenance of publicly available systems, there is:	Likelihood	[ENISA.14] Targeted attacks	30	Specific policy and procedures that include patch management, vulnerability management and regular security assessments	0	Specific policy and procedures that include patch management and vulnerability management	2	Specific policy and procedures that include patch management	3	No specific policy or procedures	5		
Do the publicly available systems include business critical information?	Likelihood	[ENISA.14] Targeted attacks	40	No	0	Some critical information, that is replicated in other systems	3	Critical information that doesn't exist in other systems	5				
What would be the possible benefit of a successful attack on your public sites?	Likelihood	[ENISA.14] Targeted attacks	30	None	0	Cause minor damage to the organisation's image	1	Cause public embarassment or serious damage to the organisation's image	2	Steal valuable information such as personal data	4	Conduct fraudulent transactions	5
Do you have a policy in place to warn users not to click on links received in e-	Impact	[ENISA.1] Drive-by downloads	80	No	5	Informal policy	4	Formal policy	2	Formal policy and awareness training	1		

mail messages?													
Is the end user laptop or workstation maintained with security policies and patching policies ?	Impact	[ENISA.1] Drive-by downloads	10	No	5	Applicable to some users	4	Applicable to most users	2	Applicable to all users	1		
Are your user's local administrators of their laptops or workstations?	Impact	[ENISA.1] Drive-by downloads	10	No	0	Few	1	Some	2	Most of them	4	All	5
Is there a software suite selection that reduces the number of software to be managed by the organisation's patching policy?	Likelihood	[ENISA.1] Drive-by downloads	30	Restrictive suite of software with no exceptions	0	Restrictive suite of software with some exceptions	1	Recommended suite of software, with few restrictions	2	Recommended suite of software, with no restrictions	4	No policy on the suite of softwar e to be used	5
Do you have an effective anti-spam and e-mail virus screening system?	Likelihood	[ENISA.1] Drive-by downloads	60	Yes, with hourly updates	0	Yes, with daily updates	1	Yes, with frequent updates	2	No	5		
Is there a centralized log system (SIEM) that can correlate network and Anti-Virus logs in a way that a possible drive-by attack would be blocked?	Likelihood	[ENISA.1] Drive-by downloads	10	Yes	0	No	5						
Are major assets behind a SSLv3 supported infrastructure?	Impact	[ENISA.13. b] Informatio n leakage	30	None	0	Few	1	Some	2	Most of them	4	All	5
Is sensitive or critical information using SSLv3 (SSL) as a method of transport from the network to the outside and from the outside to the inside of the organisation?	Impact	[ENISA.13. a] Informatio n leakage	60	None	0	Few	1	Some	2	Most of them	4	All	5
Is there any security guideline in best practice or list of implementation referring the best Cipher Suite to use in case of a SSLv3 dependence?	Impact	[ENISA.13. a] Informatio n leakage	10	None	0	Few	1	Some	2	Most of them	4	All	5

Is there any internal service or server using SSLv3?	Likelihood	[ENISA.13.a] Information leakage	10	None	0	Few	1	Some	2	Most of them	4	All	5
In case of SSLv3 usage is the usage restricted to the internal network or to internal and external ?	Likelihood	[ENISA.13.a] Information leakage	10	None	0	Few	1	Some	2	Most of them	4	All	5
Do you have a process in place to replace systems using weak cryptography such as SSLv3?	Likelihood	[ENISA.13.a] Information leakage	80	Yes, already in place	0	Yes, ongoing	1	Yes, in planning phase	3	No	5		
Does the organization conduct internal security audits with a focus the security of personal data?	Impact	[ENISA.12] Data Breaches	50	Yes	0	No	5						
Is all personal data stored using encryption?	Impact	[ENISA.12] Data Breaches	25	The organization does not store personal data	0	All personal data stored using encryption	1	Most personal data stored using encryption	2	Encryption is not use in the storage of personal data	4		
Is all personal transmitted through the network using encryption?	Impact	[ENISA.12] Data Breaches	25	The organization's systems do not transmit personal data	0	All personal data transmitted using encryption	1	Most personal data transmitted using encryption	2	Encryption is not use in the transmission of personal data	4		
Are data breaches detected and investigated?	Likelihood	[ENISA.12] Data Breaches	10	Yes	0	Most data breaches are investigated	2	Some data breaches are investigated	3	No	5		
Does the organization manage personal data of clients, associates or employees?	Likelihood	[ENISA.12] Data Breaches	45	No	0	Only employees	2	Only employees and associates	3	Yes	5		
Does the organisation have specific legal requirements regarding the processing of personal data?	Likelihood	[ENISA.12] Data Breaches	45	No	0	Yes	5						

4.4. Energy sector questions

Question Text	Impact/ Likelihood	Associated threat	Question Weight	Answer 1		Answer 2		Answer 3		Answer 4	
				Text	Value	Text	Value	Text	Value	Text	Value
Does your organisation have controls in place to detect attacks on your systems?	Likelihood	[ENISA.14] Targeted attacks	85	YES	2	NO	4	NOT SURE	3		
Does your organisation have provisions in place to prevent data leakage of safety relevant information?	Likelihood	[ENISA.13.a] Information leakage	65	YES	1	NO	5	NOT SURE	3		
How critical for your organisation would the loss of a single power station be?	Impact	[ENISA.6.a] Physical damage	80	Very critical	5	Somewhat critical	3	Not critical	1		
What service disruption period is your organisation able to tolerate?	Impact	[ENISA.8] Denial of service	78	> 5 days	0	1-5 days	1	8-24 hours	2	< 8 hours	5
Does your organization operate critical facilities, like nuclear power plants?	Impact	[ENISA.6.a] Physical damage	90	YES	5	NO	0				
How often is your organisation the target of cyber-attacks ?	Likelihood	[ENISA.8] Denial of service	55	Infrequently	1	Frequently	3	Daily	4	Constant	5
Do you run background checks of your employees?	Likelihood	[ENISA.13.a] Information leakage	42	YES	1	NO	4	SOMETIMES	3		
Does your organisation operate spare transformers?	Likelihood	[ENISA.6.a] Physical damage	72	YES	1	NO	4				
Does your organisation use a private communication network, like a powerline-carrier (PLC)-system?	Impact	[ENISA.13.a] Information leakage	62	YES	1	NO	3				
Is your organization's private communication network adequate protected against cyber-attacks?	Likelihood	[ENISA.14] Targeted attacks	52	YES	1	NO	5	NOT SURE	3		
Has your organisation adopted special security measures for smart grid controls?	Impact	[ENISA.14] Targeted attacks	67	YES	0	NO	5	NOT SURE	3		
Has your organisation installed security measures like encryption or authentication technologies?	Likelihood	[ENISA.12] Data Breaches	50	YES	1	NO	5	NOT SURE	3		
How does your organisation rank the risk of	Likelihood	[ENISA.13.a]	48	Very likely	5	Somewhat	3	Unlikely	1		

industrial espionage?		Information leakage				likely					
Has your organisation adopted measures to prevent industrial espionage?	Likelihood	[ENISA.13.a] Information leakage	45	YES	1	NO	5	NOT SURE	3		
Does your organisation sees itself as a possible target for "hacktivists"?	Likelihood	[ENISA.8] Denial of service	30	YES	4	NO	1				
Can your organisation ensure system functionality in case of reduced availability of operational control systems?	Likelihood	[ENISA.8] Denial of service	80	YES	1	NO	5	NOT SURE	3		
How long can your organisation ensure system functionality with reduced availability of operational control systems?	Impact	[ENISA.8] Denial of service	71	> 5 days	0	1-5 days	1	8-24 hours	2	< 8 hours	5
Do your systems comply with international security guidelines?	Impact	[ENISA.14] Targeted attacks	68	YES	1	NO	5	NOT SURE	2		
Does your company intend to have its it-security system certified?	Impact	[ENISA.14] Targeted attacks	50	YES	3	NO	5	Already certified	1		
How tamper-proof is your hardware against physical attacks?	Impact	[ENISA.3] Code injection	70	Very tamper-proof	1	Somewhat tamper-proof	2	Not tamper-proof	4		
Does your hardware have automated system protection measures, like data erasure?	Impact	[ENISA.6.c] Equipment Loss	44	YES	0	NO	5	NOT SURE	2		
Does your organisation separate energy delivery and energy management networks?	Impact	[ENISA.14] Targeted attacks	74	YES	0	NO	5	NOT SURE	3		
Does your organization employ distinct personnel supervising it-security, i.e. an IT-security officer?	Likelihood	[ENISA.12] Data Breaches	75	YES	0	NO	5	NOT SURE	3		
Does your organisation operate energy transmission systems?	Impact	[ENISA.8] Denial of service	77	YES	4	NO	0				

5. Conclusions

We have realised that developing a tool such as CRISK is not an easy task; especially when it is oriented to different sectors. Most of the tools identified have a more defined scope, but with the support of the CYSPA Alliance and the self-maintained design that we have implemented we believe it brings an added value and that it has a great potential to become a very useful service for members of the Alliance.

Although the tool is oriented towards risk assessment, due to its flexible design, it may be adapted to different evaluations such as regulatory compliance with the ISO standards. On this side, the CYSPA consortium has evaluated the possibility of joining forces with the CoBlue [7] company, developing the CoAble [8] product. After some phone calls held between CRISK and CoAble teams, the Consortium decided not to integrate CRISK and the CoAble tool because of the different goals of both solutions and the effort that this integration represents, which has been evaluated as too high in the context of the CYSPA project.

The tool will now be used by the CYSPA Alliance and its community. It represents a first real service to CYSPA members and we hope that they will find it useful not only as a tool for assessing their own organisation's risk but also as a mechanism for community-building. As the number of users for the tool increases so too will the content and reliability of outputs. As such, we see a real value in continuously bringing in other communities to be part of CYSPA and take part in and benefit from its activities and services.

6. REFERENCES

[1] CYSPA Description of Work, 2011
[2] D2.1.1 Impact report – Transport, 2013
[3] D2.1.2 Impact report – Energy, 2013
[4] D2.1.3 Impact report – e-Government, 2013
[5] D2.1.5 Impact report – Finance, 2013
[6] CYSPA Community Portal, https://cyspa.eng.it/
[7] CoBlue, www.coblue.eu
[8] CoAble, http://www.coable.eu/
[9] CoAble Overview, https://www.coblue.eu/products
[10] D3.6.2 Solutions & Threats dataset – final release
[11] ISACA (2006). CISA Review Manual 2006. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3.
[12] PMBOK 5th edition, http://www.pmi.org/PMBOK-Guide-and-Standards/pmbok-guide.aspx
[13] OPENNESS, http://openness.eng.it/