



REWIRE - Cybersecurity Skills Alliance

A New Vision for Europe

R6.3 Impact

Evaluation report No. 1



Title	R6.3 Impact Evaluation Report No. 1
Document description	The Impact Evaluation Report No. 1 presents the first Impact Evaluation of the REWIRE project covering the evaluation of the impact of project outputs delivered between month 1 and 12, namely from 01 November 2020 to 30 October 2021.
Nature	Confidential
Task	Task 2: Continuous quality control
Status	Final
WP	WP 6
Lead Partner	ReadLab
Partners Involved	All partners
Date	02/02/2022

Revision history	Author	Delivery date	Summary of changes and comments
Version 01	Olga Karamichailidou	11/01/2022	First version shared with the project coordinator.
Version 02	Olga Karamichailidou	27/01/2022	Second version shared with the project coordinator
Final Version	Olga Karamichailidou	02/02/2022	Final version incorporating the project coordinator's feedback

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
2	INTRODUCTION	5
2.1	Project background	5
2.2	Project objectives	5
2.3	Methodology and data collection	6
3	INTERNAL IMPACT EVALUATION	7
3.1	Internal Impact Evaluation Survey results	7
3.1.1	<i>R1.3 EAB Framework</i>	7
3.1.2	<i>R1.7 Privacy policy & procedures</i>	8
3.1.3	<i>R1.8 Open Data procedures and guidelines</i>	9
3.1.4	<i>R2.1.1 PESTLE Analysis results</i>	10
3.1.5	<i>R2.2.2 Cybersecurity Skills Needs Analysis</i>	12
3.1.6	<i>R2.2.3 Methodology to anticipate future needs</i>	13
3.1.7	<i>R6.1 Quality Assurance Plan</i>	14
3.1.8	<i>R6.2 Quality Assurance Report M1 – M8</i>	15
3.1.9	<i>R7.1 Stakeholders analysis</i>	16
3.1.10	<i>R7.2 Targeting key policymakers</i>	17
3.1.11	<i>R7.3 Dissemination Plan</i>	18
3.1.12	<i>R7.4 Project website</i>	19
3.1.13	<i>Partner collaboration</i>	20
3.2	Work package evaluation	21
4	STAKEHOLDERS	25
4.1	Stakeholders analysis	25
4.2	Stakeholder evaluation form	25
5	CONCLUSION	27
6	REFERENCES	28
7	LIST OF ABBREVIATIONS AND ACRONYMS	29
8	LIST OF FIGURES	30
9	LIST OF TABLES	31

1 EXECUTIVE SUMMARY

The evaluation of the REWIRE project deliverables and other tangible results is essential for its continuous improvement. The report at hand presents the first Impact Evaluation of the REWIRE project summarizing the major achievements of the REWIRE project from month 1 to month 12, namely from 01 November 2020 to 30 October 2021, and discussing whether the project objectives had been met.

The 1st Impact Evaluation Report employs a mixed methodology in order to collect and analyse both qualitative and quantitative data on the first twelve months of project delivery (M1 – M12). It assesses the status and the levels of involvement, difficulty in achieving the objective, utility and cooperation regarding the main deliverables of this period from a partner point of view as well as the milestones and they key performance indicators achieved at work package level.

Overall, all assessed deliverables were deemed useful, with low to moderate difficulty, and with few suggestions for further development. Most milestones and key performance indicators were reached. While project stakeholders were identified and mapped, it was too early to assess their satisfaction on project results/achievements.

2 INTRODUCTION

2.1 PROJECT BACKGROUND

The Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project is the Alliance formed from the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap": CONCORDIA, ECHO, SPARTA and CyberSec4Europe. Thus, the REWIRE Alliance represents the more than 160 partners of the four pilot projects, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

This project aims to provide concrete recommendations and solutions that would lead to the reduction of skill gaps between industry requirements and sectoral training provision and contribute to support growth, innovation, and competitiveness in the field of Cybersecurity. REWIRE is co-funded by the ERASMUS+ programme of the European Union (Agreement Number – 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B) for a duration of four years (01.11.2020 to 31.10.2024).

2.2 PROJECT OBJECTIVES

REWIRE builds a Blueprint for the Cybersecurity industry and a concrete European Cybersecurity Skills Strategy. This strategy will bring together lessons learned from other initiatives (i.e. CONCORDIA, SPARTA, ECHO, CyberSec4Europe) and will be outlined from a holistic approach, identifying political, economic, social, technological, legal and other factors which may be affecting sector skills and training offer. Encompassed with activities, milestones, outcomes and outputs, these activities will be developed during the course of the project:

- Design and implementation of a Blueprint for the Cybersecurity industry
- Develop a European Cybersecurity Skills Strategy
- Develop a common methodology for the assessment of the current situation and to anticipate future needs, through identification of existing and emerging skills needs.
- Create a European Cybersecurity Skills Observatory integrated by specific actions, activities and tools that allow for anticipation and matching of skills supply and demands.
- Support the strategy and framework through the implementation of a digital on-line publicly accessible European Cybersecurity Skills Digital Observatory – CyberABILITY (for cybersecurity skills merging the market needs, the profiles, the competencies and the available training courses).
- Create a Cybersecurity Skills Framework containing profiles for the needed cybersecurity profiles and their analysis.

- Pilot a federated cyber range hosted by multiple project partners to support the goals of the project.
- Create at least four (4) educational curricula and relevant skills certification schemes for profiles contained in the Cybersecurity Skills Framework.
- Promoting the attractiveness of the sector and gender balance through specific actions to engage all relevant stakeholders
- Develop actions for encouraging mobility through promoting the use of existing European tools (Erasmus+, EURES, EAfA etc.).
- Create networks to improve skills intelligence and information mechanisms and strengthen the exchange of knowledge and practice between the cybersecurity industry and the VET providers, adapting VET provision to the skills needs demanded by the sector.

REWIRE aims to get main market players involved taking up opportunities to make the best of their talents. They will constitute together with the partnership, the Sector Skills Alliance, the necessary driver to push a sustainable sectoral strategy and Blueprint implementation as mentioned above.

2.3 METHODOLOGY AND DATA COLLECTION

The REWIRE Quality Assurance and Evaluation focuses on three dimensions, namely on the project process, impact and results and, more particularly this report documents the impact attained vis-à-vis the overall objectives and expected results as defined in the REWIRE Quality Assurance Plan.

An internal project evaluation form was administered by ReadLab. The impact evaluation questionnaire was uploaded on the Google Forms platform in the account owned by the REWIRE project in order to facilitate the compilation and subsequent collection of data. Requests to fill in the impact evaluation questionnaire were sent by email to all partners and communicated during December's WP Leaders meeting. The data were collected and processed in anonymous and aggregate form to prepare a summary report of the main elements emerging from the survey.

The impact evaluation questionnaire assessed the status, level of involvement in each deliverable, the level of difficulty in achieving the objective, the level of utility of the deliverable for the overall project and the level of cooperation while working on each deliverable. The last question (level of cooperation) was directed only to the task leaders.

In addition, ReadLab conducted a quantitative and qualitative analysis of the responses coming from the WP Leader Monitoring Forms, that were previously administered, and of the deliverables R7.1 Stakeholder analysis report and R7.2 Targeting key policymakers.

3 INTERNAL IMPACT EVALUATION

3.1 INTERNAL IMPACT EVALUATION SURVEY RESULTS

A total of 23 partners completed the questionnaire on the internal impact evaluation.

Below we will report the most significant results in the form of graphs and/or tables.

All scores for each question are on a Likert scale as follows:

- from 1 to 5 where 1 corresponds to never and 5 corresponds to completely
- from 1 to 4 where 1 corresponds to none and 4 corresponds to high
- from 1 to 3 where 1 corresponds to poor or no and 3 corresponds to excellent or yes

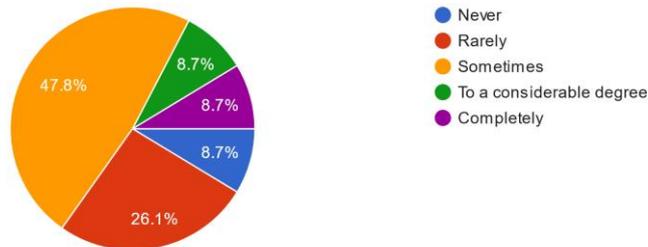
We advised all participants to fill in questions 1 – 4 and only the task leaders to fill in question 5 for each deliverable. Some reviewers mentioned that they were unable to properly assess the status or the impact of some deliverables due to lack of involvement or handover with the previously assigned person in their organisation.

3.1.1 R1.3 EAB Framework

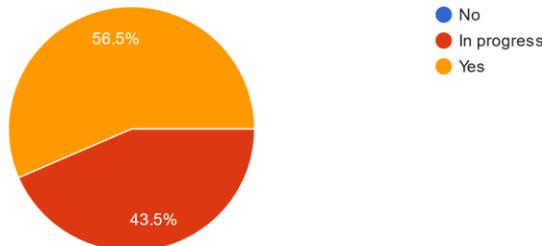
R1.3 was prepared by MRU. This report provides information to EAB members and elaborates in detail the EAB mission and tasks, defines verifiable criteria of the selection procedure of EAB members. The EAB Framework received a good score on the level of utility.

Figure 1 EAB Framework

1. How much have you been involved?
23 responses

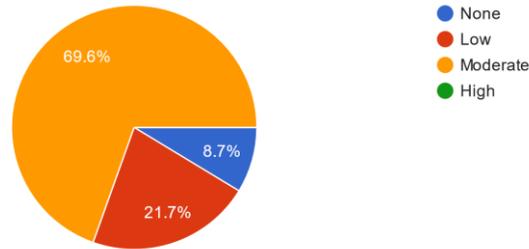


2. Has the deliverable been achieved?
23 responses



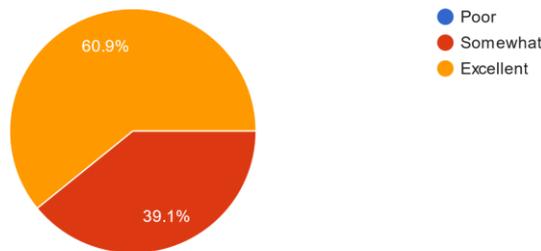
3. What was the level of difficulty in achieving the objective?

23 responses



4. What is the level of utility of the deliverable for the overall project?

23 responses



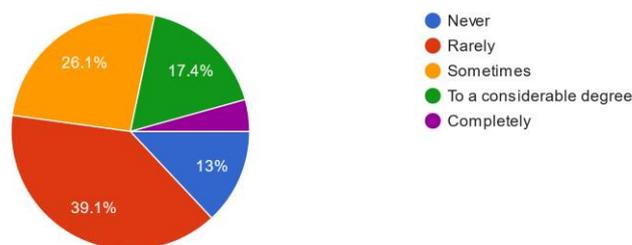
3.1.2 R1.7 Privacy policy & procedures

R1.7 was prepared by Apiroplus and it provides the input for the implementation of the relevant policies and procedures on the protection of privacy that will govern the REWIRE project data privacy issues. The document includes the methodology, analysis of the personal data protection regulatory and legal framework, the principles relating to the processing of personal data, the collection of personal data processed by the REWIRE project partners and the project Data Protection Policy. The Privacy policy & procedures received a good score on the level of utility.

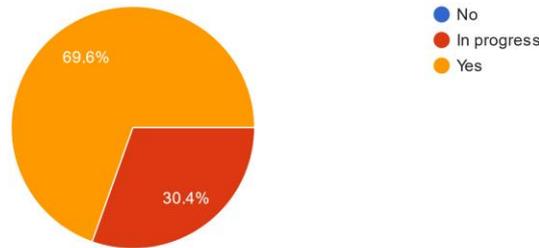
Figure 2 R1.7 Privacy policy & procedures

1. How much have you been involved?

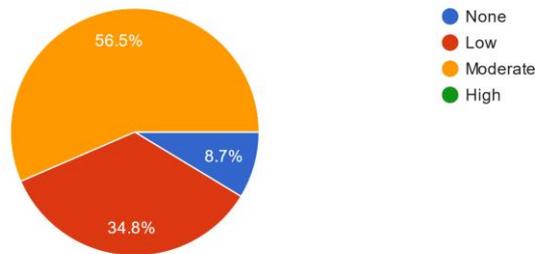
23 responses



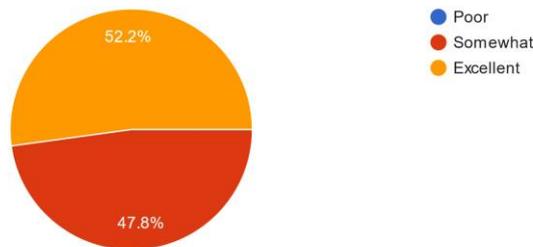
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses



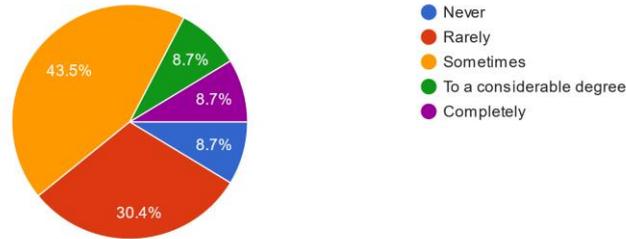
3.1.3 R1.8 Open Data procedures and guidelines

R1.8 was prepared by Apiroplus and it provides an analysis regarding the requirements imposed by European, Project and National laws, regulations, agreements and rules. This analysis provides the input for the implementation of the relevant policies and procedures on the handling of open data. The Open Data procedures and guidelines received good score on the level of utility.

Figure 3 Open data procedures and guidelines

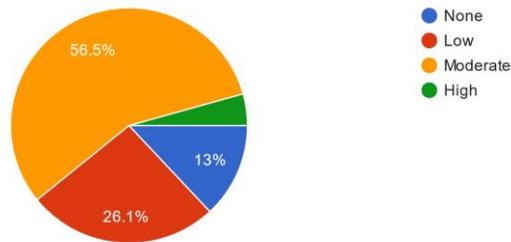
1. How much have you been involved?

23 responses



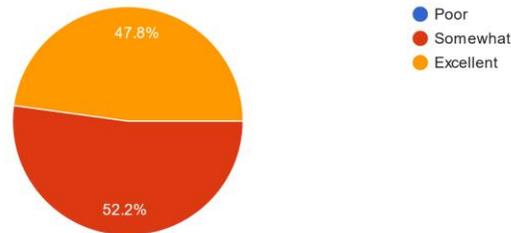
3. What was the level of difficulty in achieving the objective?

23 responses



4. What is the level of utility of the deliverable for the overall project?

23 responses



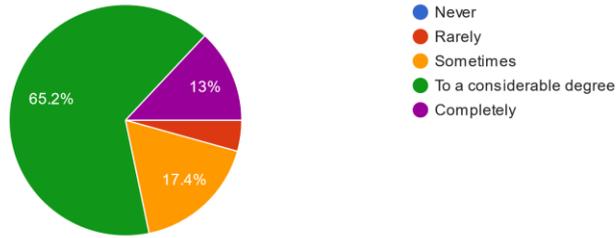
3.1.4 R2.1.1 PESTLE Analysis results

R2.1.1 was prepared by BUT. A report was created for each participating country containing the Political, Economic, Social, Technological, Legal and Environmental factors, which can impact the cybersecurity sector. The PESTLE Analysis report received a very high score on the level of utility. In some reviewers' words,

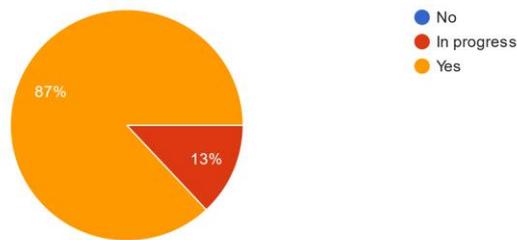
"PESTLE analysis report is a very useful report as it sets the ground for the launch of the project."
"Good result"

Figure 4 PESTLE Analysis results

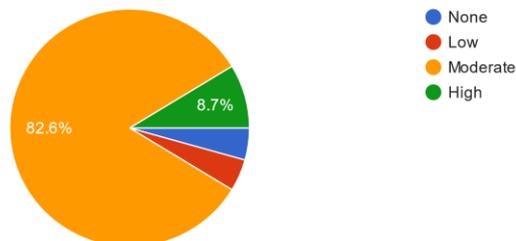
1. How much have you been involved?
 23 responses



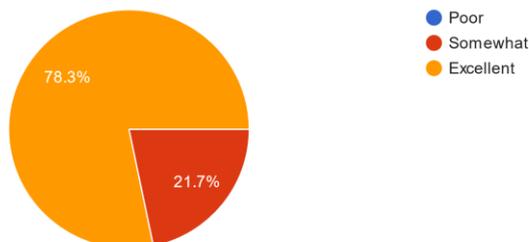
2. Has the deliverable been achieved?
 23 responses



3. What was the level of difficulty in achieving the objective?
 23 responses



4. What is the level of utility of the deliverable for the overall project?
 23 responses

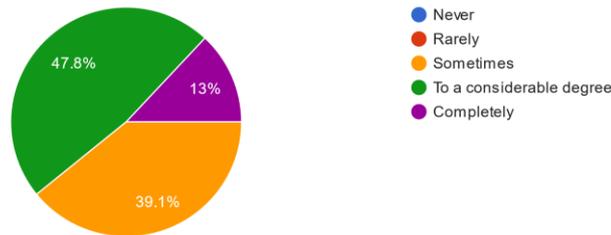


3.1.5 R2.2.2 Cybersecurity Skills Needs Analysis

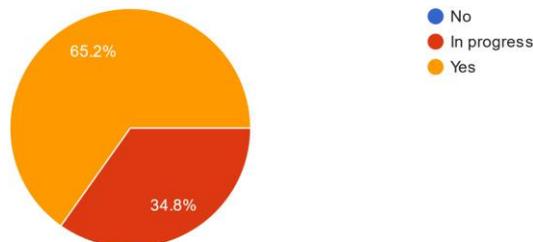
R2.2.2 was prepared by KTH and it contains the current “state of the art” of the cybersecurity sectoral skills. The Cybersecurity Skills Needs Analysis received a very high score on the level of utility. A reviewer noted that there was room for further development.

Figure 5 Cybersecurity skills needs analysis

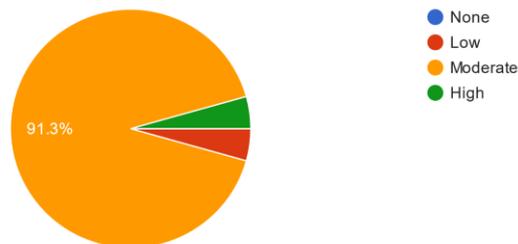
1. How much have you been involved?
23 responses



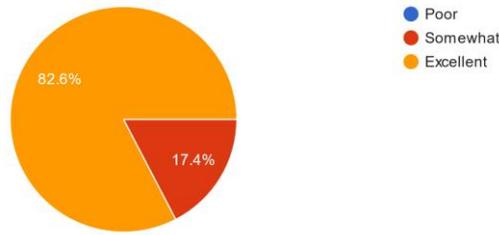
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

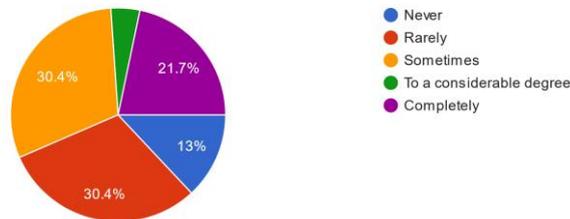


3.1.6 R2.2.3 Methodology to anticipate future needs

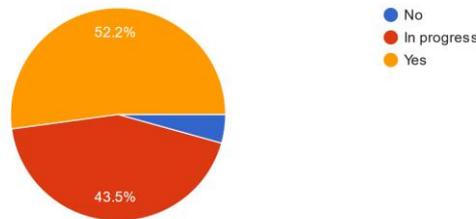
R2.2.3 was drafted by MRU and it allows for the reliable anticipation of future cybersecurity skills needs. The methodology received a good score on the level of utility. A reviewer noted that it was a difficult task and that it could be further developed.

Figure 6 Methodology to anticipate future needs

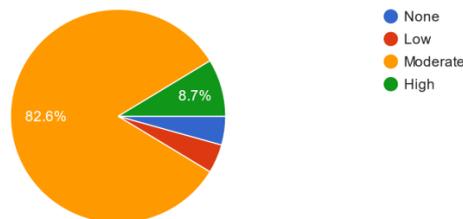
1. How much have you been involved?
23 responses



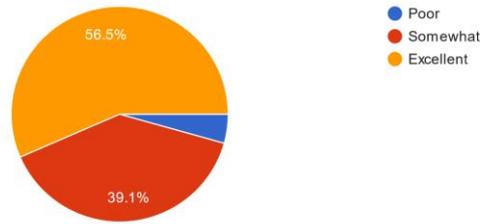
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

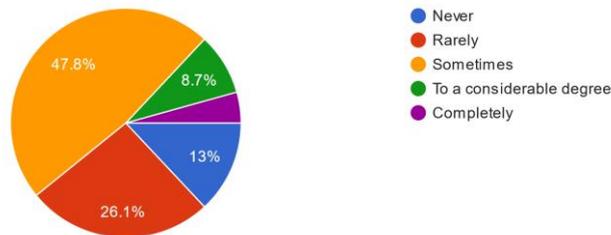


3.1.7 R6.1 Quality Assurance Plan

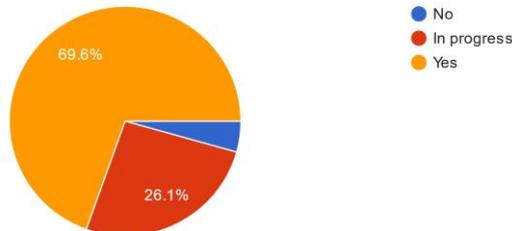
R6.1 was developed by ReadLab with the aim to familiarize the consortium with the quality processes, methodologies and evaluation tool. The quality assurance plan received a high score on the level of utility.

Figure 7 Quality Assurance Plan

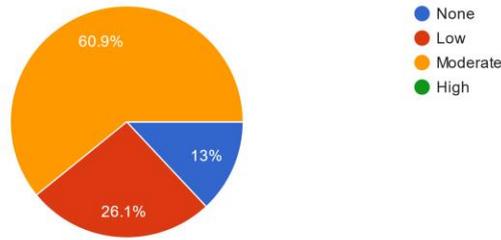
1. How much have you been involved?
23 responses



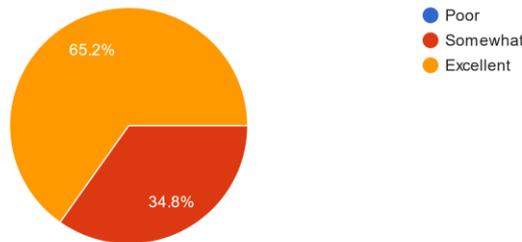
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

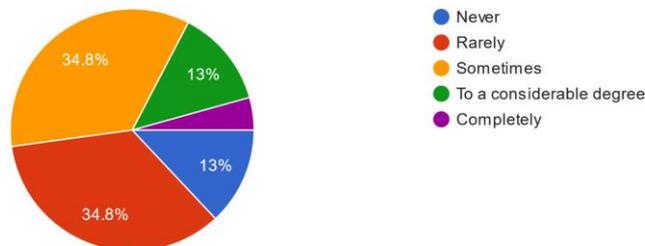


3.1.8 R6.2 Quality Assurance Report M1 – M8

R6.2 was developed by ReadLab and contains the findings and recommendations for the improvement of the project implementation for the first 8 months of the project. The quality assurance report M1 – M8 received a moderate score on the level of utility. The main difficulty with respect to this report was the data collection from all partners.

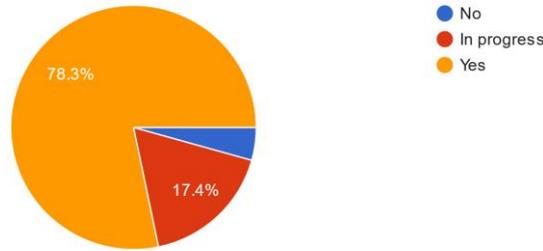
Figure 8 Quality Assurance Report M1 -- M8

1. How much have you been involved?
23 responses



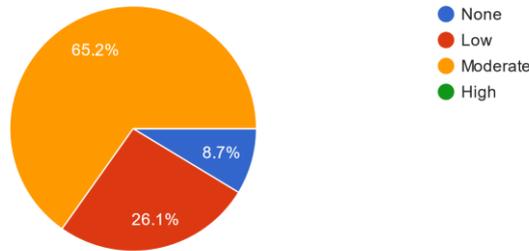
2. Has the deliverable been achieved?

23 responses



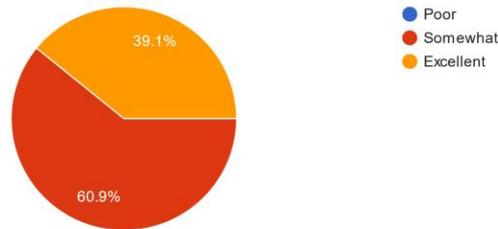
3. What was the level of difficulty in achieving the objective?

23 responses



4. What is the level of utility of the deliverable for the overall project?

23 responses



3.1.9 R7.1 Stakeholders analysis

R7.1 was developed by EFVET. It is a comprehensive map of all stakeholders that have either a direct or indirect interest, influence, and impact on the REWIRE project at local, regional, national, and European levels. The stakeholders' analysis received a high score on the level of utility.

1. How much have you been involved?

23 responses

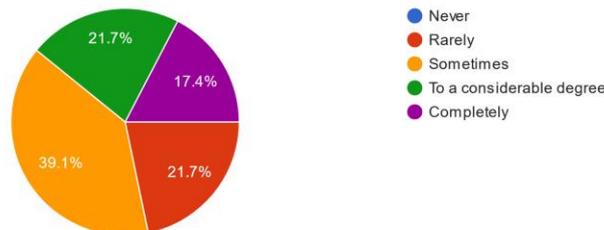
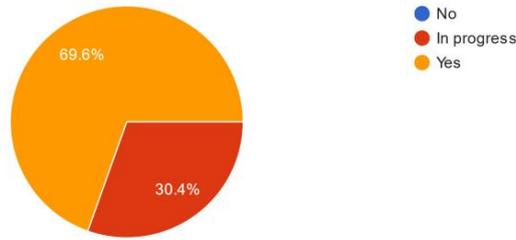
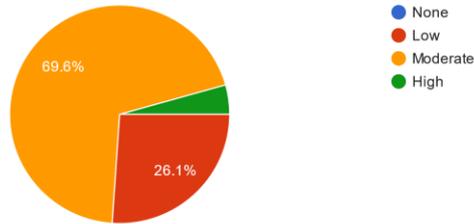


Figure 9 Stakeholders analysis

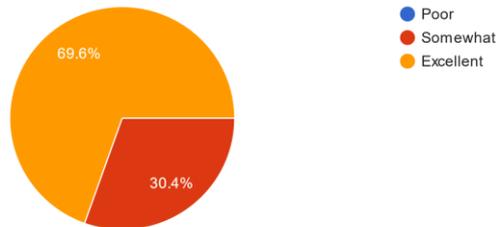
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

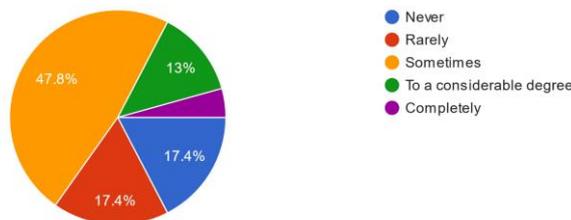


3.1.10 R7.2 Targeting key policymakers

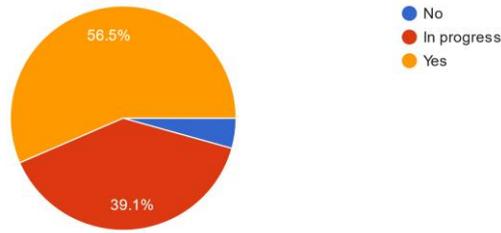
7.2 was developed by EFVET and it identifies the policymakers to which the project can have an impact and the degree of that impact. The targeting of policymakers received a moderate score on the level of utility. As on reviewer noted, this task is to be considered continuous.

Figure 10 Targeting key policymakers

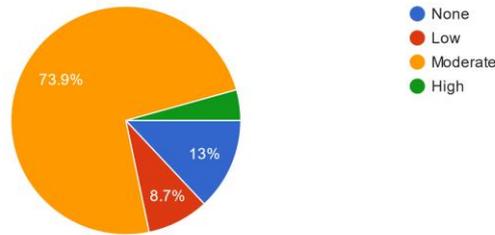
1. How much have you been involved?
23 responses



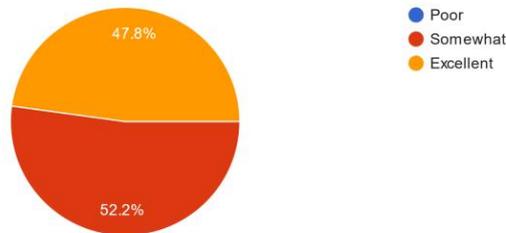
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

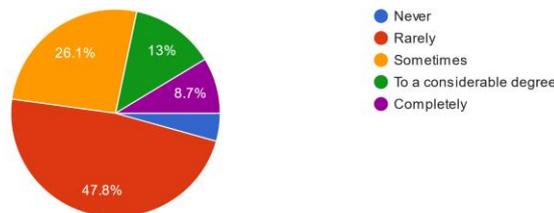


3.1.11 R7.3 Dissemination Plan

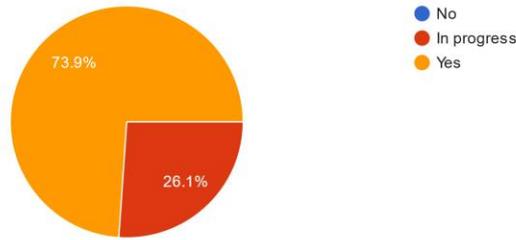
R7.3 was developed by EVTA and it is a live report that contains both the dissemination plan and the results from its execution. The dissemination plan received a moderate score on the level of utility. A reviewer noted that more attention should be given to education institutions.

Figure 11 Dissemination plan

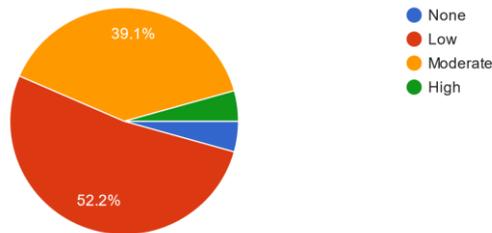
1. How much have you been involved?
23 responses



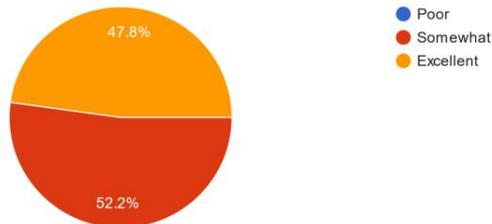
2. Has the deliverable been achieved?
23 responses



3. What was the level of difficulty in achieving the objective?
23 responses



4. What is the level of utility of the deliverable for the overall project?
23 responses

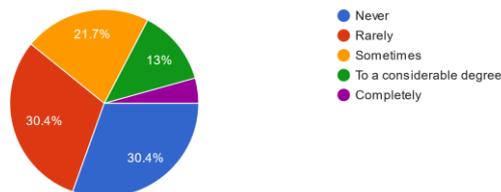


3.1.12 R7.4 Project website

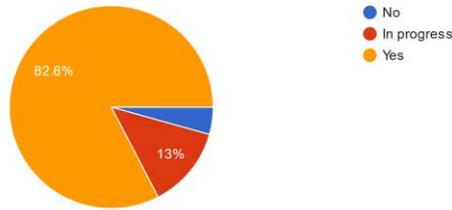
R7.4 was prepared by ReadLab and it embeds all important sections such as a homepage, project description and its objectives, results and partners, blueprint, training, cyberability, a media corner, news and contact. The page includes the privacy policy according to the GDPR regulations and cookies policy. The project website received a high score on the level of utility.

Figure 12 Project website

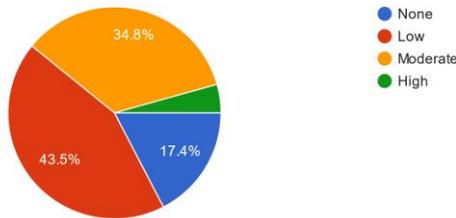
1. How much have you been involved?
23 responses



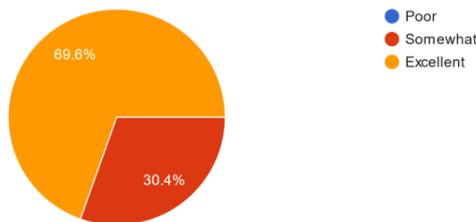
2. Has the deliverable been achieved?
 23 responses



3. What was the level of difficulty in achieving the objective?
 23 responses



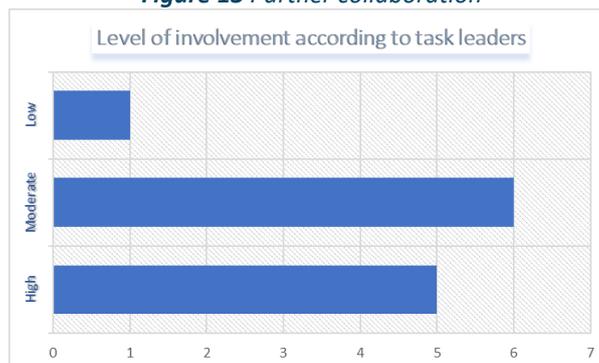
4. What is the level of utility of the deliverable for the overall project?
 23 responses



3.1.13 Partner collaboration

A special note should be made for the level of partnership involvement towards the achievement of the deliverables for the period M1-12. We asked from the 6 partners that held the main responsibility in delivering the assessed deliverables to evaluate the contributions that they received from other partners. In the below graph, it can be concluded that the level of involvement was deemed satisfactory.

Figure 13 Partner collaboration



3.2 WORK PACKAGE EVALUATION

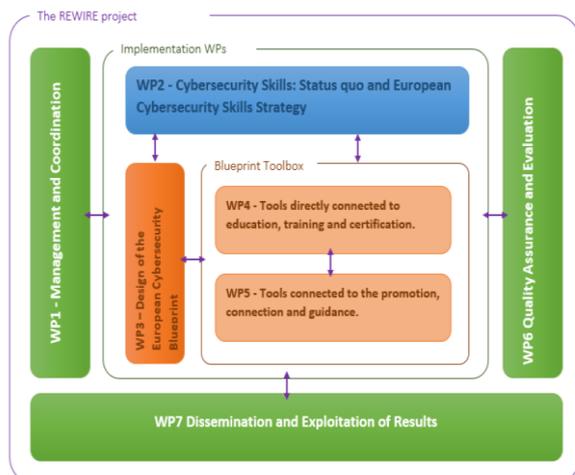


Figure 14 REWIRE work packages

To tackle the objectives of the REWIRE and to deliver tangible project results, the project is structured in seven interrelated work packages. REWIRE is implemented through three horizontal work packages and four core work packages that will lead to core results and activities.

Each work package contains performance indicators which are measured by the corresponding WP leader through the WP Leader Evaluation Form. The below figure lists key performance indicators for impact regarding overall performance.

Impact	<ul style="list-style-type: none"> • Number of persons trained (at least 2.000 ICT professionals in total) • Number of profiles updated/created • Number of stakeholders reached and involved in project activities (at least 1.500) 	<ul style="list-style-type: none"> • User experience/satisfaction • Number of profiles updated/created • Number of stakeholders reached and involved in project activities
--------	---	---

Figure 15 Impact indicators

Four work packages were active during reporting period M1 – 12 and their performance is examined below.

Work Package 1 | Management and Coordination

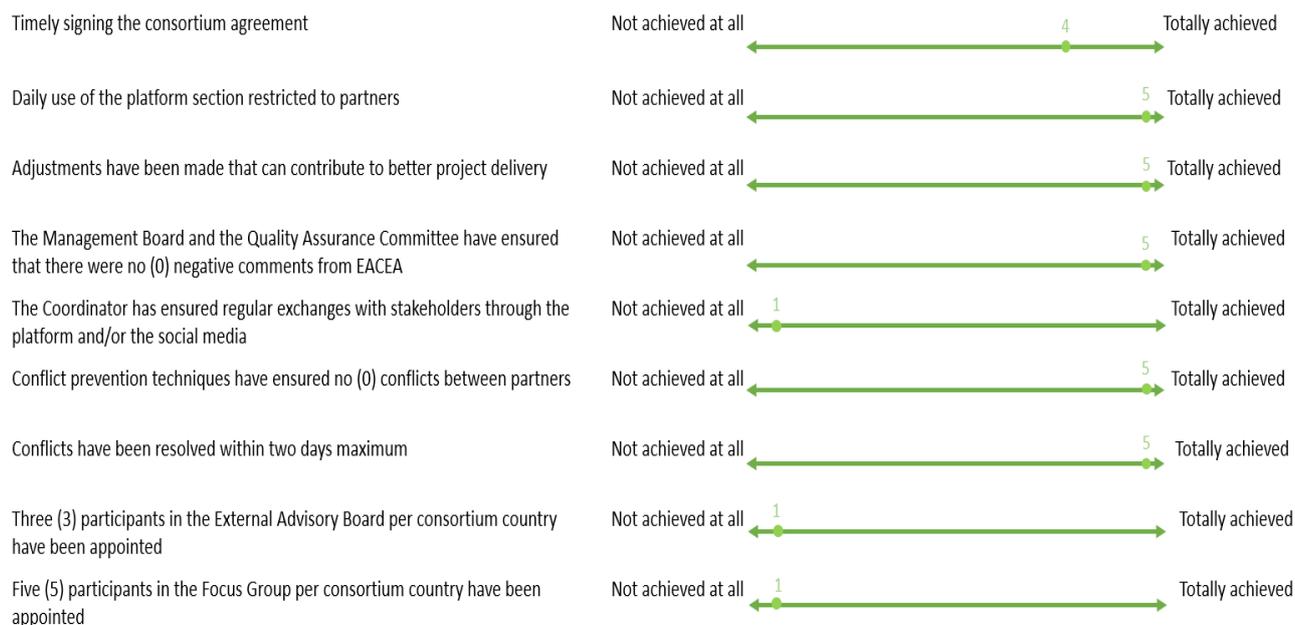
WP1, led by MRU, delivered most tasks for reporting period M1 – 12 (R1.1. Consortium Agreement, R1.2. Project Management Handbook, R1.3. EAB framework, R1.4. Coordination and Communication Platform, R1.5. Project meetings: kick-off and project meeting M8, R1.6 Progress Report #1 – M12) except for R1.8 Open Data procedures and guidelines that was in progress and was finalized right after the end of the reporting period. As per below overview, the WP1 milestones for reporting period M1 – 12 were reached.

Milestones of Work Package 1	Reached/ Partially reached / Not reached
R1.6 Progress Report #1 – M12	Reached

Table 1 WP1 milestones

WP1 reached the majority of each KPIs. The next QA output will elaborate on the measures that the coordinator has taken to address a few deviations.

Figure 16 WP1 indicators



In addition to the above, WP1 reached fully the following indicators:

- Maximum three (3) corrective measures applied.
- At least one (1) DPO appointed and an analysis carried out regarding the privacy requirements imposed by European, Project and National laws, regulations and rules

Work Package 2 | Cybersecurity Skills: Status quo and European Cybersecurity Skills Strategy

WP2, led by BUT, concluded most tasks for reporting period M1 – 12 (R.2.1.1. PESTLE Analysis results, R.2.2.1. Stakeholder database, R.2.2.2. Cybersecurity Skills Needs Analysis). Extra time and effort were needed for the conclusion of R.2.2.2 Cybersecurity Skills Needs Analysis and R.2.2.3 Methodology to anticipate future needs which led also to the postponement of the deadline for R.2.3.1. Cybersecurity Skills Strategy. As per below overview, half of the WP2 milestones for reporting period M1 – 12 were reached. The Cybersecurity Skills Strategy is in progress and will be included in the next reporting period.

<i>Milestones of Work Package 2</i>	<i>Reached/ Partially reached / Not reached</i>
R.2.2.2. Cybersecurity Skills Needs Analysis – M8	Reached
R.2.3.1. Cybersecurity Skills Strategy – M12	Partially reached

Table 2 WP2 milestones

Linked to the above, it was for early for WP2 to assess some of its KPIs as the analysis was still ongoing at the end of the reporting period. WP2, through the PESTLE analysis report which received a good rating from the partners, identified a number of factors that could impact the future of the sector and by the end of the reporting period it had identified a substantial number of stakeholders that will increase overtime in order to reach the project’s goal (see further below, WP7 – Dissemination and exploitation of results). An additional achievement was a conference article on PESTLE analysis was submitted to the ARES-ETACS conference.

Number of PESTLE factors identified, which can impact the cybersecurity sector	31
Number of stakeholders identified	507
Number of areas that need to be further researched and analysed	2
Number of skills mismatches and gaps currently existing in both national and EU level	0
Number of existing and emerging skills needs identified	0
Number of strategies measures, activities, milestones and results included in the Cybersecurity Skills Strategy	0

Table 3 WP2 indicators

Work Package 6 | Quality Assurance and Evaluation

WP6, led by ReadLab, concluded most of the tasks for reporting period M1 – 12 (R6.1 Quality Assurance Plan, R6.2 Quality Assurance Report #1) except for the R6.4 Impact Evaluation Report – M12 that took longer time to conclude. As per below overview, the majority of WP6 milestones for reporting period M1 – 12 were reached. The Impact Evaluation report – M12 is ready for peer review and will be included in the next reporting period.

<i>Milestones of WP6</i>	<i>Reached/ Partially reached / Not reached</i>
R6.1 Quality Assurance Plan – M3	Reached
R6.3 Quality Assurance Report – M8	Reached
R6.4 Impact Evaluation Report – M12	Partially reached

Table 4 WP6 milestones

According to the quality assurance and evaluation procedure, several questionnaires were administered and collected by ReadLab in order to receive partner feedback on project performance as per identified quality criteria, peer-review feedback on deliverables, WP leaders’ feedback on WP performance and risk analysis. There were no interviews taking place even though the next QA output will aim at incorporating feedback from semi-structured interviews with WP leaders. As per below overview, the first QA report (M1 - 8) identified a good number of evaluation criteria and recommendations.

Number of evaluation criteria identified	24 in total
Number of evaluation questionnaires collected	71 in total

Number of interviews conducted	0
Number of recommendations made	20 in total

Table 5 WP6 indicators

Work Package 7 | Dissemination and Exploitation of Results

WP7, led by EFVET, delivered all tasks (R7.1. Stakeholders Analysis, R7.2 Targeting key policymakers, R7.3 Dissemination Plan, R7.4 REWIRE website, R7.5 Portfolio of dissemination material together with a dissemination log). As per below overview, WP7 milestones for reporting period M1 – 12 were reached.

<i>Milestones of WP7</i>	<i>Reached/Not reached</i>
REWIRE portfolio of dissemination material (M4)	Reached

Table 6 WP7 milestones

Due to low stakeholder involvement at the beginning of the project, that was identified in QA Report No.1 and is currently discussed at WP and Consortium level in order to create synergies and increase outreach, WP7 has reached partially its KPIs. The next QA output will elaborate on the corrective measures that have been undertaken to increase the outreach and visibility of the project objectives, final results and future online and/or offline face to face activities. Considering that we have only reached the first year of a four-year project with many activities starting later, WP7 is on track.

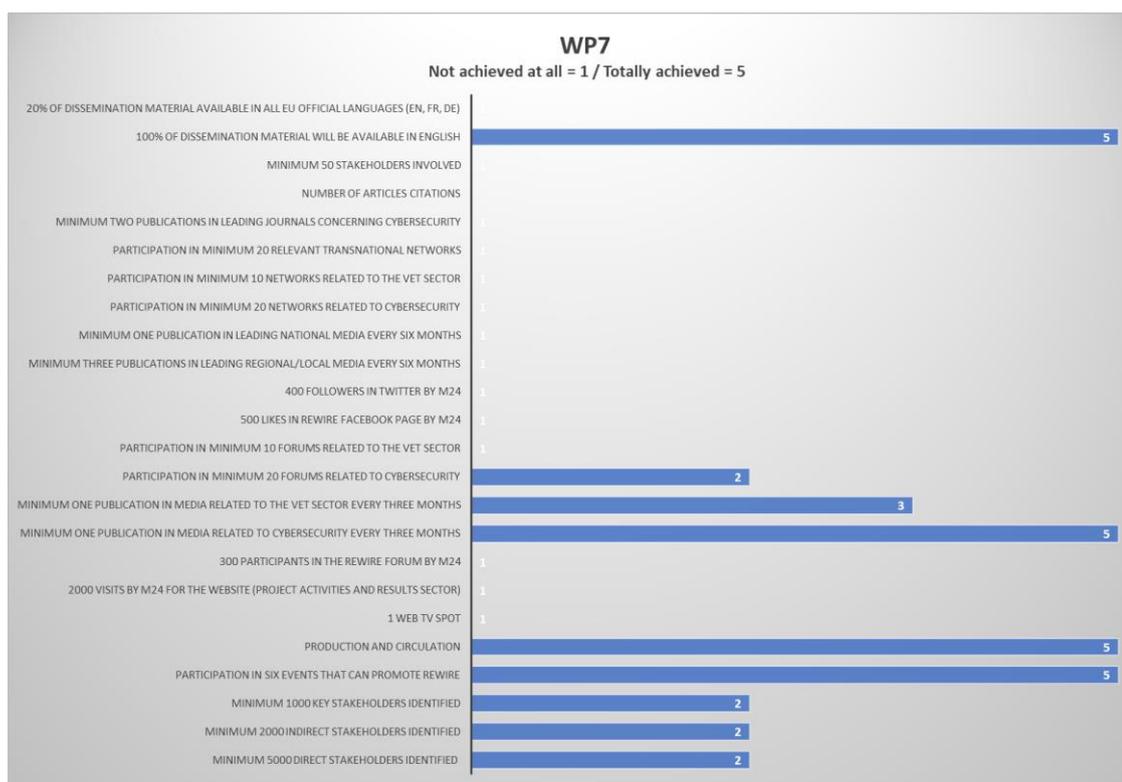


Figure 17 WP7 indicators

4 STAKEHOLDERS

4.1 STAKEHOLDERS ANALYSIS

So far, 732 stakeholders (508 in 31 countries when the stakeholder analysis report was drafted) have been identified and mapped in a commonly shared file in the REWIRE project platform. Out of those stakeholders, a total of 147 policymakers were identified by REWIRE partners in 14 different countries operating at local, regional, national, and European levels.

They were mapped in 3 main categories, namely: primary stakeholders (directly interested in the project's activities), secondary stakeholders (indirectly affected) and key stakeholders. The previously identified categories of stakeholders were also used, in recognition of their relevance in the cybersecurity sector namely: End Users- ICT Professionals; Academia/ Research Institutes; Higher Education; Education and Training providers/VET providers/ VET Networks; Industrial/Sectorial partners/ Companies/Industry; Certification and Standardisation Bodies; Governments/ Authorities/ Policymakers.

The steps that were used for the mapping were the following:

- Listing per name of the organisation, country, geographical scope and category of stakeholder
- Identifying each Stakeholder's level of influence and importance to the project taking into consideration its goals and activities planned
- Analysing the stakeholders based on the attributed level of influence and importance

This resulted in grouping the stakeholders in 4 main categories which determine the level of priority in terms of communication and engagement (Group A – Meet the Needs/Keep Satisfied, Group B - Key player/Engage, Group C – Keep Informed, Group D – Monitor). A detailed analysis can be found in R7.1 Stakeholder analysis report.

This mapping is an important reference point for the dissemination and exploitation strategies and plans of the REWIRE project. Regardless of categorisation, information related to project is shared with all groups. As an example, the first project newsletter was sent to our stakeholders and disseminated on the project [website](#), on [Facebook](#) and [LinkedIn](#) in mid-October 2021. All partners were tagged to maximise the viewers of both newsletter and website.

4.2 STAKEHOLDER EVALUATION FORM

According to the QA plan, project impact is also monitored through the stakeholder evaluation form to assure that *“target groups are satisfied and use the products and methodologies developed by the project, and targets planned for dissemination and exploitation are met”*. This form should *“be distributed after each project session where tangible project results are presented, ie. events or meetings where stakeholders are engaged such as training seminars and awareness raising events that will take place in partners' countries”*.

Since there were no activities directly involving stakeholders and few core package results were finalised during the reporting period, no use of this form was made. To receive

stakeholders' feedback, we have decided to use surveys that will be shared via communication channels (next newsletters and social media posts) and, also, by directly following-up with certain stakeholders.

5 CONCLUSION

The results of the internal evaluation indicate that the REWIRE project partners are satisfied with the achieved deliverables and that most of the work package milestones and key performance indicators for the period M1 to M12 of the project delivery, namely from November 2020 to October 2021, were reached. Considering the above graphs and tables and that, as we are at the end of the first project year, it is possible to assess the impact of the project only to a limited extent, we think that the whole project has maintained a high level of performance and collaboration.

6 REFERENCES

REWIRE project – R.6.1 Quality Assurance plan

REWIRE project – R.6.2 QA report no. 1

REWIRE project – R7.1 Stakeholder analysis report

REWIRE project – R7.2 Targeting key policymakers

7 LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/Definition
ARES - ETACS	International Conference on Availability, Reliability and Security - Workshop on Education, Training and Awareness in Cybersecurity
BUT	Brno University of Technology
EAB	External Advisory Board
EFVET	European Forum of Technical and Vocational Education and Training
EVTA	European Vocational Training Association
GDPR	General Data Protection Regulation
KTH	Kungliga Tekniska Hoegskolan (Royal Institute of Technology in Stockholm)
KPI	Key Performance Indicator
ICT- Professionals	Professionals working on the sector of information and communications technology
M1	Month 1
MRU	Mykolas Romeris University
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
QA	Quality Assurance
ReadLab	Research Innovation and Development Lab
SME	Small and medium-sized enterprise
VET	Vocational Education and Training
WP	Work Package

Table 7 List of abbreviations and acronyms

8 LIST OF FIGURES

Figure 1 EAB Framework	7
Figure 2 R1.7 Privacy policy & procedures	8
Figure 3 Open data procedures and guidelines	9
Figure 4 PESTLE Analysis results	11
Figure 5 Cybersecurity skills needs analysis	12
Figure 6 Methodology to anticipate future needs	13
Figure 7 Quality Assurance Plan	14
Figure 8 Quality Assurance Report M1 -- M8	15
Figure 9 Stakeholders analysis	16
Figure 10 Targeting key policymakers	17
Figure 11 Dissemination plan	18
Figure 12 Project website	19
Figure 13 Partner collaboration	20
Figure 14 REWIRE work packages	21
Figure 15 Impact indicators	21
Figure 16 WP1 indicators	22
Figure 17 WP7 indicators	24

9 LIST OF TABLES

Table 1 WP1 milestones	21
Table 2 WP2 milestones	22
Table 3 WP2 indicators.....	23
Table 4 WP6 milestones	23
Table 5 WP6 indicators.....	24
Table 6 WP7 milestones	24
Table 7 List of abbreviations and acronyms.....	29