Project Code :	2020-1-NO01-KA202-076464								
Action Type :	KA202								
SubProgram :	Strategic Pa	Strategic Partnerships for vocational education and training							
Agency :	NO01								
Call :	2020	Round :	1	Date :	21.04.2020				



Assessment Sheet

Erasmus + Call for Proposals 2020

Name of the Organisation:	Godalen Videregående Skole
Title of the proposal:	Cyber Clever-Integration of cyber security in initial VET-education
Reference No:	2020-1-NO01-KA202-076464 - Beneficiary Report-1

I. ASSESSMENT CONCLUSION

Criteria	Score
Impact and dissemination	36
Quality of the project design and implementation	22
Quality of the project team and the cooperation arrangements	14
Relevance of the project/strategy	18
Total:	90

Project Code :	2020-1-NO01-KA202-076464	***
Action Type :	KA202	* * * *
SubProgram :	Strategic Partnerships for vocational education and training	****
Agency :	NO01	
Call :	2020 Round: 1 Date: 21.04.2020	

Impact and dissemination	Score
	36

Impact is well sorted out along target groups and levels, from the local to the European scene. The main target group was teachers and trainers, secondly students and stakeholders in general. The use of tangible and intangible indicators clearly served the purpose of measuring impact. Yet the reporting on tangible or quantitative targets seems somewhat inflated, particularly when measuring the number of persons reached through social media and the dissemination activities in general, claimed to add up to 20,000 people.

The impact at the level of the participating organisations and institutions seems considerable, witnessed by the vocational schools of the partnership now using the course materials in several or all of their study programmes, while the HEIs have integrated parts of the materials in ongoing teacher training and continuing vocational courses.

Also the dissemination activities are well sorted out along the abovementioned target groups and levels (from the local to the European). A sufficient range of tools, channels and platforms were adopted to disseminate the project results.

An asset is that the course materials (from IO3) are available for free download in English, Norwegian, Icelandic, German, Turkish, Swedish and Estonian on several platforms (project's website, coordinator's website, SharePoint, later also Salto Youth). It is also positive that the project website will be operational for at least 5 years after the project expires.

Impact on wider stakeholders was achieved when leaning on associated partners at a regional or local level, as well as during the multiplier events. Wider impact can also accrue from the partner NTNU now planning to set up part 2 of "cybersecurity for teachers", conceived as a very practical programme with exercises and student-centred methods drawing on the practical exercises from part 1 of the course. Similar impact can be expected if the HEI HKR (i.e. the Swedish partner) finally decides to set up a micro-credit programme for teachers.

The beneficiary plans for maintaining and sustaining the project outputs and outcomes concentrate on all partners regularly providing further and continuing training to their staff, as well as competence development for other teachers in all programme areas. This probably means programmes both for vocational and general programmes at EQF 4-5, but this vision is not further specified. When trying to transfer the project results to other contexts, some partners will start developing a new project within the field of Cyber Security in a collaboration with SMEs and primary schools.

All this is positive and the coordinating institution hints at a future project differently designed than the one now reporting, namely with a smaller group of development partners complemented by a larger group of partners for LTTAs, testing and implementation. This reflection seems appropriate in view of the reported experience with frequent changes of IO leaders for reasons of competence lacunae.

Quality of the project design and implementation	Score
	22

The main obstacle encountered during the implementation of the work plan was Covid-19 restrictions, imposing a kind of standstill in the partner institutions, later alleviated by an extension of the project contract.

The project objectives were successfully attained and all IOs were delivered with quality, including the supporting LTTAs and MEs. The way in which stakeholders and end users were approached and involved was primarily by attending local multiplier events, and by piloting or testing of the training course. The FR claims that 3500 persons not receiving a specific grant benefited from or were targeted by the activities organised by the project. Yet this estimate is not well supported by indicators.

The approach to monitoring and quality assurance was inspired by recognised management theories, while using qualitative and quantitative indicators to monitor progress. Internal evaluation of how the partners and the project as such performed, is well accounted for, while what is called the "external assessment of the achievements" is presented in very vague terms.

The quality of the IOs is high, well aligned with the EQF and supplied with precise learning outcomes inscribed in a KSC framework. The pedagogical and didactical aspects of the curriculum and the five-module course are well catered for. Overall, the high quality suggests that the collaboration between HEIs and initial vocational schools was fruitful. As pointed out in the FR, the idea of endowing initial VET with Cyber Security in all subjects and study programmes is innovative per se. Innovation also lies in developing a cybersecurity curriculum for VET teachers together with students (ranging from initial vocational training to a university level) through a LTTA (Blended mobility of VET learners). Strikingly, the Status Report on Cyber Security (cf. IO1) does not account for the US

Project Code :	2020-1-NO0	***				
Action Type :	KA202	* * * *				
SubProgram :	Strategic Par	****				
Agency :	NO01					
Call :	2020	Round :	1	Date :	21.04.2020	

programme GenCyber from which the partners sought inspiration, which is a minor shortcoming.

The European state-of-the-art in the targeted field was well analysed in IO1. Among the partners themselves, only the applicant organisation had prior experience with Cyber Security, thus suggesting a kind of dissemination project towards other countries, ranging from Iceland to Turkey, though there were i.a. partners from Finland and Estonia well rooted in national strategies of digitalisation. The state-of-art was also improved within the applicant organisation, represented in the project by one of its six departments, now all of the school's study programmes are offering a Cyber Summer School for their students.

The LTTAs consumed 37,100€ against 49k€ as originally planned, probably for reasons of mobility restrictions during the pandemic, but this lower spending is not well explained. Both activities were held on site, a Short-term Joint Staff Training event in EE and a Blended Mobility of VET learners in NO. The first LTTA gathered teachers graduated at universities and administrators, the second was attended by students from initial vocational training to university level who were accompanied by trainers. Both activities called on external expertise, including from local enterprises, which is an asset.

Given that the course (cf. IO3) consists of 11 hours per module of which there are five at EQF level 4-5, there should be ample room for awarding ECTS to the VET teachers who have passed this course. Yet a mid-term assessment is said to conclude that no existing European transparency and recognition tools would give added value to any participant, because no practical change in salary or recognition in the partner institutions was envisaged. While the first argument might be true, the second is questionable, as the project partners have considerable persuasive power to explain the course participants which value European recognition tools does have at institutional level. In the end, only in-house certificates (for each partner?) were awarded throughout the project period.

Quality of the project team and the cooperation arrangements	Score
	14

The partnership of eight from seven countries comprised two HEIs, four VET schools and one private adult education centre; finally one accreditation, certification or qualification body. Different fields of education were therefore well covered by the partnership that also leaned on one associated partner in most countries, for example in NO where the Norwegian national cyber security authorities were advisors to the project. Overall, the associates were useful for disseminating the results at a local level, while also communicating perspectives from below to the national teams in all partnership countries.

Roles, tasks and responsibilities were from the outset well divided among partners. In particular, lead roles for developing the course modules (IO3) were well distributed between the partners. Later, IO responsibilities underwent some modifications as the lead partners of some intellectual outputs were changed. This particularly occurred when one IO leader was replaced during staff turnovers but then turned out to lack sufficient experience. Being the most experienced partner, the coordinator then took over lead roles, without any clear sign that this entailed internal discontent.

The relevance of the cooperation and collaboration mechanisms was particularly demonstrated in developing the materials for IO3, unfolding in fruitful team work that entailed learning materials of high quality.

Negative aspects of the communication process seem only related to COVID-19 restrictions, hampering the process of team building and the forging of ownership around joint work tasks. Hence, the FR informs that the restriction of only arranging online meetings in reality postponed joint efforts for around six months, even though the work on IO1 and IO2 had started before the lock-downs.

Relevance of the project/strategy	Score
	18

The original objective was maintained, namely to develop a joint programme for Cyber Security for teachers in initial VET, with the high ambition to train ordinary teachers to teach cybersecurity to every student. The problems encountered during the pandemic did not deviate the partners from reaching this objective.

The way in which the partners, according to their mission and professional profiles, are using the project outputs suggests that they now can benefit from positive and long-lasting effects.

In the absence of similar training programmes in Europe (cf. IO1), the partners maintained their initial idea to seek inspiration in the US GenCyber programme, which they complemented, notably by inscribing the new programme in the EQF.

There are strong indications that the project brought forth positive and sustainable effects for persons involved in LTAAs, teachers and

Project Code :	2020-1-NO0:	***				
Action Type :	KA202	* * * *				
SubProgram :	Strategic Par	****				
Agency :	NO01					
Call :	2020	Round :	1	Date :	21.04.2020	

stakeholders attending local multiplier events as well as persons engaged in piloting or testing of the training course.

The five modules of the training course (IO3) are well aligned with the EQF and supplied with precise learning outcomes according to a framework of Knowledge, Skills and Competences (KSC).

Added value in terms of learning outcomes, improved knowledge, skills and competence is reported for teachers appreciating that the developed materials were apt for trainers without deep knowledge in ICT. And among students, added value accrued from the design of a training programme not particularly addressing VET students in Electro and ICT, but the whole range of vocational programmes offered by schools.

Overall comments to the beneficiary

The original objective was maintained, namely to develop a joint programme for Cyber Security towards teachers in initial VET. There are strong indications that the project brought forth positive and sustainable effects among persons involved in LTAAs, teachers and stakeholders attending local multiplier events, alongside persons engaged in piloting or testing of the training course.

The quality of the IOs is high, well aligned with the EQF and supplied with precise learning outcomes inscribed in a framework of Knowledge, Skills and Competences. Given that the course (cf. IO3) consists of 11 hours per module of which there are five at EQF level 4-5, there should be ample room for awarding ECTS to the VET teachers who have passed this course. Yet a mid-term assessment surprisingly concluded that no existing European transparency and recognition tools would give added value to any participant.

Different fields of education were well covered by the partnership that also leaned on one associated partner in most countries. The relevance of the cooperation and collaboration mechanisms was particularly demonstrated in the development of training materials for the course (cf. IO3).

Measures for impact and dissemination are well sorted out along target groups and levels, from the local to the European scene

Impact on wider stakeholders was achieved when leaning on associated partners at a regional or local level, as well as du multiplier events. Yet the reporting on tangible or quantitative targets seems somewhat inflated.						•