GEIGER

Deliverable D6.2

Year One Report

Point of Contact	Bettina Schneider
Institution	Fachhochschule Nordwestschweiz (FHNW)
E-mail	bettina.schneider@fhnw.ch
Phone	+41 61 279 17 54

Project Acronym	GEIGER
Project Title	GEIGER Cybersecurity Counter
Project Website	project.cyber-geiger.eu
Grant Agreement No.	883588
Topic	H2020-SU-DS03
Project start date	01/06/2020
Period Covered Report	from 01/06/2020 to 31/05/2021
Reported on basis of	Original Grant Agreement
Dissemination level	Public
Due date	31/05/2021
Date of submission	31/05/2021
Lead partner	FHNW
Contributing partners	UU, TECH.EU, KSP, PHF, MI, KPMG, BBB, ATOS, SKV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Authors	Bettina Schneider (FHNW), Samuel Fricker (FHNW), Natalie Jonkers (FHNW), Petra Maria Asprion (FHNW), Heini Järvinen (Tech.eu), Stelian Brad (CLUJIT), Marco Spruit (UU), Bernd Remmele (PHF), Jose Ruiz (ATOS), Wissam Mallouli (MI), Katharina Hoffmann (FHNW)
Reviewers	MI, ATOS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Revision History

Version	Date	Author	Comment
0.1	22/12/2020	Bettina Schneider, FHNW	Initial version of the report based on • What was announced in GA (innovations, objectives, impacts) • ToC provided by Swiss NCPs • inputs provided by WP leads in CM2 • inputs by partners in EMDESK • existing deliverables • existing management processes such as risk management
0.2	04/01/2021	Samuel Fricker, FHNW	Review of Document
0.3	06/01/2021	Bettina Schneider, FHNW	Restructuring the report based on EC template for periodic reports: https://ec.europa.eu/research/participants/data/ref/h2020/gm/reporting/h2020-tmpl-periodic-rep_en.pdf
0.5	03/03/2021	Bettina Schneider, FHNW	Restructuring the report based on feedback from scientific and technical coordinators
0.6	12/04/2021	Bettina Schneider, FHNW, Heini Järvinen, Tech.eu	Questionnaire input from WP5 & 6 incorporated
0.7	12/04/2021	Petra Asprion, FHNW	Update on the Advisory Board section
0.8	13/04/2021	Bettina Schneider, FHNW Jose Ruiz, ATOS	Questionnaire input from WP2 incorporated
0.9	15/04/2021	Natalie Jonkers, FHNW Jose Ruiz, ATOS	Project Description, Input Project Management Updated input on data management in chapter 7
1.0	26/04/2021	Heini Järvinen, Tech.eu	Review of WP5 contents
1.1	28/04/2021	Bettina Schneider, FHNW Bernd Remmele, PHF	Questionnaire input from WP3 incorporated
1.2	04/05/2021	Marco Spruit, UU	Chapter 9, Readiness for Piloting
1.3	06/05/2021	Heini Järvinen, Tech.eu	Chapter 5, Dissemination
1.4	06/05/2021	Bettina Schneider, FHNW	Check of abbreviations and glossary
1.5	10/05/2021	Samuel Fricker, FHNW Bettina Schneider, FHNW	Review Feedback of Samuel Fricker incorporated
1.6	17/05/2021	Samuel Fricker, FHNW Bettina Schneider, FHNW	Questionnaire Input from WP1 incorporated
1.7	19/05/2021	Bettina Schneider, FHNW Katharina Hoffmann, FHNW	Review Feedback from FHNW research support incorporated
1.8	20/05/2021	Stelian Brad, CLUJIT	Chapter 6, Innovation and Impact
1.9	25/05/2021	Bernd Remmele, PHF	Review of WP3-related contents in the report

2.0	25/05/2021	Heini Järvinen, Tech.eu	Review of WP5-related contents in the report
2.1	26/05/2021	Jose Ruiz, ATOS	Review of WP2-related contents in the report and overall report review
2.2	26/05/2021	Petra Maria Asprion, FHNW	Review chapters 1-3
2.3	27/05/2021	Samuel Fricker, FHNW	Reporting of WP7 and ethics status
2.4	27/05/2021	Samuel Fricker, FHNW	Overall report review
2.5	30/05/2021	Petra Maria Asprion, FHNW	Review chapters 4-9
2.6	31/05/2021	Stelian Brad, CLUJIT	Review of chapter 6
2.7	31/05/2021	Wissam Mallouli, MI	Overall report review
2.8	31/05/2021	Natalie Jonkers, FHNW	Language check, formatting, review
2.9	31/05/2021	Samuel Fricker, FHNW Bettina Schneider, FHNW	Final check before submission

Contents

Purpose and Structure of the Document

This document is representing the D6.2 Year One Report, a public deliverable that was promised as part of the overall GEIGER project deliverables. With its submission in month 12 after project start (M12), the report summarises the work performed in the GEIGER project in ‘year one’ (M1-12).

D6.2 provides an overview of the project progress, deliverables, milestones, and information about the status for dissemination, innovation, and creation of impact.

The first section of D6.2 provides a general description of the GEIGER project and introduces the concept, the work packages, and overall objectives. This general description is followed by an elaboration of the overall project results, deliverables & milestones. Section 3 summarises each work package's progress towards the objectives and lists the achievements and exploitable results. The impact that has been created so far and the fulfilment of related KPIs that measure the project impact/achievements are the focus of section 4. Next, in section 5, dissemination activities are described. In section 6, exploitation and innovation activities, further efforts regarding policy and standards contributions are described. In section 7, ethics, diversity, and data management are summarised. Section 8 provides background on project management. Finally, the deliverable closes with an outlook on the upcoming project period.

Abbreviations, participant short names and glossary

Abbreviations

AB	Advisory Board
API	Application Programming Interface
CERT	Cybersecurity Emergency Response Team
CSIRT	Cybersecurity Incident Response Team
CEO	Chief Executive Officer
CM	Consortium Meeting
CSD	Cyber Security Defender
CtA	Call to Action
D	Deliverable
DMP	Data Management Plan
DoA	Description of Action
EB	Executive Board
EC	European Commission
EOY	End of year
EU	European Union
EY	Ernst & Young
GA	Grant Agreement
GDPR	General Data Protection Regulation
IP	Intellectual Property
IT	Information Technology
ISAC	Information Sharing and Analysis Centre
IUA	Interpretation and Use Argument
KPI	Key Performance Indicator
M	Month
ME	Micro-Enterprise
MoU	Memorandum of Understanding
MS	Milestone
MSE	Micro and Small Enterprise
MVP	Minimum Viable Product
NCP	National Contact Point
NIS	Network and Information Security
NL	The Netherlands
PMH	Project Management Handbook
PMO	Project Management Office
PO	Project Officer
PPT	PowerPoint
REA	Research Executive Agency
SME	Small and Medium-Sized Enterprise

ToC	Table of contents
TRL	Technology Readiness Level
UI	User Interface
UK	United Kingdom
UX	User Experience
WP	Work Package

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
TECH.EU	Fores Media Limited
KSP	Kaspersky Lab Italia Srl
PFH	Pädagogische Hochschule Freiburg
MI	Montimage EURL
KPMG	Somekh Chaikin Partnership
BBB	Berufsfachschule BBB Baden
ATOS	Atos IT Solutions and Services Iberia SL
SKV	Schweizerischer KMU Verband
HAAKO	Haako GmbH
CERT-RO	Centrul National de Raspuns la Incidente de Securitate Cibernetica
CLUJ IT	Asociatia Cluj IT
E-ABO	e-abo GmbH
SCB	Braintronix Srl
PT	Public Tender Srl
SRA	Samenwerkende Registeraccountants en Accountants-Administratieconsulenten
CL	Coiffure Loredana

Glossary

Term	Description
Competence	Competence is the capability of a person to deal with a specific task, i.e., there are always two sides: the operation/action and the object of the operation. Accordingly, a usual definition of competence consists of an operator and an object. Competence usually refers to declarative knowledge (about a topic) and practical skills (acting with a topical object). It can also include motivational and volitional aspects, i.e., the ability and readiness to fulfil a task.
Competence Grid	For complex educational purposes, it is useful to structure the set of competencies to be trained. First, this concerns the (cumulative) competence development, from easy to difficult. This development can refer to the

advancement of the complexity of the topical issue and the operation. Second, as competences refer to tasks, it can be useful to distinguish topical fields that systematically, i.e., in regard of learning, subdivide the given field of knowledge.

Curriculum A curriculum defines the set of trainings/modules of a specific course in a general manner. In the given context, this implies that there will be different curricula for the heterogeneous target groups that include specific selections from the competence grid and a set of topics. In this sense, curriculum refers to the link between the competence grid and the syllabus.

DEIP DEIP Protocol (or Intellectual Capital Protocol) is a Web 3.0 Layer-2 application specific protocol for intangible assets and derivatives. The protocol enables discovering, evaluation, licensing, and exchange of intangible assets. It is designed specifically for intangible assets tokenization (as F-NFT), governance (via DAO), and liquidity (via DeFi instruments and derivatives).
https://www.deip.world/

DevOps DevOps is a set of practices that combines software development (Dev) and IT operations (Ops). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.

DTC The Netherlands (NL) Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security jointly launched the 'Digital Trust Center' programme. The DTC's mission is to increase the resilience of businesses to cyber threats (https://www.digitaltrustcenter.nl).

EMDESK EMDESK is an all-in-one project and work management solution for collaborative research projects (https://www.emdesk.com).

ENISA The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe (https://www.enisa.europa.eu).

MISP Malware Information Sharing Platform for sharing, storing and correlating indicators of compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

Multiplier An organisation or individual who contributes to the promotion of and communications around the project towards its target audiences, amplifying the messages and bringing higher visibility to the project.

NCSC The ´National Cyber Security Centre´ is Switzerland's competence centre for cybersecurity (https://www.ncsc.ch).

P2PKOS Project to policy kick off seminar for security research by EC.

SCORM A set of technical standards for eLearning products providing a communication method and data models that allow eLearning content and Learning Management Systems to work together.

SME&ME, MSE Terms used interchangeably for the end-user group of the GEIGER project, the micro, small and medium-sized enterprises also sometimes referred to as small businesses in this document.

Syllabus A syllabus defines the set of trainings/modules of a specific course in a detailed manner. In addition to the competences and topics to be taught, a syllabus can include lesson plans, education materials, references to further resources etc.

xAPI The Experience API (xAPI) is an e-learning software specification that allows learning content and learning systems to speak to each other in a manner that records and tracks all types of learning experiences.

X-ISAC A supporting Information Sharing and Analysis Centre for other ISACs, information sharing communities or CSIRT networks. It provides core software, cross-sector threat intelligence, taxonomies, and open standards.

List of tables

List of figures

1 Project Description

The GEIGER Horizon 2020 innovation project develops a so-called 'Geiger Counter' for cybersecurity. This indicator will help SMEs&MEs (MSEs) become aware of their risks. Explanations are provided to the risk assessment with recommendations concerning data protection, data privacy, and cybersecurity. Trained security defenders offered assistance to the MSE in implementing the recommendations, thus reducing the risks.

GEIGER will dynamically show the status of the existing cyber threats and it can be used from the web or installed locally on a computer or smartphone. Small businesses can react immediately and take simple measures to significantly lower their risk level, for example, from red to green (see the middle part of Figure 1). The 'GEIGER indicator' will be connected to a 'GEIGER Cloud' and link to a 'GEIGER Toolbox'. The ´GEIGER Framework´ will serve as an 'Information Sharing and Analysis Centre' (ISAC) platform connecting small businesses, related associations, and 'Cybersecurity Emergency Response Teams' and 'Cybersecurity Incident Response Teams' (CERTs&CSIRTs). The project will also build an ecosystem of competent individuals and organisations that offer their support to small businesses by collaborating with schools and partners to develop a standardised learning programme, the 'Certified Security Defenders' (CSDs).

GEIGER will pilot in Switzerland, the Netherlands and Romania. In Switzerland, apprentices can have themselves qualified as 'Certified Security Defenders' at their vocational school. In the Netherlands, the training programmes target accountants. In Romania, small business and start-up owners will be addressed. As part of the certification, the trainees experience cyberattacks against small businesses and learn how a company can protect itself with the help of GEIGER. The Certified Security Defenders will pass on their awareness of cyber risks and the knowledge of possible countermeasures to the company in or with which they are working (see the blue part of Figure 1).

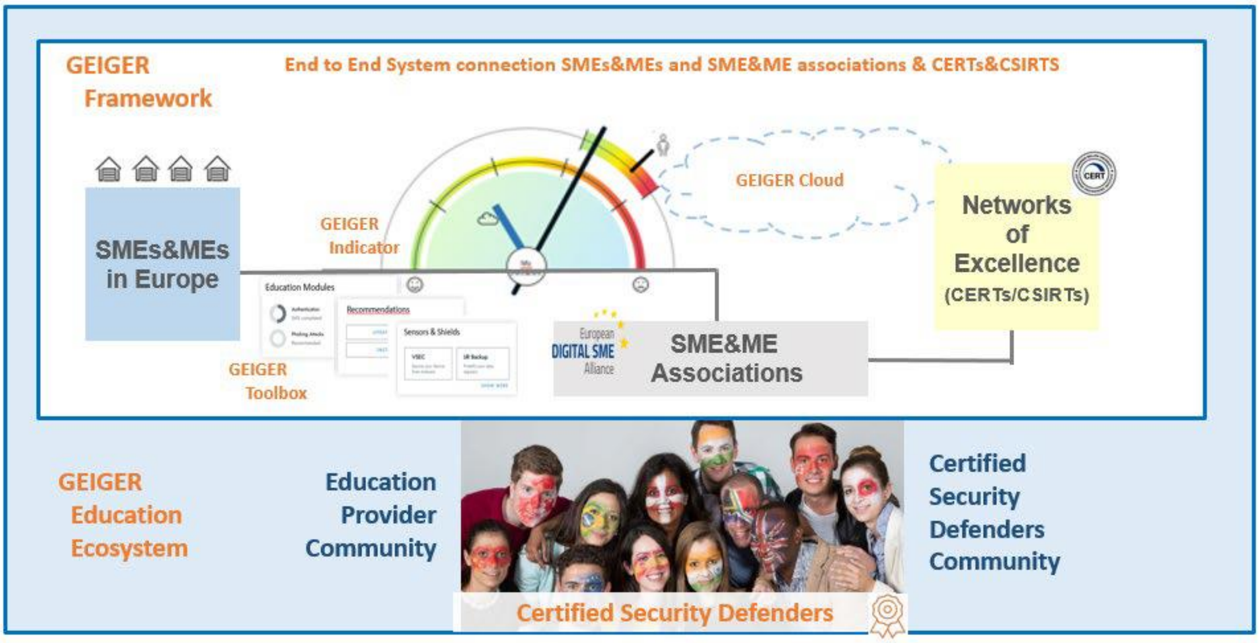

GEIGER Framework
End to End System connection SMEs&MEs and SME&ME associations & CERTs&CSIRTS
SMEs&MEs in Europe
GEIGER Indicator
GEIGER Cloud
CERT
Networks of Excellence (CERTs/CSIRTs)
Education Modules
Recommendations
Sensors & Shields
GEIGER Toolbox
European DIGITAL SME Alliance
SME&ME Associations
GEIGER Education Ecosystem
Education Provider Community
Certified Security Defenders
Certified Security Defenders Community

Figure 1: GEIGER Ecosystem Concept

Figure 1 describes the overall concept targeted for MSEs: Firstly, the GEIGER Framework is enabled by a technological infrastructure. The GEIGER Indicator will be developed, which is a flexible, accurate, easy-to-understand 'Tool' for risk awareness, monitoring (status), and improvement of the status quo (Objective 1). Secondly, a trusted do-it-yourself GEIGER Toolbox for risk reduction is built (Objective 2).

The GEIGER project is composed of seven work packages (WPs), which in their combination ensure the fulfilment of the overall project objectives.

The work package ‘WP1 Requirements, Architecture, and Methodology’ (M1–12) has elicited and analysed the requirements from the use case countries and organisations to specify the GEIGER Framework. The ‘TwinPeaks’ method supported the iterative refinement of the vision into detailed requirements and architecture. Furthermore, the GEIGER Framework enables sharing and exchanging data between different actors targeted for MSEs in the form of an Information Sharing and Analysis Centre (ISAC) platform (Objective 3).

‘WP2 GEIGER Framework’ (started in M4) is building upon the WP1 specifications and takes further the iterative approach. Applying an iterative and agile DevOps process method, WP2 implements the end-to-end GEIGER Indicator, adapts, and integrates the tools into the GEIGER Toolbox. In collaboration with the standardisation and policy task T5.2, the formats and procedures for data exchange are being defined. Building upon these specifications, WP2 iteratively develops the Information Sharing and Analysis Centre (ISAC) components.

‘WP3 Security Defender Education’ emphasises the social aspect by initiating and developing a GEIGER Education Ecosystem to reach the MSEs with a low threshold over their peer groups. In the first year, WP3 focused on developing experiential training and education in a curriculum to bring security, privacy, and data protection experience to MSEs (Objective 4). This curriculum is a good basis for community building. Applying Murphy’s reverse mentoring theory and the community canvas framework, WP3 has already initiated the first steps towards building the Education Provider Community and has conducted some pre-work to initiate the Certified Security Defenders Community (which starts at M13). With this ecosystem concept, the GEIGER project will address the problem of cybersecurity and reduce cyber risks for small businesses regarding awareness, motivation, self-efficacy, and usability.

In the first project period, requirements have been elicited, and technological as well as social components for a Minimum Viable Product (MVP) have been developed. The upcoming project phase will be dedicated to validating and demonstrating the approach in diverse, relevant operational environments (Objective 5) and using the feedback and lessons learned to refine the design and complete the implementation.

‘WP4 GEIGER Validation and Demonstration’ will validate the GEIGER solution in the operational environment of the MSEs within the GEIGER consortium (Technology Readiness Level (TRL) 5), following by validation with external MSEs from the three use case pilot countries (Switzerland, Netherlands, Romania, TRL7).

‘WP5 Dissemination and Exploitation’ will provide showcases for dissemination, concepts for standardisation, and policy contribution. The WP aims at attracting 100’000 MSEs to create a user account for the GEIGER solution. Finally, business experiments necessary to verify the product market alignment for the GEIGER solution and initiate the exploitation of the project results will be carried out.

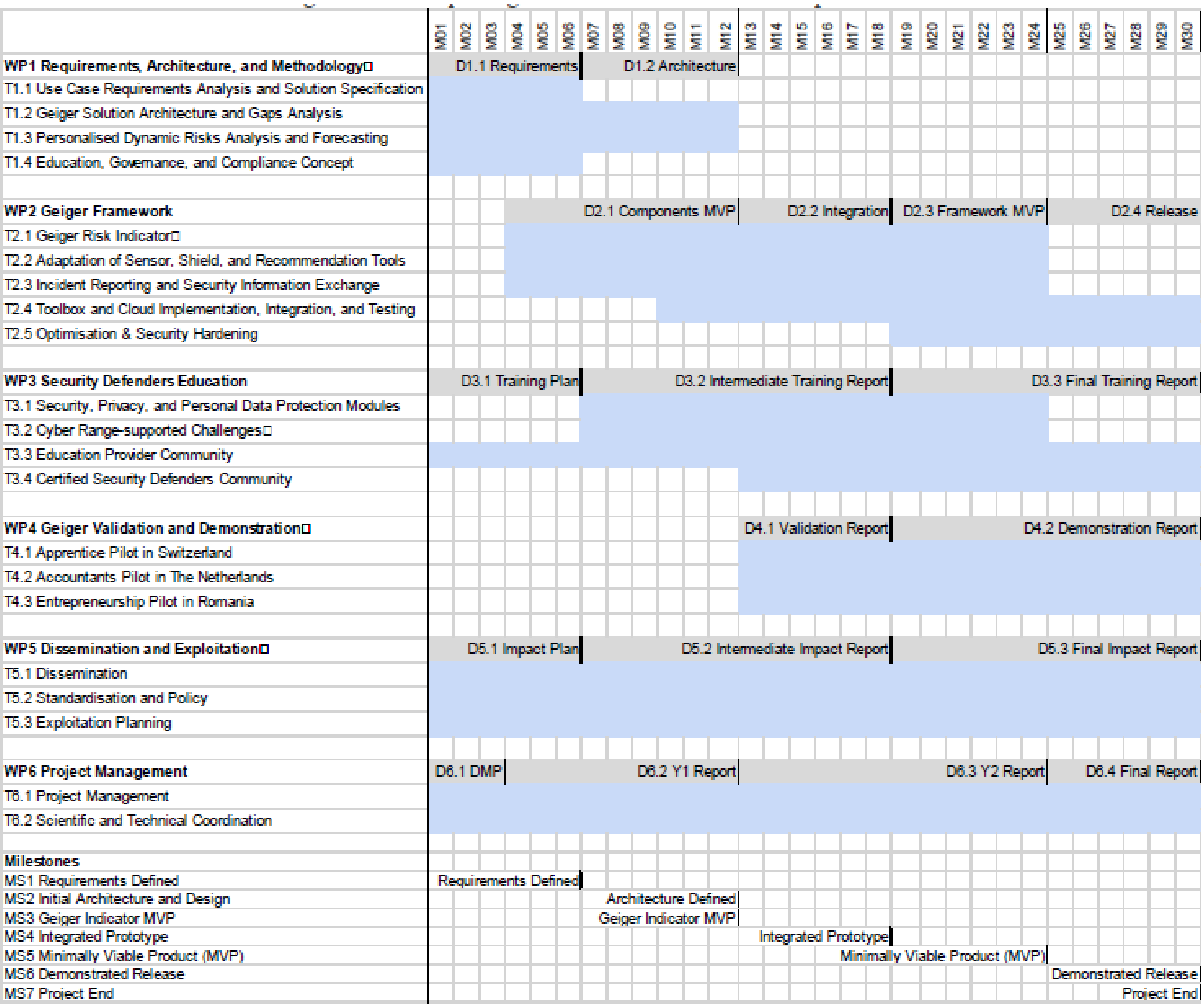
‘WP6 Project Management’ and ‘WP7 Ethics’ serve as enablers for effective and efficient project work and ensure compliance, among others, with data protection and ethics rules.

Table 1 shows the five project objectives from the Description of Action (DoA).

Obj 1: Flexible, accurate, easy to understand indicator ‘tool’ for risk awareness, monitoring (status), and improvement (of the status quo) targeted for MSEs.
Obj.2: Trusted do-it-yourself toolbox for risk reduction of MSEs.
Obj.3: A framework to share and exchange data between different actors targeted for MSEs.
Obj.4: Experiential training and education for Cyber Security Defenders bringing security, privacy, and data protection experience to MSEs.
Obj. 5: Validate and demonstrate the approach in diverse, relevant operational environments.

Table 1: GEIGER Objectives, Retrieved from DoA

Figure 2 provides an overview of the GEIGER work packages and timeline.



	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30
WP1 Requirements, Architecture, and Methodology□	▨	▨	▨	▨	▨	D1.1 Requirements	▨	▨	▨	▨	▨	D1.2 Architecture																		
T1.1 Use Case Requirements Analysis and Solution Specification	🟦	🟦	🟦	🟦	🟦	🟦																								
T1.2 Geiger Solution Architecture and Gaps Analysis	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦																		
T1.3 Personalised Dynamic Risks Analysis and Forecasting	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦																		
T1.4 Education, Governance, and Compliance Concept	🟦	🟦	🟦	🟦	🟦	🟦																								
WP2 Geiger Framework				▨	▨	▨	▨	▨	▨	▨	▨	D2.1 Components MVP	▨	▨	▨	▨	▨	D2.2 Integration	▨	▨	▨	▨	▨	D2.3 Framework MVP	▨	▨	▨	▨	▨	D2.4 Release
T2.1 Geiger Risk Indicator□				🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦						
T2.2 Adaptation of Sensor, Shield, and Recommendation Tools				🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦						
T2.3 Incident Reporting and Security Information Exchange				🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦						
T2.4 Toolbox and Cloud Implementation, Integration, and Testing										🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T2.5 Optimisation & Security Hardening																			🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP3 Security Defenders Education	▨	▨	▨	▨	▨	D3.1 Training Plan	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D3.2 Intermediate Training Report	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D3.3 Final Training Report
T3.1 Security, Privacy, and Personal Data Protection Modules							🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦						
T3.2 Cyber Range-supported Challenges□							🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦						
T3.3 Education Provider Community	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T3.4 Certified Security Defenders Community													🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP4 Geiger Validation and Demonstration□													▨	▨	▨	▨	▨	D4.1 Validation Report	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D4.2 Demonstration Report
T4.1 Apprentice Pilot in Switzerland													🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T4.2 Accountants Pilot in The Netherlands													🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T4.3 Entrepreneurship Pilot in Romania													🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP5 Dissemination and Exploitation□	▨	▨	▨	▨	▨	D5.1 Impact Plan	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D5.2 Intermediate Impact Report	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D5.3 Final Impact Report
T5.1 Dissemination	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T5.2 Standardisation and Policy	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T5.3 Exploitation Planning	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP6 Project Management	▨	▨	D6.1 DMP	▨	▨	▨	▨	▨	▨	▨	▨	D6.2 Y1 Report	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	D6.3 Y2 Report	▨	▨	▨	▨	▨	D6.4 Final Report
T6.1 Project Management	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T6.2 Scientific and Technical Coordination	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Milestones																														
MS1 Requirements Defined						Requirements Defined																								
MS2 Initial Architecture and Design												Architecture Defined																		
MS3 Geiger Indicator MVP												Geiger Indicator MVP																		
MS4 Integrated Prototype																		Integrated Prototype												
MS5 Minimally Viable Product (MVP)																								Minimally Viable Product (MVP)						
MS6 Demonstrated Release																														Demonstrated Release
MS7 Project End																														Project End

Figure 2: GEIGER Project Schedule, Retrieved from DoA

2 Overall Project Progress, Deliverables and Milestones of the Period

2.1 Progress of the Period

Our **main achievements** from the requirement elicitation (WP1) are a) documented requirements from the use case countries and organisations b) documented specifications of the GEIGER Framework including the GEIGER Indicator, GEIGER Toolbox, the GEIGER Cloud as well as information sharing components c) documented education, governance, and compliance requirements.

As the main **scientific** achievement within WP1, Task T1.1 has performed a public one-week requirements elicitation workshop, 'RE CARES'[1]. The workshop was held in conjunction with the 28th IEEE International Requirements Engineering Conference in Zurich, Switzerland. The workshop raised awareness of MSE cybersecurity within the global research community and harvested knowledge and innovative ideas existing in that community.

The main **technological** achievements (WP2) are an initial version of a) the GEIGER Indicator, b) the Information Sharing and Analysis Centre (ISAC) platform, c) the GEIGER Cloud data repository and APIs for communication with the GEIGER Toolbox and the ISAC, and d) the technical development of the GEIGER Toolbox.

The **educational** work (WP3) has resulted in a) defined competence levels (level 0, i.e., everyday knowledge, to level 4, i.e., expert knowledge) and related to learning scenarios in MSE contexts, b.) a respective interoperable educational curriculum (GEIGER Cybersecurity Curriculum) specified as xAPI statements (around 200 statements) that supports the communication between the GEIGER Framework and educational tools. In terms of educational tools, c) prototypes of gamified learning features have been developed and tested, and d) the education provider community has been outlined.

Regarding **dissemination**, WP5 has contributed to establishing a) awareness and interest of GEIGER in 'multiplier' organisations[2] – such as existing networks of Education Providers, CERTs/CSIRTs, and MSE associations. In addition, b) MSEs have been involved in shaping and testing a compelling value proposition of the GEIGER solution, c) supporting setting up targeted messaging and d) helping define a competitive business model definition.

As a **contribution to the state-of-the-art**, the GEIGER Cybersecurity Curriculum for MSEs developed in WP3 focuses on previously neglected – non-IT – target groups[3] and guides pertinent policies. Discussions in this regard with, for example, ENISA have been undertaken to exploit the curriculum. WP1 contributed to the state-of-the-art by detailing the requirements into user journeys for the (Certified) Security Defenders and 'regular' non-IT employees of MSEs.

As **innovative contributions**, the concepts used and the work performed in WP1 represent an innovation in software engineering and cybersecurity. There is no systematic method published for engineering a large-scale digital ecosystem, neither in general nor in cybersecurity. There is a lack of case studies describing with rich detail the approach and experiences of such engineering. The two deliverables resulting from WP1 (D1.1 Requirements, D1.2 Architecture) are useful to close this gap. As the main **educational, innovative contribution** (WP3), the GEIGER Indicator will include data on the competence levels of people working in an MSE into the calculation. The GEIGER Education Ecosystem will include automated training recommendations for individual learners, i.e., employees of an MSE, and a set of

[1] https://re20.org/index.php/re-cares/

[2] 'Multipliers' in the GEIGER context relates to organisations that will help us convey our message to the potential end-users through their channels.

[3] See D3.1 Training Plan, where the target groups and competence levels are elaborated

training sequences in this regard. The **technologically innovative contribution** (WP2) is taking privacy awareness to the next level and contributing to 'privacy-by-design.'

The developed GEIGER Cybersecurity Curriculum will significantly impact the large target group of non-IT professionals working in MSEs. The covid-19 restrictions have boosted digitalisation and, at the same time, led to a stiff increase in cybercrime. Increasing the awareness and security level of the MSEs will have a major impact on society and the economy in Europe. The impact created by the GEIGER Education Ecosystem will be validated and demonstrated in the upcoming project period (in WP4). The GEIGER introduction communication materials (WP5) have already been successfully used with potential multipliers and supporting partners (e.g., cyberwatching.eu), which has led to fruitful contacts and promising leads for future collaboration. The project impact will be strongly influenced by the capacity of the GEIGER solution to meet the expectation of the target market (MSEs). In this period, the consortium has acted to design and test various possible value propositions to address our end user group optimally.

Results related to **Intellectual Property Rights (IPR)** are planned for the second project period, as the results will be more mature and clearer in the project

Recommendations received when obtaining the grant have been addressed. The GEIGER project initially had six work packages, and upon feedback when receiving the grant, the WP7 Ethics has been added and successfully worked upon. Ethics deliverables D7.1 and D7.2 have been submitted.

The **overall project work has been performed well.** In each WP, appropriate methods have been applied to achieve the objectives professionally. The WPs were efficiently building upon each other. WP1 results were sharpened iteratively and taken further in implementation in WP2 and WP3. WP2 and WP3 collaborate closely to ensure a harmonised GEIGER concept addressing technical and social aspects. WP5 has supported the work by dissemination, standardisation, policy, and exploitation efforts.

The **commitment from the project Coordinator and partners** is evident by the constant engagement of the 18 partners on their assigned tasks. All participants actively participate in the regular meetings. Individual exchanges between partners and the project management office ensure a targeted information flow between Coordinator and partners. WP6 and WP7 applied a professional project management methodology enabling an effective, smooth, and successful collaboration, reporting, and monitoring.

Overall, the project has achieved its intended objectives for the first period while guaranteeing efficient use of resources. The project has successfully achieved to overcome the challenges of the covid-19 pandemic situation. The **adequacy of the progress of research and innovation** work is confirmed.

2.2 Deliverables of the Period

D1.1 Requirements (due M6, submitted M7) reports the work performed in 'Task 1.1 Use Case Requirements Analysis and Solution Specification', complementary with the requirements analysed in 'Task 1.4 Education, Governance, and Compliance Requirements' and included an initial description of the architecture drafted in T1.2. To avoid redundancies of the deliverables, the requirements for cybersecurity education and governance were reported in the deliverable D3.1. Deliverable D1.1 defines the GEIGER vision and ecosystem to be served by the GEIGER solution. It specifies the use case contexts and requirements for Switzerland, Romania, and the Netherlands that are positioned within the GEIGER Ecosystem and used to operationalise the vision. Based on a preview of the GEIGER Framework architecture (designed in Task T1.2) and the GEIGER Indicator (designed in Task T1.3), the deliverable also defines the technical features and requirements for the GEIGER Cloud, GEIGER Toolbox, GEIGER Indicator, GEIGER Testbed, and Certified Security Defenders education. Besides the specification of functionality, it also includes a definition of quality requirements and requirements for GDPR compliance.

D1.2 – Architecture (due M12, submitted M12) reports the work performed in 'Task T1.2 GEIGER Framework Architecture and Gaps Analysis' and 'T1.3 Personalised Dynamic Risk Forecasting'. It defines and describes the architecture of the GEIGER Framework as a security platform. It covers all the components of the GEIGER Framework, including the most important blocks: GEIGER Toolbox and GEIGER

Cloud. In addition, it explains all the subcomponents and the tools that are engaged with GEIGER, including cloud infrastructure apps and external tools. The platform architecture has considered various scenarios or use cases, such as a) local-only mode, b) the hybrid GEIGER Cloud and local mode, and c) the combined Cloud, local and external mode. This variety of use cases can help get a real idea of the flexibility of the proposed solution. For clarifying how data is managed in GEIGER, information flows have also been described in the document. They cover issues such as who and how to request information, who is responsible for providing it, and the path data are expected to traverse to the destination. Finally, and to guide and support better the implementation activities in WP2, the deliverable includes information about information flows, roles of GEIGER, information to be shown, data exchanged and stored in each component, etc. The idea was to provide this deliverable as the guideline for WP2 and work on top of it in the implementation phase, building and enhancing on top of any new feature or modification.

D2.1 – Adapted components (due M12, submitted M12) describes the technical work done in WP2 until M12 in the different areas of the GEIGER Framework: GEIGER Indicator, GEIGER Toolbox, GEIGER Cloud, communications system, data storage structure, and APIs. It elaborates the methodology followed for each component, extension of tools, integration in the GEIGER platform, communication channels, etc. This deliverable is complementary to the work presented in D1.2, which focuses on the architecture of GEIGER.

D3.1 – Training Plan (due M6, submitted M6) reports the work performed in ‘T1.4 Education, Governance and Compliance Requirements’. It describes the specific situation, respective conditions, and requirements for providing the GEIGER Education Ecosystem and presents the result already achieved in this way. The conditions and requirements were systematically deriving from: a) the specific expertise of partners contributing to the GEIGER Education Ecosystem, b) non-IT-experts in MSE environments being the major target group of the Certified Security Defenders Education, c) the organisational conditions and specific target groups of partners providing courses, and d) perspectives of sustainable management of the GEIGER communities.

D5.1 – Impact Plan (due M6, submitted M6) reports the work performed in WP5 until M6. It describes the GEIGER dissemination and communication goals, its target audiences, key messages, tools, channels, activities and materials, and the initial strategy and timeline for actions. It presents the methods of tracking the progress and mitigating risks related to different areas of the strategy. It also elaborates the dissemination and communication results achieved during the M1-M6 of the project. Furthermore, it describes existing standardisation and planned contributions to standards and policy. Finally, it presents the initial implementation strategy for rolling out the GEIGER solution.

D6.1 – Data Management Plan (due M3, submitted M4) provides information about data the project will generate, when and how it will be used or made accessible for validation or reuse and how it will be stored and protected. The DMP has the purpose of providing information about: a) the handling of research data during and after the end of the project, b) what data will be collected, processed, or generated, c) the methodology and standards to be used, d) whether data will be shared or made open access and, e) how data will be stored (also after the end of the project). Additionally, the methodology to follow by all the partners for working with the data in the project was defined. Finally, and as this document is updated when the project progresses, the plan is to include any additional information or requirement from the use cases for the validation of GEIGER in project management deliverables.

D6.2 – Year One Report (due M12, submitted M12) reports the state of the overall project at M12 and summarises the work performed in all work packages. It describes the overall work, including progress towards objectives, major achievements, impact, deliverables, and milestones of the first project period. A summary of the work per WP is provided, including project management activities (WP6).

D7.1 – H-Requirements (due M3, submitted M3) addresses ethical issues concerning human involvement and the protection of personal data identified and reported in the Ethic Summary Report. D7.1describes the procedures for identifying and selecting research participants, including the criteria that will be applied for the selection. The procedures for informed consent and data processing were defined. The informed consent forms and information sheets that will be provided to the research participants were provided.

D7.2 – POPD Requirements (due M3, submitted M12) provides information on what kind of personal data is collected and processed within the GEIGER project and which steps need to be taken to ensure secure and compliant processing. It declares the appointed Data Protection Officers (DPO) of each organisation leading a validation use case, describes the technical and organisational measures for safeguarding the rights and freedoms of the data subjects participating in the research, elaborates the access authorisation security measures and anonymisation/pseudonymisation techniques used to protect the personal data, and how the data minimisation principle will be applied in the GEIGER project

The deliverables (D) in the scope of the first period of the GEIGER project are listed in Table 2.

No	**Name**	**WP**	**Lead**	**Type**	**Diss. Level**	**Delivery Date Planned**	**Actual delivery date**	**Forecast Delivery Date** (if applic.)
D1.1	Requirements	1	**FHNW**	Report	Public	30.11.20	14.12.20 submitted	
D1.2	Architecture	1	**ATOS**	Report	Confi-dential	31.05.21	31.05.21 Submitted	
D2.1	Adapted Components	2	**ATOS**	Report	Confi-dential	31.05.21	31.05.21 submitted	
D3.1	Training Plan	3	**PHF**	Report	Public	30.11.20	30.11.20 submitted	
D5.1	Impact Plan	5	**Tech.eu**	Report	Public	30.11.20	30.11.20 submitted	
D6.1	Data Management Plan	6	**ATOS**	Report	Public	31.08.20	30.09.20 submitted	
D6.2	Year 1 Report	6	**FHNW**	Report	Public	31.05.21	31.05.21 submitted	
D7.1	H – Requirements	7	**FHNW**	Report	Public	31.08.20	31.08.20 submitted	

D7.2	POPD Requirements	7	**FHNW**	Report	Public	31.08.20	31.05.21 submitted	

Table 2: GEIGER Deliverables, Period 1

2.3 Milestones of the Period

MS1 Requirements Defined has been **achieved** on 14.12.2020 on submission of D1.1 Requirements. The deliverable allows each consortium partner to understand how GEIGER will be used, how the GEIGER Framework (WP2) and GEIGER Education (WP3) contribute to realising the overall GEIGER vision, what the use case context and stakeholder needs are that drive validation and demonstration of GEIGER (WP4), and what the actors and arguments are for modelling the business of the GEIGER solution (WP5).

MS2 Architecture Defined has been **achieved** on 31.05.2021 on submission of D1.2 Architecture. The deliverable allows the consortium partners to understand their contribution and how the technical contributions fit together and interoperate to realising the overall GEIGER vision (WP2) and provide the fundamental technical contributions to standardisation (WP5).

MS3 GEIGER Indicator MVP has been **achieved** on 31.05.2021 on submission of D2.1 Adapted Components. The deliverable describes the GEIGER Framework: GEIGER Indicator, GEIGER Toolbox, GEIGER Cloud, communications system, data storage structure, and APIs. A demonstration of the adapted components at the project review meeting (set for 07.07.2021) will show milestone fulfilment. The functionality of the GEIGER Indicator is available for initial testing, and simulated data is used to start validating/calculating results. This result is complemented by the work-in-progress of the user interface, which will also require validation and several iterations to adapt the information in the most accessible and easy-of-understand possible way.

The milestones (MS) in the scope of the first period of the GEIGER project are listed in Table 3.

No	**Name**	**WP**	**Lead**	**Delivery Date Planned**	**Means of Verification**	**Achieved**	**Forecast Achiev. Date** (if applic.)
1	Requirements Defined	1	**FHNW**	30.11.20	D1.1 delivered	Yes	
2	Architecture Defined	1	**FHNW**	31.05.21	D1.2 delivered	Yes	
3	GEIGER Indicator MVP	2	**ATOS**	31.05.21	D2.1 delivered	Yes	

Table 3: GEIGER Milestones, Year 1

3 Summary of Work Carried out per Work Package

In the following, an overview of each WP status is provided. 'WP4 GEIGER Validation and Demonstration', which starts at M13, is not included in the following listing. Some initial preparatory work has already been done to allow a rapid and efficient start of the piloting phase (see more in section 9). The WP risks and their management are elaborated in section 8.4 of this document.

Work Package 1: Requirements, Architecture, and Methodology

WP1 contributed to the **overall project objectives** by defining the GEIGER Indicator requirements (Objective 1) and the GEIGER Toolbox requirements (Objective 2). WP1 defined an approach for handling MSEs profile data and incidents. WP1 reported the design of the technical architecture connecting the MSEs end-users experiencing incidents using the GEIGER Cloud and end-to-end with a CERT/CSIRT interoperating with GEIGER through a 'Malware Information Sharing Platform' (MISP) (Objective 3). WP1 contributed with requirements for the GEIGER Certified Security Defenders education and with governance-related requirements for the education provider and security defender communities (Objective 4). Finally, WP1 contributed with a rich description of the use case contexts in Switzerland, Romania, and the Netherlands, including the stakeholders representing the GEIGER ecosystem and for which the GEIGER solution is expected to create value. The WP1 results enable the design and planning of validation and demonstration of GEIGER at TRL7 in WP4 (Objective 5).

Regarding the **work package objectives** of the first period, WP1 aimed at a) eliciting and analysing the requirements from the use case countries and organisations and b) iteratively refining the overall GEIGER vision, and c) specifying the GEIGER solution, which includes the GEIGER Framework, Indicator, Toolbox, and Education Ecosystem.

WP1 has achieved its objectives by eliciting, analysing, and specifying requirements by involving all GEIGER partners and collaborating with WP2 and WP3. It followed the TwinPeaks method of iterative refinement of the overall project, use case requirements, technical framework, and education visions into requirements detailed enough for solution implementation and future validation and demonstration work. Besides the specifications reported in the **deliverables D1.1 and D1.2**, the significant contribution of the WP1 is a shared understanding of requirements, framework, and education within the whole consortium and agreement of these results among all GEIGER partners. These requirements and information about the needs of the use cases will be used later as the basis for the validation of the platform.

WP1 elicited and analysed the requirements from the three use case countries Switzerland (involving the organisations BBB, SKV, CL, E-ABO, and HAAKO), Romania (involving the organisations CLUJ IT, SCB, and PT), and the Netherlands (involving the organisation SRA).

WP1 specified the GEIGER Framework, including comprehensive requirements for the GEIGER Toolbox and GEIGER Cloud and the Design of the GEIGER Framework architecture enabling the technical use case scenarios and functional requirements and satisfying the GEIGER Framework quality and compliance requirements.

WP1 researched cybersecurity indicators and specified the expected behaviour and algorithmic approach of the GEIGER Indicator supporting the following:

- Risk data collection with sensor tools integrated into the GEIGER Toolbox and Cloud,
- Risk forecasting reflecting CERT-communicated threats, GEIGER-aggregated sensor, and incident data, and the MSE end-user profile, and
- Risk communication that is personalised, thus intuitive and motivating for the recipient MSE and human end-user.

WP1 specified and designed the GEIGER Toolbox as an open platform of cybersecurity tools deployed on the end-user's devices. It specified the interoperability with the GEIGER Cloud and with the GEIGER partners' and any third party-contributed tool offering sensors and shields.

WP1 specified GEIGER compliance requirements with a focus on data protection and GDPR compliance. This work was reported in D1.1 Section 5 and represented the first step towards the full specification of the GEIGER POPD approach reported in the deliverable D7.2. The WP also specified GEIGER education requirements reported in the deliverable D3.1 Section 2 and governance-related requirements for the education provider and security defender communities reported in D3.1 Section 10.

The accomplished results are:

- WP1 has elicited and analysed use case requirements and specified the ecosystem actors and value exchanges targeted by GEIGER.
- WP1 has specified the requirements and architecture of the GEIGER Framework, including the GEIGER Toolbox with sensor and shield tools, GEIGER Cloud, and GEIGER Indicator.
- WP1 has specified the requirements for the GEIGER Certified Security Defender education leading to the education framework being elaborated in WP3.
- WP1 has established a shared understanding of GEIGER use case context and needs, solution requirements, and framework architecture within the GEIGER consortium, aligned the GEIGER Framework and Certified Security Defenders education with that use case context and needs, and has reached an agreement among the partners concerning the requirements, architecture, and scope.

In addition, the WP1 Task T1.1 has performed a public one-week requirements elicitation workshop ‘RE CARES’. The workshop was held in conjunction with the 28th IEEE International Requirements Engineering Conference in Zurich, Switzerland. The workshop raised awareness of MSEs cybersecurity within the global research community and harvested knowledge and innovative ideas existing in that community.

Work Package 2: GEIGER Framework

WP2 contributes to the **overall project objectives** by developing the GEIGER technological framework. WP2 develops the GEIGER Indicator (Objective 1) and the GEIGER Toolbox (Objective 2). In addition, WP2 contributes by implementing the components for an Information Sharing and Analysis Centre (ISAC) platform (Objective 3). The resulting components from WP2 build an essential base to validate and demonstrate the GEIGER approach in diverse, relevant operational environments (Objective 5). These components are supported by the GEIGER Cloud, which allows for synchronisation and common operations for the indicator. In addition, it allows for the processing and support of the GEIGER ISAC. Finally, it will allow for the integration and usage of external tools in GEIGER, which will allow its expansion in the future with additional tools.

Regarding the **work package objectives**, WP2 aims at developing the end-to-end GEIGER Indicator system, adapting, and integrating the GEIGER tools into the GEIGER Toolbox, and releasing the optimised and hardened resulting GEIGER Framework. Even though the MVP of GEIGER was planned initially for M18, WP2 has worked towards an initial version of the GEIGER Framework that allows user testing during the months M13-M18.

WP2 has achieved the work package objectives of the first period following an iterative agile DevOps process method. WP2 has created a plan for each component's development to generate an initial version of the GEIGER Framework as soon as possible for its usage and testing from the technical expected functionality, security and privacy requirements and needs, and the use case partners for usability. Regarding each activity, which is closely linked to each task of WP2, it was developed in the following way:

- Design, creation, and implementation of the initial version of the GEIGER Indicator. This version supports the information that will be shown to the end-users (following the requirements obtained in WP1), how the information is used, its analyses and how it is obtained from the several data sources of GEIGER. The specification of the information to be shown to the users was worked on, differentiating between roles, information for each type, company-specific and user-specific ones, etc. Then came the design of the algorithms, identification of data to be used and how to show the information to the end-users. In this way, user experience is a key aspect of the GEIGER Indicator, so we also are working in iterative versions.

- Development of the GEIGER client, covering the internal structure (data storage), communication and interface. This development also includes the adaptation of the different tools to be integrated into the GEIGER Framework and the life cycle of the data that is generated. The GEIGER Toolbox (client) provides an API for the different tools to use for communicating/exchanging data with the GEIGER Indicator.
- Definition of GEIGER data sharing methodology, formatting, and its implementation. Currently the development of the GEIGER cybersecurity data sharing and integration with CERTs is being worked on. It is planned to initially use the support of CERT-RO for initial integration and testing and then extend the way of working with other CERTs. The GEIGER MISP instance has already been deployed and is connected to the CERT-RO instance to test the exchange of information. Additionally, a common methodology and structure that other CERTs of Europe and Switzerland can use, is being produced. Possible partners have already been identified and plans to extend beyond that by connecting and using the sources of information of other cybersecurity EU research projects are in place. Finally, a component that will allow GEIGER to share information with CERTs about the cybersecurity of MSEs is also being worked on.
- Development of GEIGER Cloud component. WP2 develops the cloud component of GEIGER, focusing on the data storage and communication with the different elements of GEIGER with which data is exchanged (GEIGER client, GEIGER data sharing, external apps, etc.). The communication supports data protection and privacy solutions, integrated into GEIGER naturally. The design follows the requirements provided in WP1 about how the data can be used and managed. The GEIGER Cloud acts as the central component for synchronising information between different devices and calculating the GEIGER Indicator scoring at the company level. In addition, it processes and uses the information of the CERTs and external tools, providing security and privacy mechanisms for using the data as a basis for the GEIGER Indicator or providing end-users with new functionalities.

All the work done in WP2 follows the architecture developed in WP1 (initially presented in D1.2) and aim to fulfil the requirements of the end-users (presented in D1.1). WP2 has a continuous synchronisation between all the tasks as they are all much related. Thus, weekly synchronisation meetings are being held to have all our work in line and check for possible misconceptions, issues, or deviations.

All partners have participated in each task according to their expected work (as described in the DoA) and have contributed to additional tasks to help develop the GEIGER Framework. Finally, training tools are also being considered for the GEIGER Framework. WP2 ensured with bi-weekly meetings the synchronisation between WP2 (technology) and WP3 (education). Those tools are correctly integrated from both the technical and architectural points of view, providing information to the GEIGER Indicator and Cloud for further processing. The final goal is to have a common central solution (GEIGER Framework) that uses both the technical and educational information of the MSEs for providing awareness, recommendations and security to their companies and employees.

The **results WP2 has accomplished** so far are:

- initial version of the GEIGER Indicator,
- communication system and storage for the GEIGER Toolbox,
- initial version of the GEIGER Cloud,
- initial version of the GEIGER ISAC, methodology and structure for data sharing,
- authentication and data protection mechanisms for the platform.

The work done so far is documented in Deliverable D2.1. The initial proof of concept of GEIGER supporting the more important functionalities is released for the date of the integrated prototype planned by M18 in the project. At the end of the first period, an initial proof of concept of GEIGER providing all these functionalities is achieved, so the work on updated versions and feedback from initial usage by the end-users can start. In the next project phase, WP2 will also ensure the security hardening of the technological framework.

Work Package 3: Security Defender Education

WP3 contributed to the **overall project objectives** with the development of an Education Ecosystem that addresses cybersecurity and data privacy protection for MSEs in Europe (Objective 4). The resulting educational curriculum, the communities, and target-group specific training and learning formats from WP3 build an essential base to validate and demonstrate the GEIGER approach in diverse and relevant operational environments (Objective 5).

Regarding the **work package objectives of the first project period**, WP3 aims at starting to build the GEIGER Educational Ecosystem by a) developing a curriculum along with the first version of experiential learning formats including learning games and cyber range-enabled challenges as core elements, and b) initiate an Education Provider Community.

WP3 has achieved the work package objectives of the first period. The work of the first half-year (M1-M6) is documented in the GEIGER Training Plan (D3.1). It summarises the specific conditions and requirements for providing the GEIGER Education Ecosystem and presents the result already achieved in this way. Meanwhile (M7 – M12), WP3 started to work on the Intermediate Training Plan (D3.2) (due at M18). That plan implies more advanced matters such as

- the development of a detailed and interoperable curriculum,
- the integration of learning features into the technical infrastructure of GEIGER,
- detailed user journeys for Certified Security Defenders (internal/external, Information Technology (IT) / non-IT background) and for ‘regular’ non-IT employees (low learning motivation, with learning barriers),
- the alignment of educational features of GEIGER and educational objectives given by the different use cases,
- monitoring and supporting the development of learning materials.

The detailed and interoperable curriculum is the basic instrument to align and monitor the heterogeneous elements, objectives, and contexts of the GEIGER Education Ecosystem within the whole GEIGER approach.

WP3 has worked on the target group-specific learning format. Of the two cyber ranges (together addressing five threats/challenges) that will be provided. One was already tested with students at FHNW. A Data Protection Impact Assessment Tool for MSEs was newly developed and tested with MSEs in Switzerland. A virtual cybersecurity escape room was enhanced and applied in several trainings with young students in collaboration with the ‘TecDays’ organised by ‘Swiss Academy of Engineering Sciences SATW’ in Swiss Schools[4]. The learning game ‘Cyber Safety Management Game’ (CSMG) was adapted targeting the end-user group of IT-lay persons. More learning formats (e.g., phishing cyber range, data protection quiz) were either newly designed or analysed to adapt them to the GEIGER target groups to start the development. The adaptation of the SMESEC Coach CYSEC into a mobile learning application with learning materials tailored for GEIGER was initiated.

WP3 initiated the Education Provider Community by applying the education canvas approach (see section 10, D3.1) and starting with the educational bodies within the GEIGER consortium. As an example, the xAPI-format curriculum is being adapted to the competence format used at BBB. This adaptation is a showcase of how further education providers can apply the xAPI-format curriculum to their competence descriptions. Outreach to consortium-external institutions was reached, such as ENISA that is currently engaged in developing guidelines for cybersecurity education. A collaboration between FHNW and the education initiative SCN DNA in Switzerland was official launched. Exchange with peer project SPARTA enhanced the discussion of curriculum frameworks for European MSEs. Preparatory work for the

[4] https://www.satw.ch/en/tecdays

Cybersecurity Defender Community has been conducted. The procedure of certifying future Cybersecurity Defender has been tested with a hairdresser apprentice in the Trinational Cybersecurity Days 2021[5].

WP3 tightly aligns with WP2 to develop an interoperable curricular scheme, which feeds into the MS2 'Architecture Defined'. Because human behaviour is essential for cybersecurity, the level of pertinent competences and how they can be developed with training is part of the threat level; thus, it needs to be part of the 'GEIGER Indicator' data structure of MS3 'GEIGER Indicator MVP'. The need for communication between toolbox modules led to the development of a curricular approach based on xAPI.

As main results, WP3 has particularly defined:

- Competence levels (Level 0, i.e., everyday knowledge, to Level 4, i.e., expert knowledge) and an aligned competence grid (see D3.1),
- user journeys for Certified Security Defenders and 'regular' non-IT employees (will be published in D3.2),
- competence levels and ENISA threats integrated into a curriculum formulated as xAPI statements (will be published in D3.2),
- the schedule for breaking down the integrated curriculum into syllabi with fine-grained learning objectives, target groups, prioritisation, time limitations (will be published D3.2),
- community Canvas for Education Provider Community (D3.1),
- learning tools in first tested versions (Data Protection Impact Assessment Tool, cybersecurity escape room game, cyber range-challenges),
- first test of the procedure to certify Security Defenders.

The work of WP3 builds the base for the next project phase. From M13, WP3 will start its task to build the Cybersecurity Defender Community and, based on this, begin to mentor MSEs (applying Murphy's reverse mentoring[6]).

Work Package 5: Dissemination and Exploitation

WP5 contributed to the **overall project objectives** by achieving widespread awareness, interest, and support, which is needed for the GEIGER Educational Ecosystem – in particular the communities - (Objective 4) and the GEIGER validation and demonstration (Objective 5). With its standards- and policy-defining activities, WP5 contributes to the development of the technical GEIGER platform and education (Objectives 1–4). Additionally, WP5 will continue working in the business model of GEIGER, adapting it to the needs of the MSEs in technical, functional, and financial aspects. The business model will be defined in close collaboration with the pilots in WP4 (Objective 5) and preparing the GEIGER organisation needed to operate GEIGER according to the European risk reduction roadmap sustainably.

Dissemination: Regarding the **work package objectives of the period**, WP5 **dissemination** aimed at a) identification of target audience and set up the tools and branding to raise awareness about GEIGER, b) promoting project visibility and awareness, and c) disseminating in strategic networks of the partners and supporters.

WP5 dissemination has achieved the work package objectives of the first period by building the infrastructure for the project's communications. WP5 established the project's **external** communications channels, including website, social media, and newsletter mailing list. Together with the consortium members involved in the work of WP5, different communications styles were developed and tested to find the best fit for the primary target audience, small business owners and employees. To allow easy and active participation in the dissemination work to all project partners, WP5 defined, tested, and adjusted practices for internal collaboration and communications within the consortium, documented in the Communications Handbook, made available to the consortium within the Project Management Handbook

[5] www.tri-csd.ch

[6] Murphy, W. (2012). Reverse mentoring at work: Fostering cross-generational learning and developing millennial leaders. Human Resource Management, 51(4), 549-573.

(PMH). Tools to measure and evaluate the impact of the GEIGERs communications actions were put in place. To start building the networks that will be necessary for the success of the dissemination of the project results, WP5 conducted an initial mapping of stakeholders that have the potential to act, in the next phases of the project, as ‘multipliers’ to the communications towards the end-users of the GEIGER solution, and drafted a strategy for reaching out to these multipliers. To facilitate the consortium partners’ outreach towards them, WP5 drafted comprehensive step-by-step guidelines, made available customisable communications material templates, and promoted the possibility for tailored support in all their outreach activities. WP5 work done to date successfully paves the way for communicating the Minimum Viable Products, recruiting early adopters to the GEIGER solution, and finally, the sustainable exploitation of the project results and the rollout of GEIGER across Europe.

As main dissemination results, WP5 work led to:

- communications tools and channels, and defined best practices,
- an initial stakeholder/audience mapping,
- communications and dissemination plan (D5.1),
- documented strategy/guidelines for building a network of relevant multipliers (step-by-step checklist and templates),
- an initial crisis communications plan (defined procedures and contact within the consortium for dealing with critics from media representatives).

Standardisation and policy: Regarding the **work package objectives** of the **standardisation and policy work**, it is the aim to align the GEIGER solution with related activities within Europe and worldwide, to achieve harmonisation and mutual recognition with GEIGER-related initiatives, and to contribute with recommendations on security, privacy, and data protection for policy development.

Regarding the **work package objectives of the period**, WP5 **standardisation & policy** aimed at identifying and selecting standard, Standards Developing Organisations (SDOs), and initiatives fitting to the GEIGER project. Further, the aim is to support standards adoption in GEIGER development (WP2+WP3) and establish partnerships with significant external entities.

WP5 standardisation & policy has achieved the work package objectives of the first period by contributing to achieving awareness of the GEIGER project among several important stakeholders:

- the peer projects funded under in the Digital Society programme: AI4HealthSec, CitySCAPE, CyberKit4SME, E-CORRIDOR, HEIR, Palantir, Puzzle, Trapeze,
- other related peer projects funded in the H2020 programme: CyberSec4EU,
- standards-defining organisations ADLNET and Small Business Standards,
- the CERTs ENISA, NCSC in Switzerland, and Digital Trust Center (DTC) in the Netherlands (NL).

For the definition of a European MSEs risk-reduction roadmap, WP5 has created a map of related standards and policies. The map reflects the current state-of-the-art and points to organisations and initiatives that could be involved in road mapping. This contribution allows the technical work to build on existing state-of-the-art and collaborating with relevant third parties to research and develop relevant progress beyond the state-of-the-art.

In particular, WP5 mapped standards and initiatives related to measuring risks and building knowledge regarding effective risk-mitigating controls and communicated the results to WP1 and WP2 for raising awareness about that work. WP5 also mapped standards and initiatives related to the identification of tools candidates and enabling interoperability. The GEIGER project adopted xAPI. Finally, WP5 mapped standards and initiatives related to information sharing. These include work being performed in ENISA Operational Cooperation, X-ISAC, and MISP Information Exchange and Data Modelling. Here, the GEIGER project adopted MISP. WP5 members were accepted in the Digital SME Alliance working group of ‘cybersecurity and data’ to represent GEIGER. Additionally, GEIGER initiated a regular exchange on cybersecurity for SME with ENISA and agreed with sister projects, including Trapeze and Puzzle, to collaborate on scientific and technical interoperability events.

As main standardisation & policy work results, WP5 led to:

- delivered a map of related organisations and initiatives leading to recommendations for the alignment of the technical work on the GEIGER indicator, information exchange, and education,
- established contact with third parties useful to be involved for validation and demonstration of GEIGER interoperability in the operational environment at TRL7,
- formulated a draft policy brief concerning compliance problems observed among GEIGER use case and third-party MSEs. The policy brief has been presented at the P2PKOS kick-off with the participation of the EC Research Executive Agency (REA).

Exploitation: Regarding the **work package objectives for exploitation of the first period**, WP5 aimed at defining the value proposition for the GEIGER solution and defining the vision of the future GEIGER organisation that puts further the GEIGER solution.

WP5 exploitation work has achieved the work package objectives of the first period by working on the value proposition of the GEIGER solution and deriving effective messaging towards stakeholders. The impact of the GEIGER solution will be strongly influenced by the capacity to meet the expectation of the target market (MSEs). To deliver high value for money services to this segment, an important aspect is the right calibration of the value proposition − and subsequently of the GEIGER solution − to the culture and needs of the target segment. In this period, various possible value propositions have been designed and tested. This work has been done in close collaboration with representatives from MSEs. GEIGER is now in the position to have a mature formulation of the value proposition, which will be tested in the next phase on a wider basin of target customers (to be reported in D5.2 due at M18). On top of what was planned, WP5 investigated a procedure for Intellectual Property (IP) management. Initial indicators for IP acceptance have been defined, a platform (named DEIP[7]) was identified and configured, and first inputs uploaded to test the platform. The value proposition definition is being finalised. WP5 has prepared an early market testing based on the value proposition and theoretical prototype. WP5 created a database with multipliers in Europe (extending the list of the multipliers from the dissemination work). In addition, WP5 achieved that GEIGER was accepted for the European H2020 Booster Programme. This programme will lead to external assistance related to the business plan and exploitation plan.

As main exploitation work results, WP5 led to:

- a suggested procedure for IP management including a dedicated platform (DEIP),
- a database with multipliers in Europe,
- a value proposition of the GEIGER solution,
- initial view on the GEIGER business model (D5.1).

Work Package 6: Project Management

WP6 contributed to the **overall project objectives** by embracing the overall administrative, scientific, and technical coordination.

Regarding the **work package objectives**, WP6 provides an effective overview and enhances the consortium's performance through professional project management, scientific steering, and data management. WP6 will focus on a) productive collaboration and integration of all partners, b) dealing with overall administrative and financial issues, c) meeting EC requirements, reporting, d) scientific/technical coordination, progress monitoring, and risk management.

WP6 has achieved the work package objectives by fulfilling the planned work of the GEIGER project management. On project start, a clear definition of roles and tasks and implementation of WP6 meetings ensured seamless collaboration between Scientific and Administrative Coordinator (FHNW) and Technical Coordinator (ATOS). An effective overview and enhanced performance of the consortium was ensured by

[7] https://www.deip.world/

aligning our procedures with the approach from PMI published in their manual entitled "A Guide to the Project Management Body of Knowledge (PMBOK® Guide)". WP6 worked towards

- Productive collaboration and integration of all partners:

The Project Management Office (PMO) was established as the first contact point and support for the consortium. The support includes tools, services, and processes such as a secure document management/exchange, a collaboration platform supporting, e.g., mailing and contact lists, and project management tools (EMDESK, 360inControl for risk management). Regular meetings have been established[8], such as General Assembly every six months, Executive Board (EB) meetings monthly, and WP6, T6.1 and T6.2 meetings scheduled on a bi-weekly basis. An Advisory Board (AB) was established with members from different disciplines and perspectives to ensure that both the results and the decisions could be critically scrutinised, and recommendations could be obtained from independent experts and stakeholders. The first AB meeting took place. The second meeting is already planned and confirmed for the first week of June 2021. Timely invitations, a clear agenda before, and precise minutes after the meetings ensured the integration of all partners. Templates for meeting minutes and PPTs were provided.

- Dealing with overall administrative and financial issues:

Each partner was introduced to the project management tools and processes and continually supported. Requests for contractual adaptations from the partners for eventual amendments of the Grant Agreement (GA) were collected. Quarterly one-on-one meetings between WP6 lead and partners ensured constant and effective dealing with administrative and financial questions.

- Progress monitoring:

Continuous progress tracking and monitoring were ensured threefold. Firstly, the financial expenses were collected and monitored. Secondly, the technical progress was requested and monitored in accordance with the time schedule (Gantt chart). Thirdly, the progress towards KPI fulfilment was collected from WP Leads. FHNW compiled a report per partner on their resource consumption and conducted a one-on-one review session with each partner on a quarterly basis.

- Meeting EC requirements, reporting:

Consortium Agreement and EC Grant Agreement were coordinated. Clear management guidelines recapitulating governance and management procedures were documented and distributed in the PMH and the data management plan (D6.1).

- Scientific/technical coordination:

A data protection policy for the project and the measures for safeguarding the data subjects' data, rights, and freedoms were compiled. WP6 contribution to the design thinking for the GEIGER solution and ecosystem, resulting in the refinement of the original vision at the level of third-party roles and GEIGER solution components, including their assigned responsibilities/capabilities and interdependencies. The integration, validation, and readiness for piloting of the overall GEIGER solution (scientific) and the execution of the GEIGER Framework development, integration, and deployment (technical) were coordinated. Innovation opportunities were identified, and the associated scientific research and publication actions launched. Scientific coordination monitored the work packages together with technical coordination in regular meetings. Project progress was supervised, and risks managed, assessed, and mitigated. The alignment between the core pillars – education and technology – was a major focus area. Exchange with further EU project has been initiated. The partners' scientific work that led to deliverables and publications was reviewed, verified for quality, consistency, and respect of deadlines. In case of conflicts, a professional resolution relating to technical and organisational issues was defined. Scientific decision-making bodies such as executive committees were coordinated and advised.

[8] The meeting dates are listed in section 8 of this document.

- Risk management:

As specified in the Project Management Handbook, risk management procedures have been established to continuously track and update the risks and discuss them in the EB meetings. The risk management process has been transferred to professional compliance software to visualise, track changes and monitor the risks. This solution allows transparency, traceability, and clear ownership of risks, assigns and tracks mitigating actions, conducts regular risk assessment reporting, and contributes to lower the overall project risks.

As main **results**, WP6 achieved:

- effective and transparent project management procedures documented transparently in the Project Management Handbook,
- guidelines for handling of personal data in the project in compliance with GDPR documented in the Data Management Plan (D6.1),
- overview of year one of the GEIGER project documented in the Year One Report (D6.2).

The project management structures and rules for data management and ethics set the ground for the overall project work, enable partner to work professionally, efficiently, and compliant with the overall project objectives.

Work Package 7: Ethics

WP7 contributed to the **overall project objectives** by specifying the overall ethical approach and requirements related to the project, including the experimentation with humans and the protection of personal data prepared for validation and demonstration (Objective 5). The ethics approach has been aligned with the technical work on the GEIGER solution and agreed with the use case owners. During the months M13-M18, the ethics approach will regulate how the GEIGER solution will be validated with the GEIGER use case MSEs. During the months M19-M30, the ethics approach will regulate how the GEIGER solution will be demonstrated with an increasing number of third party MSEs at TRL7.

Regarding the **work package objectives**, WP7 aimed at specifying the ethics approach during the months M01-M12 and will monitor the implementation of this approach during the months M13-M30. The resources needed for monitoring the implementation will be provided by WP4 “GEIGER Validation and Demonstration” and WP6 “Project Management.”

WP7 has achieved the work package objectives by defining how humans will be involved in the validation and demonstration research studies and how personal data regarding these humans will be protected in compliance with ethical principles and the GDPR.

The **deliverable D7.1** defines the purpose and scope of the research, the approach of GEIGER for identifying research participants, and the criteria to be used for selecting or removing research participants. In addition, D7.1 defines the procedures for dynamic, informed consent, which will be implemented by the use case leaders BBB in Switzerland, CLUJ IT in Romania, and SRA in the Netherlands. Finally, D7.1 offers the consent form to be used for involving the human subjects in the studies.

The **deliverable D7.2** gives the overview of data processing that will be performed in the GEIGER Framework, including the GEIGER Cloud, the GEIGER Toolbox, and tools that will be integrated into the GEIGER Toolbox. It describes how data will be minimised and protected in compliance with the GDPR with technical and organisational measures.

- It specifies the principles used to keep personal data needed to deliver the personalised GEIGER threat assessment and protection recommendation services stored and protected in the toolbox on the end-user device.
- It describes the cookie-enabled pseudonymisation-based approach of managing user data needed to track dissemination campaigns, assessing the attractiveness of the user interface and content, and letting the user set filters.

- It also describes how the directory of security defenders will be maintained. The technical, security, and organisational measures have been described for the GEIGER Framework and the tools integrated as plugins into the toolbox.
- It shows the privacy policies for the GEIGER Cloud and the GEIGER Toolbox.
- The deliverable finally declares the GEIGER joint controllers with their data protection officers and data protection frameworks.

The key results that have been accomplished in the first period are:

- Definition of how humans will be involved in the GEIGER validation and demonstration research.
- Dynamic informed consent procedures and form for the involvement of humans.
- Definition of the approach and measures for the protection of personal data.
- Organisation and procedures for joint controlling for personal data.
- Privacy policies for the GEIGER Cloud and the GEIGER Toolbox.

4 Impact and status KPIs of the Period

4.1 Overview of the Generated Impact

GEIGER has started to make MSEs better protected and become active players in the Digital Single Market, including implementing the NIS directive[9] and the application of the General Data Protection Regulation (GDPR). With the elicitation and explicit specification of the MSE context and needs, the GEIGER consortium gained a profound understanding of how to help MSEs to be better protected and more compliant to the GDPR. With the specification of the GEIGER solution, MSEs have been involved as active players and partners of cybersecurity tool vendors, cyber ranges, and CERTs/CSIRTs in the GEIGER digital ecosystem. The Minimum Viable Product of the technological framework contains a data protection technology in the GEIGER platform to protect the information of the MSEs and their users.

Moreover, GEIGER has developed and tested the messaging for efficiently reaching MSE owners and employees and a value proposition that addresses their needs (will be documented in D5.2)[10]. The communications have started to raise awareness of the importance of cybersecurity among MSEs and empower them to take the first steps to protect themselves and their businesses against cyber threats better.

GEIGER started to strengthen security, privacy, and personal data protection as shared responsibility along with all layers in the digital economy, including MSEs. The specified GEIGER ecosystem grounded on the results of comprehensive elicitation with diverse stakeholders. The ecosystem specification describes the security, privacy, and data protection needs of MSEs and how responsibilities for their effective protection are to be allocated as responsibilities to the ecosystem actors, facilitated by the GEIGER Framework. With the development of the GEIGER Indicator and the communication system, all users will be made aware aware about how their data is managed and protected, strengthening the security of their information and making them more open to sharing their data, which will have a beneficial impact on the digital economy.

In addition, the of the ´Data Protection Impact Assessment Tool´ that was validated by MSEs[11] contributes to strengthening personal data protection within MSEs.

Furthermore, GEIGER has identified standards for information exchange useful for GEIGER as an Information Sharing and Analysis Centre (ISAC) with third-party education providers, tool vendors, and CSIRTs/CERTs, identified standardisation-related gaps hindering information exchange, and initiated contact with related organisations and initiatives for a dialogue on filling the standards gap. These include the CERTs ENISA, NCSC in Switzerland, and Digital Trust Centre in the Netherlands and the peer projects in the Digital Society programme CitySCAPE, CNR E-CORRIDOR, PALANTIR, and PUZZLE.

GEIGER started to reduce economic damage caused by harmful cyber-attacks and privacy incidents, and data (including personal data) protection breaches. Individuals are the weakest link of the cybersecurity chain. With the educational tools (see section 3 of this report) the awareness of individuals can be increased, and damage avoided.

The project team specified the GEIGER solution and validated it conceptually with the consortium partners and stakeholders. The solution offers MSEs access to risk assessment and protection recommendations with the GEIGER Indicator, cybersecurity tools with sensor, protection, incident resolution, reporting

[9] For example, GEIGER helps improve national as well as EU-wide cybersecurity capabilities by creating an ecosystem with CERTs/CSIRTs and establishing an ISAC platform to improve communication with relevant stakeholders. In addition, cross-border collaboration between EU countries is foreseen.

[10] Messaging was developed simultaneously with the value proposition, discussing it with the MSEs in the consortium during the brainstorming sessions and workshops around the value proposition. On a small scale, different wordings and styles were used in social media posts and analysed according to reach and engagement.

[11] Workshop at the Trinational Cybersecurity Days https://www.fhnw.ch/plattformen/iwi/2021/03/29/trinational-cybersecurity-days-2021/

capabilities, educational tools for awareness, practical guidance, and secure behaviour training. In this context, a solution is being worked on that reduces the risk of economic damage and increases their awareness of MSEs. Due to the needs of the end-users, GEIGER has distributed clearly how each type of information will be stored in the local system of the end-users or the cloud. The aim is to clearly inform all users about how their data will be managed and receive permission to do this, describing how their information will be used.

Furthermore, GEIGER identified the account blocking attack that threatens many MSEs that utilise third-party cloud services and social networks. Once executed, the attack blocks the concerned MSEs from complying with GDPR data processor obligations. A draft policy brief describing the problem was formulated and presented at the P2PKOS kick-off with the participation of the EC REA.

GEIGER started to pave the way for a trustworthy EU digital environment benefitting all economic and social actors. The project team specified the GEIGER ecosystem, which takes a shared responsibility approach for protecting MSEs in any domain, including unskilled micro-enterprises. Responsibility is shared among MSE associations, trained individuals, educators, certifiers, tool vendors, CERTs/CSIRTs, third-party data sources, and security experts. Thus, diverse economic and social actors contribute to and benefit from a trustworthy EU digital environment.

Using GEIGER, the end-users will know how their data will be used and the protection mechanisms that will be used. They will always be able to change how it is managed. This way, the trust of the users in digital Europe will be increased. Additionally, creating a community of Education Providers is and will help build a network of trustworthy educational actors.

GEIGER started the diffusion of security and data privacy knowledge within the whole European industry incl. MSEs. The project team described cybersecurity educator and learner profiles and, in collaboration with the education work, derived requirements for the GEIGER educational approach for spreading security and privacy knowledge applicable for MSEs in the European industry. The channels considered were vocational training of apprentices employed by MSEs (Swiss use case), diffusion through accountants as service providers to MSEs (Dutch use case), and diffusion through training of entrepreneurs (Romanian use case). It is important to integrate the GEIGER platform with cybersecurity training and awareness as they are complementary to each other. Courses and training will inform users about their cybersecurity status and technical development, making them more aware of different ways to improve it. This awareness will make end-users more informed about cybersecurity and increase their resilience. GEIGER has facilitated the consortium members' outreach towards MSE and industry associations and networks to raise awareness among a variety of different industries in as many geographical areas as possible.

A gap in educational standards and offerings regarding security and data privacy education for users of cybersecurity technologies has been identified and resulted in a recommendation to address this gap in the P2PKOS policy workshop with the involvement of the EC REA and identified peer projects interested in cooperation for establishing such educational standards, including HEIR, PUZZLE. GEIGER has also initiated contact with the ENISA SME project and Small Business Standards as a potentially relevant standards-definition organisation. A discussion with the SPARTA project has also been initiated in this regard.

4.2 Overview of KPI Achievement

The following tables provide an overview of the impact and key performance indicators used to ensure that GEIGER reaches its objectives and continuously monitor and check the project's status[12]. Some of these indicators complement or are partly covered by deliverables. Even though the achievement of the indicators is a joint effort and often cross-cutting, they are nevertheless assigned to the ownership of exactly one WP. In the following, the progress summarising the status of the work so far is described. The indicators assigned to the pilot phase (WP4) are not included in this Year One Report as WP4 is starting officially in year two (M13).

[12] More detailed numbers will be reported in the 1st periodic report.

Indicators under the leadership of WP2

KPI	Description	Status at Month 12	Key Actions & Explanation on Operationalisation
1.1	1 dynamic context-specific indicator of the current risk status (GEIGER Indicator)	Initial version achieved	Initial version ready and used for testing data/results. Specification of information to be calculated for the GEIGER Indicator and how to better present it to MSEs
3.1	1 central GEIGER Cloud.	Initial version achieved	Initial version of the data repository and communications ready. Working in authentication and security mechanisms, the structure of data to be stored and exchanged has been defined. APIs for communication with different components of GEIGER developed as initial versions
3.2	4 open APIs allowing connectivity with MSEs, MSE associations, and CERTs/CSIRTs, and third-party tool and framework providers.	defined, in progress	Design done for the 4 APIs. Initial working versions for communicating with GEIGER Toolbox (tools), CERTs and MSE associations. Decide how the integration will be done; Decide on tools to integrate
I2.1.2.4	≥1000 MSEs are connected to the GEIGER Cloud	development in progress	Integrating functionality in the system. Decide in the authentication process and access control
I2.1.2.5	≥3 CERTs/CSIRTs have access to the incident database	development in progress	API for communicating with CERT implemented as initial version and structure of the data to be exchanged. Work with CERTs for refining the data structure
I2.1.2.6	≥3 data protection authorities have access to the incident database	development in progress	API for communication following the same work as the one for the CERTs. Work in the functionality of the data protection authorities in the GEIGER platform.
I2.1.2.7	≥150 Security Defenders have access to the incident database	development in progress	Developing access to the incident database, closely linked to WP3 activities. Define how the cyber security defenders will access the incident database, access control to users and the data they will interact with.
I2.1.4.6	≥10 tools providers will have confirmed their intent to integrate their tools into the GEIGER toolbox.	design in progress	Design of API for integrating external tools under work. Work in the integration of tools in the GEIGER platform in terms of data and communication.

Indicators under the leadership of WP3

KPI	Description	Status at Month 12	Key Actions & Explanation on Operationalisation
2.1, 2.3	≥ 5 Capability areas addressed by training modules	defined, in progress	Three-dimensional differentiation of curriculum, among others: pragmatic design of threat landscape (or its ‘areas’) – the targeted development of learning materials is following
2.2, 4.2	≥ 2 Learning games	defined, in progress	Conceptualisation of and integration into the educational ecosystem of game-based learning features from different partners advancing on different stages.
2.3, 4.3	≥ 5 Cyber-range supported challenges	defined, in progress	Conceptualisation of and integration into the educational ecosystem of two cyber-range like features, for IT lay-persons and experts, from partner MI with different sets of tasks or ‘challenges’ advancing on different stages

I2.1.4.4	≥50 education providers, incl. schools/universities, professional associations or unions, and incubators or accelerators for start-ups, will have confirmed their intent to offer the GEIGER education.	planned	GEIGER education has not reached the concreteness to be disseminated on this practice-oriented level.
I2.1.5.2	≥200 educated CSDs	definition started	Initial workshop with 'test' CSDs has been conducted.
I2.1.5.3	≥100 certified CSDs	planned	Initial workshop with 'test' CSDs has been conducted. Criteria for pertinent certification scheme have been discussed.

Indicators under the leadership of WP5

KPI	Description	Status at Month 12	Key Actions & Explanation on Operationalisation
I2.1.1.1, I2.1.5.1	>500'000 MSEs will be aware of the GEIGER Indicator as a dynamic risk monitoring instrument, and ≥1'000 industry-diverse MSEs that know the GEIGER Indicator.	definition ongoing	Delay in launching the newsletter subscription form and in launching the active outreach towards multipliers, the progress of this KPI is under the set goals. Mitigating actions to improve the progress on this KPI: • Enforced promotion to sign up for the GEIGER news. • New GEIGER 'editorial team' composed of consortium members from different areas of expertise (kick-off May 2021): coordination of planning, production, and quality control for the communication materials towards multipliers.
I2.1.1.2	>50'000 MSEs will have tried the personalised GEIGER Indicator for their own specific MSEs by registering on GEIGER Solution	planned (M19-M30)	1) Communications through all channels to familiarise the potential end-users with the GEIGER interface and functionalities 2) Targeted training & workshops on the use of the GEIGER tools
I2.1.2.8	1 open API with API access governance policies for querying incidents and submitting information	defined, in progress	See KPI I2.1.2.9.
I2.1.2.9	4 contributions to standardisation work or Memorandum of Understandings with related initiatives for harmonising external GEIGER Framework interfaces and the security defenders education. ≥2 contributions to standardisation	defined, in progress	Following contribution are defined and in progress: curriculum with packaged syllabi, xAPI-based interoperability, API for information sharing with CERTs (incl. incident query), and P2PKOS policy recommendations
I2.1.4.1	≥1'000'000 impressions of the GEIGER Indicator as measured by the number of impressions of media channels.	defined, in progress	14% of the KPI target has been reached, exceeding our objective for this stage of the project by 2,5%. Activities:

			1) Mass media impressions 2) Targeted media impressions 3) Social media impressions (via GEIGER and partner channels) 4) Impressions in events (consortium partners' participation as speakers)
I2.1.4.2	≥100'000 small enterprises have a GEIGER account, allowing them to predict their risk with the personalised GEIGER Indicator and benefit from the GEIGER toolbox.	planned (M19-M30)	Requires MVP of the GEIGER Indicator/Toolbox. Planned activities: 1) Integration of an easy procedure to create a GEIGER account to the GEIGER website 2) Targeted 'Call to Action' communications towards subscribers and followers
I2.1.4.3	≥20 MSE associations or chambers of commerce in ≥50% of the member states will have confirmed their intent to recommend the GEIGER Framework among their member enterprises.	defined, in progress	Mapping and listing the ones already on board. Initiating contacts with potential ones. 1) Mapping the MSE associations and chambers of commerce in the EU member states represented by the consortium members 2) Facilitating the outreach by creating introduction material and best practices
I2.1.4.5	≥50% of the CERTs/CSIRTs in member states will have confirmed their intent to interoperate with the GEIGER Framework	defined, in progress	4 have already confirmed: CERT-RO, NCSC, DTC, ENISA 1) Establishing contacts in the early stages of the project 2) Collaboration and involvement of the CERTs/CSIRTs in the development of the framework

5 Dissemination Activities

Dissemination activities have advanced as planned.

During the first phase (M1-M6), the internal alignment took place within the consortium, and the tools, channels and practices of internal collaboration were set up.

During the first part of phase 2 (M7-M12), the work to generate interest and to build communities, in particular those of the 'multipliers', e.g. MSE networks and associations, has started, and the materials and guidelines for this outreach have been drafted and made available to consortium members. T5.1 has also contributed to the planning of building the GEIGER education community.

According to their capacities and focus, consortium members have participated in the planning and execution of the dissemination activities. During the reporting period, the consortium

- established the communications infrastructure for the project, including the website, social media channels, and newsletter, as well as the visual style guidelines
- defined, in the D5.1 Impact Plan, the blueprint for our outreach strategy and actions
- disseminated GEIGER in over 30 external events, in addition to the consortium's internal workshops with invited guest experts
- published 14 articles on the GEIGER website
- published in total nearly 250 posts in GEIGER and consortium members' social media channels
- sent out 11 newsletter mailings with a total reach of over 70 000 MSE owners and employees
- counted over 30 media mentions of the project
- prepared an introduction poster, flyer, short and extended versions of introduction presentations, a timeline of the project phases, as well as a step-by-step guide for reaching out to partner or dissemination 'multiplier' organisations to support the consortium in its outreach towards the project's stakeholders
- developed a crisis communication plan and guidelines to guarantee a timely and uniform response in case of a threat of a reputational crisis
- actively collaborated with the small businesses in the consortium to formulate and test the GEIGER value proposition (under the lead of T5.3) – critical also for building messaging that appeals to our primary target audience
- started adapting the communication materials to the specific needs of the pilot use case countries
- aligned the events with peer projects in the field of cybersecurity, on the EU level.

Some of the highlights of the dissemination activities were:

- Cluj Innovation Days panel discussion on 'Increasing the digital resilience of small businesses': WP5 coordinated and moderated this online panel discussion in the context of the Cluj Innovation Days, with the speakers primarily from the project consortium. The goal was to raise the audience's interest in cybersecurity issues in MSE environments and offered a starting point, GEIGER, to address these problems.
- #CyberSecMonth campaign: In October 2020, WP5 ran a social media campaign, on the occasion of the European Cyber Security Month, to promote awareness on cybersecurity risks among small business owners and to introduce some of the key concepts and skills to acquire to lower the risks. The campaign was published on the project consortium's social media channels under the GEIGER branding, actively shared by the project consortium, and raised interest around the topic of cybersecurity and the GEIGER project.
- Pilot use case workshops: The workshops with consortium members and external stakeholders[13] to kick-off the three pilot use cases of the GEIGER project in Switzerland, Romania, and the

[13] Swiss workshop: Swiss National Cybersecurity Center; Dutch workshop: Digital Trust Center, Cybersecurity and external privacy consultant, Romanian workshop: two external cybersecurity experts

Netherlands took place during the first five months of the project. They gathered the participating consortium members to discuss the use cases' requirements and goals and initiated an impressive range of contacts with third party contributors and audiences, such as MSE and start-up networks, CERTs, security experts, and potential future Security Defenders. The outcomes of these workshops are described in detail in D1.1 Requirements.

The detailed numbers will be reported in the 1st periodic report. Reference to EU funding is included in all dissemination material. Funding references were incorporated on the social media profiles.

6 Exploitation Activities, Innovation, Policy and Standards

The general objective of the GEIGER project is to design and develop a comprehensive cybersecurity solution for small businesses, including start-ups and micro-enterprises that fits with the cultural behaviour and particular needs of this target group. GEIGER project recognises the vital role that MSEs play in reducing damage due to data-related incidents for the European economy. Around 24.5 million MSEs represent 99% of the players in the EU economy and, as opposed to the large players, are more vulnerable due to lack of awareness, lack of culture preventing human error and attack, and lack of utilisation of suitable tools.

GEIGER unfolds its **innovation capacity** by developing experiential challenge-based education of security, privacy, and data protection skills for Certified Security Defenders available to MSEs. It creates an extensible GEIGER Toolbox tailored for incident avoidance, detection, and mitigation in MSEs and a GEIGER Cloud in which the GEIGER Indicator and an incident database are running. The GEIGER Framework connects MSEs, MSE associations, CERTs/CSIRTs, Certified Security Defenders, and relevant third-party actors. When eliciting the requirements in WP1, the approach towards defining and designing a digital ecosystem is putting forward the state-of-art. The technical components from WP2 show innovation capacity, such as taking privacy awareness by design to the next level. The users can control fine-grained what data is shared and with whom. From the educational part (WP3), an ambassadors' community building and involvement unfold high innovation capacity. The educational approaches move forward the state-of-the-art in applying gamification theory. The approach to developing an interoperable curriculum based on xAPI as a machine-readable format is an innovative example for digitalised education. Looking at WP5, the initial view of the GEIGER business model associated with the approach and governance will be an innovation putting forward the state-of-the-art of open innovation projects. Related to standards and policy, the taken bottom-up approach that builds on alignment and co-creation between peers in the practice/research fields has the potential to unfold innovation capacity and lead to new standards.

In the first period, WP5 followed the plan engaged by the GEIGER project. Requirements for the software toolbox have been elicited in tight connection with end-users from the target group. Besides advanced techniques for investigation, requirements extraction and structuring, end-user representatives were involved in the co-creation of these requirements. The result paves the road for defining a technical solution that fits the target group needs. Moreover, representatives of the target group were directly involved in a series of sessions for defining the value proposition. Interactions with representative organisations for standardisation and European initiatives for cybersecurity (e.g., ENISA, Cybersecurity4Europe, CERTs) have also been undertaken to prepare the transfer of project results in future standards and practices of cybersecurity that target this particular segment of MSEs. It was decided decided to introduce and apply the lean innovation concept for preparing the road to set up a sustainable start-up where GEIGER Solution will be transferred at the end of the project. In line with this, preparations have started for a safe framework for IP management generated in the project. An open innovation platform connected to potential investors will assist the foreseen approach with blockchain features to ensure safe management of foreground IP. Market education is essential to the target group envisioned by GEIGER. In this respect, up to this date, preparations have started for the database with multipliers across Europe to reach as many as possible MSEs for introducing even from early stages the GEIGER solution to the target market. The preparation of the educational programis on track as well. In this respect, interactions have been made with representatives of the target group in workshops and focus group sessions and surveys for calibrating the curricula.

Relationships with ENISA and Cybersecurity4Europe have been established to introduce GEIGER objectives and pave the road for transferring results in cybersecurity standards and the framework of the European network of cybersecurity. GEIGER is aligned with EU Cybersecurity Strategy.

The GEIGER project is explicitly **focused on MSEs**. In the first project period, the work carried out in the project involved SMEs representatives in all critical phases (needs clarification, requirements formulation, value proposition design, curricula calibration). Now, the stage to expand the connection with MSEs at the

European level with multipliers from more EU countries has been reached. In this initial exercise, called promoter test, the value proposition and the major features of the GEIGER solution with MSEs that will have the first contact with the GEIGER project will be validated.

The **exploitation activities** from the first period enhance BSc and MSc-education offering based on D1.1 at FHNW and PhD research on digital ecosystem design based on GEIGER case building upon D1.1 and D1.2 FHNW (joint publication in progress). Generally, the outcomes of WP1 (D1.1+D1.) are exploited in WP2, WP3, WP4, and WP5. As one exploitation, the GEIGER project could be exploited to support the promotion of one consortium member as a full professor. The GDPR Data Protection Impact Assessment is exploited as part of FHNW executive education. The virtual cybersecurity escape room has been exploited in the context of the SATW SwissTecLadies Mentoring Program, where the game was offered as a mini-awareness workshop. Within the consortium, the use cases will exploit the xAPI-curriculum and the learning games (CSMG) for non-IT apprentices.

For **exploitation** of the results expected to the end of the project, we analyzed potential paths and the actions we must undertake in this respect. There are five major paths for exploitation: transfer of results in the GEIGER spin-off, local exploitation of joint results, local exploitation of own results, license some of the results to third parties, and non-commercial exploitation.

In the case of the transfer of results in the spin-off, we apply the lean innovation methodology. Up to the end of the first year of the project, we formulated the value proposition. We are in progress with the first exercise to collect feedback from potential end-users by investigating the value proposition and the theoretical prototype. To design an attractive value proposition, we conducted a series of exploration sessions where representatives of end-users have been involved. The phase of requirements collection for the GEIGER solution considered the idea of co-creation, too, which involved gradual interaction and from different perspectives with end-users. To run the promoter test, we have identified multipliers all over Europe. Some of them were contacted already, and others will be contacted in the first months of the second year of the project to connect GEIGER with end-users in the various Member States of the European Union. One channel is the Enterprise Europe Network. In the countries where the GEIGER consortium has members, additional multipliers are considered (Chambers of Commerce and Industry, Professional Associations of SMEs, Cluster initiatives and DIHs, etc.).

To transfer the results of GEIGER to the spin-off, we have started to prepare the frame for IPR management. To this date, we have identified and started to configure a blockchain-based platform for IP management and the assessment criteria of IP results. The platform is called DEIP. The IPR arrangements and the related agreement between GEIGER members are in progress at this moment. We also accessed the Horizon Booster platform for assistance in business model innovation the prepare the spin-off set-up. Our application has been approved, and soon we will start to work closely with the consultant.

One path is the local exploitation plan. In this respect, we completed a first round of investigation of partners about their perspective to locally exploit the GEIGER results, both generated by each partner and those generated by the consortium. To this date, nine of the partners formulated the first draft of the exploitation and IP plan.

The second path for exploitation is to transfer results from GEIGER in a spin-off. In this respect, we have prepared the skeleton of the **exploitation plan**.

7 Ethics, Diversity and Data Management

All **ethics** requirements received from the Ethics review have been implemented. The GEIGER ethics approach is aligned with the GEIGER technical framework, the planned validation and demonstration research, and the organisation of the use cases trials in the three use case countries Switzerland, Romania, and the Netherlands. There is a documented specification and shared understanding in the consortium concerning the involvement of humans in GEIGER validation and demonstration research and concerning the protection of personal data.

When turning to the **diversity aspect**, the GEIGER consortium involves females for a bit more than one-third of the staff and males for a bit less than two-thirds. The detailed breakdown by sex and partner will be reported in the periodic reports.

We have been working with tool owners about how **data management** could bring data protection and privacy issues. So far, we have no issue highlighting or indicating we need to update the project's data management plan. As we will work more closely with use case partners after this period, we plan to have better feedback about how the data management plan and ethics align with their needs and will update as necessary. As they will contribute and work with their own data, GEIGER provides good solutions and approach for their needs.

8 Project Management

FHNW is responsible for the Project Management work package, WP6. The two tasks in WP6 are continuous tasks (T6.1 & T6.2) that last until the end of the project. In order to set up and implement project management professionally, PMBOK® and HERMES (an open project management standard developed by the federal administration of Switzerland) was adapted as the underlying method.

In the following sections, the major achievements so far are described.

1. The project office, contact point and support for the consortium, has been established.
2. Monitoring and reporting processes have been established. The contractual, legal, and financial activities are organised and managed, e.g., Consortium Agreement, EC Grant Agreement and amendments, supervision of financial issues.
3. Regular, firmly established meetings with the Consortium are scheduled and carried out every six months.
4. The PMO has set up the following infrastructures to ensure effective and efficient collaboration during the project:
   - Document repository and exchange platform on Nextcloud
   - Mailing lists, managed and adaptable by the PMO
   - EMDESK Financial Reporting Tool
   - 360inControl; Risk Management, KPI Management, and auditing tool.

In the first 12 months of the GEIGER project, the following main management tasks have been successfully carried out:

- The project kick-off meeting was held online (due to travel restrictions in the face of Covid) and hosted by FHNW on 3rd June 2020. A detailed agenda was planned to maximise the efficiency of the kick-off.
- Additional CMs were held with detailed agendas
  - CM2 on 10th December 2020, online
  - CM3 on 20th May 2021 online.

- The AB was established, and the first board meeting was held on 19 January 2021; the second is planned for 8 June 2021.
- The Executive Board, consisting of all WP leaders, the coordinator, and the ethics advisor, meets every month to discuss each WPs progress and potential issues concerning the project's advancement. Executive Board meetings are held separately on a monthly basis. The following Executive Board meetings have been held so far:
  - 06.07.2020
  - 03.08.2020
  - 07.09.2020
  - 05.10.2020
  - 02.11.2020
  - 04.01.2021
  - 08.02.2021
  - 01.03.2021
  - 12.04.2021
  - 03.05.2021
  - 10.05.2021
- The PMH has been produced detailing all project management and governance procedures within the project.
- Project procedures, templates and supporting tools for ensuring successful and effective cooperation and technical work development have been defined and set up.
- Periodic WP/task level teleconferences supported with desktop sharing tools have been held.

- In cooperation with the consortium members, a detailed data protection policy has been established.
- The scientific and technical coordinators actively contributed to the design thinking for the GEIGER solution and the aligned GEIGER ecosystem, resulting in refining the original vision at the level of third-party roles and GEIGER solution components, including their assigned responsibilities/ capabilities and interdependencies. Innovation opportunities were identified, and the associated scientific research and publication actions launched.
- Scientific work performed in the consortium was reviewed for ensuring the quality of the deliverables and innovativeness of the reported work.
- Periodic teleconferences with the Technical Coordinator, Scientific Coordinator and WP6 Lead have ensured clear tracking and steering of the project.
- The supervision and revision of the production of all the project deliverables due in the first 12 months of the project were carried out. The project's overall status with respect to the production of deliverables, adherence to plan and achievement of milestones was continuously monitored, and interventions made where necessary. The pre-payment from the Commission was distributed to partners following the terms of our Consortium Agreement. Communication was maintained.
- The project management structures and rules for data management and ethics set the ground for the overall project work, enable partners to work professionally, efficiently, and compliant with the overall project objectives. In addition, the external stakeholders, such as the Advisory Board, have a clear view of the project.
- The present report was produced by collecting inputs from all WP leaders about the progress of the different WPs and reporting about overall project progress and management tasks.

8.1 Challenges and mitigating actions due to Covid-19

FHNW had to face the ongoing Covid-19-restrictions that did hardly allow for personal meetings with the consortium and were challenging for project management. This impacted the progress of the project as it generally slowed down work due to increased need of coordination. Additionally, the pandemic led to a reduced consumption of allocated travel budget and thus required restructuring of the budget. As a reaction, risk-mitigating actions have been taken, such as:

- Immediate transfer of all foreseen face-to-face meetings to online teleconferencing tools, such as GoToMeeting, Webex, or Zoom.
- Regular One-on-One meetings between WP6-Lead and partners to review resource consumption and discuss any other business (risks, events, and concerns).
- An internal audit has been initiated and carried out to review the maturity of the project management and related governance, risk, and compliance tasks.
- Comprehensive risk management has been initiated and carried out: due to a challenging situation to manage a research project with 18 partners in 9 countries in a virtual-only environment, we recognised that the risk for the overall project is increased. Therefore, we extended our risk management approach supported by a professional compliance software (360inControl). This solution allows transparency, traceability, and clear ownership of risks. It also assigns and tracks mitigating actions, conducted regular risk assessment reporting, and contributed to lowering the overall project risks.
- Regular T6.1, T6.2 and WP6 meetings (each scheduled bi-weekly).

To ensure a smooth alignment with all WP leaders and mitigate any potential misunderstandings arising from meeting in person, regular calls have been established between the PMO and the WP leads. The financial reporting, risks, KPIs, and any other potential issues were discussed during these calls.

- As specified in the PMH, risk management procedures have been established to continuously track and update the risks and discuss them in the EB meetings. The risk management process has been professionalised through the established compliance software (360inControl) to visualise, continuously track changes and monitor the risks.

- When allowed under the difficult Covid-19 constraints, FHNW organised and participated in face-to-face meetings with partners in Switzerland, the Netherlands, Romania, Germany, and Italy in conjunction with the work performed in WP1. These meetings were performed in a hybrid manner, allowing as many partners as possible to meet physically while allowing those who could not travel to join remotely.

8.2 Project Time Planning and Status

The workplan for the GEIGER project, with a duration of 30 months, has been separated into five phases of six months each. The phased plan was documented in a Gantt diagram (using the EMDESK tool). Each of these phases has at least one milestone to be reached within that set period.

MS1 Requirements Defined M6

MS2 Architecture Defined M12 (current stage)

MS3 GEIGER Indicator MVP M12 (current stage)

MS4 Integrated Prototype M18

MS5 Minimally Viable Product (MVP) M24

MS6 Demonstrated Release M30

MS7 Project End M30

This workplan has also been integrated into EMDESK, a project management solution for research projects. This solution allows us to track exactly at what project stage GEIGER stands. To ensure that the project is progressing as planned, regular meetings are scheduled (EB, CMs, individual partner meetings) to discuss the current status and mitigate potential issues. To ensure quality and the timely completion of the deliverables, a review process has been implemented.

8.3 Progress and Financial Reporting and Monitoring

The Coordinator FHNW is a financially sound public body experienced in coordinating EU projects with the necessary experience, procedure, and staff for administrative coordination. Financial management, keeping records of the distribution of funds, monitoring partners' efforts and expenses and immediately informing the Project Coordinator of any identified deviations according to the financial plan. In addition, FHNW is also responsible for information management: developing and maintaining the adequate project information management framework, using adequate management tools, and developing and maintaining the information flow internal and external to the project.

The PMO provided a time tracking template based on EU standards to all partners and supported those who used the template. To ensure that all partners understood the process and what was required to report, the PMO implemented EMDESK to track all financial reports of each partner. The PMO personally onboarded all partners and supported the partners for the first data insertion. Every three months, the PMO compiles a report and discusses the reported numbers in detail with each partner individually.

The principle of sound financial management has been followed for the use of resources: The resources were used as described in the DoA to achieve the objectives. Deviations from the planned budget have been satisfactorily explained and justified.

8.4 Risk and KPI Management

Risk Management

As specified in the PMH, risk management procedures have been established to track and update the risks continuously, as specified in the GA, and to discuss them in the EB meetings. The risk management process has been transferred to a new software tool, 360inControl, to visualise, track changes and monitor the risks. This solution allows transparency, traceability and clear ownership of risks, assigning and tracking mitigating actions, conducting regular risk assessment reporting, and lowering overall project risks. All WP leaders were onboarded individually by the PMO. Every three months, the PMO and the WP leaders have a call to perform a risk assessment. The resulting report is discussed, incl. mitigating controls and is uploaded to the cloud.

Major risks that have already been identified during the planning of the GEIGER project and the associated and updated mitigation measures are described in the following table 4.

Risk No.	Description	WP No	Risk Mitigation Measures	Status
1	Difficulties in eliciting MSEs requirements	WP1	Partners in the consortium have a strong position in the industry, covering the overall spectrum of areas that are related to requirements specification, software development and integration. In addition, many partners have strong experience in the security area. With these two skills, the risk can be absorbed.	Retired
2	A product with similar characteristics appear in the market	WP2, WP3, WP4, WP5	Partners in the consortium have a strong footprint in ongoing research initiatives, industry trends and standards discussions; hence, covering most of the potential market segments and initiatives running in parallel to the GEIGER proposal. Right now, state-of-the-art products are far behind GEIGER objectives and expected innovations. **NEW**: Analyse similar solutions & adopt their benefits; Keep up with development in cybersecurity news channels.	Monitored
3	The integration phase of the prototype in the pilot takes longer than anticipated	WP2	If the pilot phase proves more difficult than anticipated or lasts longer than expected, we will evaluate the options to reduce the provided security functionalities. We consider this risk very low as the use cases are defined by real services already developed by the partners within the consortium. **NEW**: Increase piloting task force and evaluate planning.	Monitored
4	Withdrawal of partner, partner/s leaving the consortium	WP6	The Executive Boardwill decide whether another partner can take over the activities or initiate the replacement process as soon as possible.	Monitored
5	Key staff or skills leaving the project	WP6	Get an early indication of possible withdrawal of key staff from partner if not internally replaceable. Contact all partners to seek similar competencies. Otherwise, initiate adding a new partner to the consortium. Shift the budget to the other partner(s) that provides the competencies.	Monitored
6	Underperforming Partner	WP1, WP2, WP3, WP4, WP5, WP6, WP7	Manage grace periods initially and get the partner to focus or replace people. Otherwise, WP Leaders to improve the planning of activities for upcoming deliverables. Shift the budget from the defaulting partner to the partner(s) that achieve the committed work. **NEW**: Check with underperforming partners and re-evaluate work in the task; Ensure communication and periodic updates; Implementation on of tools (EMDESK, 360inControl) to provide assistance with financial reporting, risk and KPI management and ensure that all partners are able to deliver at the required level; implementation of internal controlling processes (Time sheets).	Monitored

7	Resistance of MSEs to share security-related data with CERTs/CSIRTs.	WP4	Trust measures as key to project design: Harnessing existing trusted relationships to introduce MSEs to the GEIGER Framework. Levelled data sharing: MSEs enabled to configure the level of data sharing (trust can be built up over time, and data sharing can be increased according to the trust level of MSE). **NEW**: Until 1. June 2021 the usability of the prototypes needs to be monitored; Until 1. Dec 2021 the promotion of upcoming availability needs to be pushed..	Monitored
8	No sufficient interest in joining and contributing to ‘Security Defender Community´	WP3,	Diversified types of potential ambassadors are involved in the project. In Switzerland, the apprentices, in the Netherlands, the accountants, in Romania, the start-up association. Commitment to the project ensured by the large consortium containing critical partners for community initialisation. Incentive schemes for ambassadors will be developed (e.g., a certification or prizes). **NEW**: Planning for adequate community management initiated.	Monitored
9	Reverse mentoring not as successful – to transfer the content to MSEs	WP3,	Reverse mentoring proves successful in familiar IT-related fields. Mentoring approach embedded into a holistic model that ensures preparation of mentors/mentees, guidance during realisation, and measures to ensure sustainable assimilation. **NEW**: Support infrastructure for potential reverse mentoring defenders is in evaluation.	Monitored
10	Communities (Education Provider Community, Security Defender Community) not sustainable after project end	WP3,	Community building based on well-tested methodology. Strong involvement of MSE association as (full and associated) partners of the consortium. In the Netherlands, SRA, an accountancy association with large spread and support of European Association ‘Accountancy Europe’, to leverage the community to an EU scope. In Switzerland, SKV, a Swiss association and support of ICT-Berufsbildung, sustainably embed the Security Defender Certification into the apprentice’s curriculum. In Romania, Cluj IT, an association linking Balkan, the Black Sea, and Baltic Cluster (+20 clusters). **NEW**: Business model including sufficient cross-subsidizing for community management initiated.	Monitored
11	Dissemination underperformance	WP5	The project's strategy for dissemination has been elaborated at the beginning of the project and is updated as needed during the project. Definition of audiences and targeted actions guide the activities, which are assessed to help maximise their impact.	Monitored
12	Inadequate project management	WP6	Demonstrated capabilities of the Coordinator as well as the consortium members in a series of successful projects. A complete and systematic project management plan. Appropriate allocation of work and tasks to project members.	Monitored
13	Delays in key milestones or critical deliverables	WP6	Carefully monitor progress using project milestones and regular meetings to detect any delay quickly. Prioritise workload and shift resources by reducing effort on non-critical tasks, even if this implies a shift of resources between partners. **NEW**: Tool 360inControls initiated for monitoring risks that might impact key milestones or critical deliverables.	Monitored
14	Conflict between partners	WP6	Apply rules on the decision-making process and conflict resolution procedure.	Monitored
15	IPR related problems	WP6	The Consortium Agreement establishes the legal framework for the project to provide clear regulations for issues within the consortium about IP ownership.	Monitored

16	Partner organisations with financial problems require restructuring the budget	WP6	The project monitors each partner's performance based on the monthly reports and the deliverables. If needed, corrective actions might be taken, including the possibility to reallocate resources between partners or bring in a new partner with the required skills and personnel availability. None of the companies in the consortium has declared current or past financial problems during the proposal preparation phase.	Monitored
17	Lack of internal communication	WP6	The regular meetings, appropriate tools (including website, mailing list) and the reporting and communication flow process described above provide the right level of internal communication. Adaptable communication tools have been adopted as needed. **NEW**: Encourage 1:1 calls instead of a flood of e-mails. Communications are not made easier due to ongoing Covid situation hindering Face-to-Face contact, and targeted communications instead of large meetings. Communication on an individual level (checking in with each partner). Should any issue arise, WP6 will escalate to the EB.	Monitored
18	Underestimation of necessary efforts for certain tasks by partners	WP6	This could introduce significant delays in tasks, and hence, a clear impact on the milestone deadlines. The project handles this risk by continuous supervision of the project progress and by (optionally and in execution time) re-allocating resources between partners.	Monitored
19	Redundancy of KSP work with TRAPEZE or CitySCAPE	WP2	KSP confirms that the allocated budget and effort corresponds to the unique work in the GEIGER project. However, if during the requirement analysis phases of the three projects (TRAPEZE, GEIGER and CitySCAPE) some common features leading to a work in Kaspersky Mobile Security Software Development Kit (KMS-SDK) which can be shared to more than one project will emerge, agreeing with the coordinators, KSP will record the related costs only to one project.	Monitored
20	Dependency of KSP work with TRAPEZE or CitySCAPE	WP2	There are no planned dependencies for KSP work in GEIGER from other ongoing/completed projects/currently under GAP projects. However, since the same team of people will be involved, if during the requirement analysis phases of the three under GAP projects KSP is involved (TRAPEZE, GEIGER and CitySCAPE) some common features leading to a work in Kaspersky Mobile Security Software Development Kit (KMS-SDK) which can be shared to more than one project will emerge. Agreeing with the coordinators, KSP will schedule the dependencies to guarantee the timely delivery of the expected input for each project.	Monitored

Table 4: Project Risks

KPI Management

Procedures for regular tracking of the KPIs have been initiated. The project has identified appropriate KPIs to monitor the performance of each activity and the overall project. The WP leads have requested the KPI planning, and the fulfilment for the first period was reported. Every three months, the progress of the KPI's is discussed in individual calls with each WP leader. A new process to capture KPI achievement has been initiated.

8.5 Advisory Board

The first Advisory Board (AB) meeting was carried out on 19 January 2021. All AB members from following affiliations were present: Cambridge Cybercrime Centre, Capgemini Invent, CERT-RO, EY, Nyenrode Business University, Swiss Academy of Engineering Sciences SATW, Swiss National Cybersecurity Centre NCSC, The Computer Laboratory of Cambridge University, Universität Koblenz Landau. It was ensured that the AB is constituted of experts in the field of education as well as technology, and that academia, industry, as well as governmental bodies are represented.

From the GEIGER consortium, the following partners were present: FHNW, UU, Tech.eu, PHF and ATOS. Individual points were then discussed with the AB members, and some recommendations were developed that will be incorporated into the continuing GEIGER project. All participants confirmed the significance of GEIGER; the AB members confirmed the GEIGER project and its objectives to be highly significant, both micro-perspectival for the individual MSEs (in the EU) and macro-perspectival for the respective economies. The following conclusions and actions were developed:

- **Certified Security Defenders:** MSE staff should be motivated to be recruited/addressed (as a target group).
- **Different MSE types need to be considered:** a risk-oriented approach depending on SEM&MEs 'business model'; e.g., baseline risks (treats); risk appetite, awareness situation.
- **Consider the specific situation in the Netherlands (auditors/tax advisors):** e.g. probability vs impact of risks; method/algorithm of the GEIGER indicator needs to be traceable; legal assurance, (without) obligation; auditors taxonomy needs to be considered; 'Future of Audit' organisation as a reference?
- **Consider specific MSE situation:** motivation to use GEIGER and educate in cybersecurity is difficult to win; also, ethics perspectives (GEIGER education tracing in the tool?) need to be well thought out.
- **Consider similar projects in Switzerland or EU-wide:** must be found out and, if necessary, connecting points must be investigated and, if possible, realised. The SATW representative offered pointers for Switzerland.
- **'Threat intelligence' needs to be considered: the** focus should be on the detection area.
- **Certifications:** ENISA should be consulted.
- **'Digital/Cyber literacy' needs to be strengthened:** focus on data privacy for the users (education result tracking) needs to be well thought out.
- **Regarding the contribution to Standards/Standardisation**: in the UK, standards in the education environment could be useful to consider; in NL, COBIT is an often used and known standard; in addition, in NL, 'Audit of the Future' could be a good discussion partner (when the project is more advanced);

The second GEIGER AB meeting is scheduled and confirmed for 8 June 2021. The names of the AB members as well as detailed meeting minutes are held on the GEIGER nextcloud.

9 Readiness for Piloting

Readiness for the trials in use case countries

Although it is too soon to determine the readiness for the GEIGER trials at this preliminary stage, it can be stateted that GEIGER is currently running ahead of the GEIGER Piloting phase schedule, as WP4 officially does not start before 1 June 2021. However, several significant steps have already been accomplished to further optimise WP4's success:

a) The ´Hopster Validation Framework´ (see Figure 3) was selected as the WP4 foundation and has been further investigated for the feasibility of this framework.
b) A preliminary planning overview to facilitate partner communication has been developed.

Regarding (a), UU (leader of WP4) has performed research to identify a scientifically validated best practice validation framework that is suitable to guide the GEIGER solution validation process during WP4:

- Hopster-den Otter, D., Wools, S., Eggen, T.J.H.M. and Veldkamp, B.P. (2019), A General Framework for the Validation of Embedded Formative Assessment. Journal of Educational Measurement, 56: 715-732. https://doi.org/10.1111/jedm.12234
- Wools, S., Sanders, P., & Eggen, T. (2010). Evaluation of validity and validation by means of the argument-based approach. Evaluation of Validity and Validation by Means of the Argument-based Approach, 1000-1020.

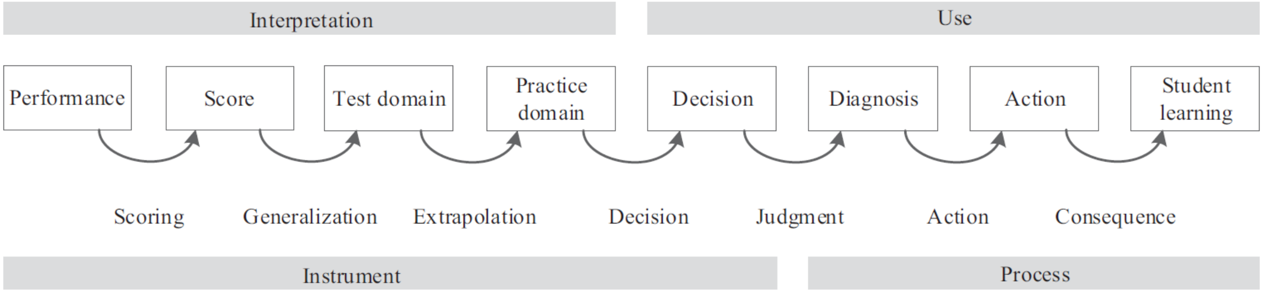


Figure 3: Hopster's Evaluation Framework

Figure 3 describes the generalisable Hopster Validation Framework. The Hopster framework takes a so-called argument-based approach to validation to the context of formative assessment, resulting in a proposed interpretation and use argument (IUA) consisting of a score interpretation and a score use. The former involves inferences linking specific task performance to an interpretation of an MSE's general performance. The latter involves inferences regarding decisions about actions and training consequences. The validity argument focuses on critical claims regarding score interpretation and score use since both are critical to the effectiveness of the formative assessment.

From February 2021 onward, UU, SRA and FNHW have initiated and coordinated several brainstorming sessions to empirically explore the feasibility of the Hopster Validation Framework in daily accountants' and their clients' practices. Furthermore, UU has discussed the GEIGER Solution application of the Validation Framework with one of the supervisors of the Hopster research to evaluate our approach with one of the experts on solution validation using formative assessments.

To align GEIGER with the Hopster Validation Framework, UU has mapped all GEIGER user journeys to the appropriate steps in the Hopster Validation Framework, a fragment of which is shown in the Figure 4, which visualises the mapping of the Hopster Validation Framework to the GEIGER end-user journey as specified in D1.1.

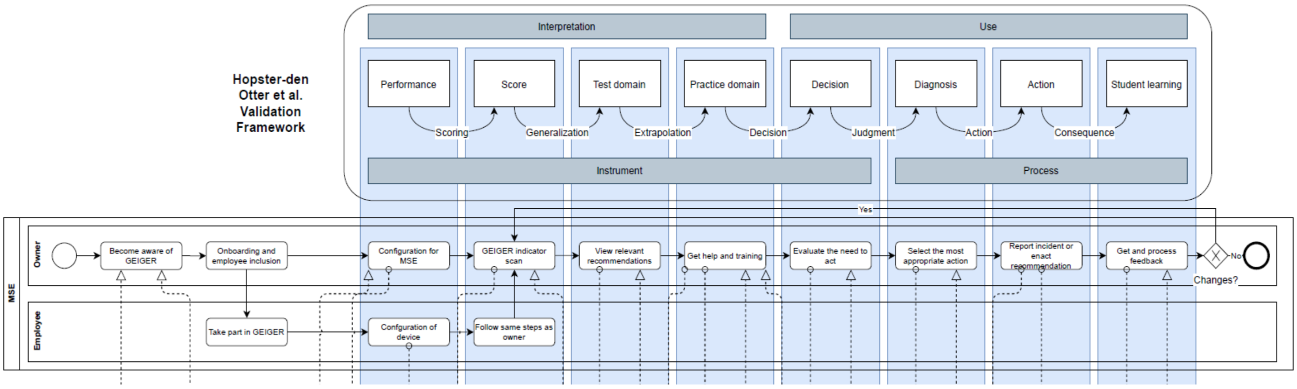
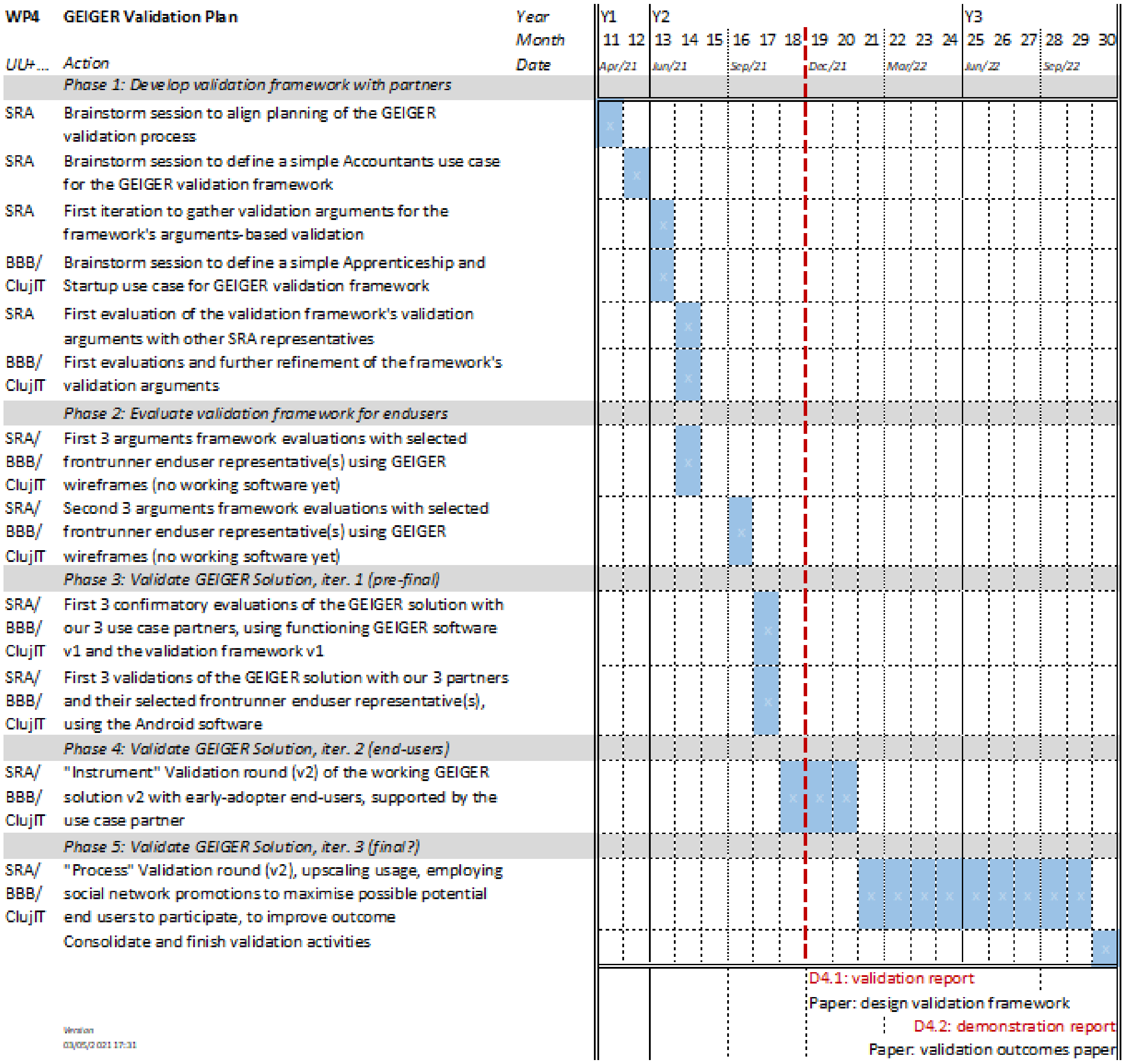


Figure 4: Mapping of GEIGER user-journey to Hopster's Validation Framework

Regarding (b), UU has created a WP4 planning overview which includes specific dates when which stakeholder is expected to perform what tasks to further WP4 progress, as shown below in Figure 5.



WP4	GEIGER Validation Plan	Year	Y1		Y2												Y3					
		Month	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
UU+...	Action	Date	Apr/21		Jun/21			Sep/21			Dec/21			Mar/22			Jun/22			Sep/22		
	Phase 1: Develop validation framework with partners																					
SRA	Brainstorm session to align planning of the GEIGER validation process		x																			
SRA	Brainstorm session to define a simple Accountants use case for the GEIGER validation framework			x																		
SRA	First iteration to gather validation arguments for the framework's arguments-based validation				x																	
BBB/ ClujIT	Brainstorm session to define a simple Apprenticeship and Startup use case for GEIGER validation framework				x																	
SRA	First evaluation of the validation framework's validation arguments with other SRA representatives					x																
BBB/ ClujIT	First evaluations and further refinement of the framework's validation arguments					x																
	Phase 2: Evaluate validation framework for endusers																					
SRA/ BBB/ ClujIT	First 3 arguments framework evaluations with selected frontrunner enduser representative(s) using GEIGER wireframes (no working software yet)					x																
SRA/ BBB/ ClujIT	Second 3 arguments framework evaluations with selected frontrunner enduser representative(s) using GEIGER wireframes (no working software yet)							x														
	Phase 3: Validate GEIGER Solution, iter. 1 (pre-final)																					
SRA/ BBB/ ClujIT	First 3 confirmatory evaluations of the GEIGER solution with our 3 use case partners, using functioning GEIGER software v1 and the validation framework v1								x													
SRA/ BBB/ ClujIT	First 3 validations of the GEIGER solution with our 3 partners and their selected frontrunner enduser representative(s), using the Android software								x													
	Phase 4: Validate GEIGER Solution, iter. 2 (end-users)																					
SRA/ BBB/ ClujIT	"Instrument" Validation round (v2) of the working GEIGER solution v2 with early-adopter end-users, supported by the use case partner									x	x	x										
	Phase 5: Validate GEIGER Solution, iter. 3 (final?)																					
SRA/ BBB/ ClujIT	"Process" Validation round (v2), upscaling usage, employing social network promotions to maximise possible potential end users to participate, to improve outcome												x	x	x	x	x	x	x	x	x	
	Consolidate and finish validation activities																					x

D4.1: validation report
Paper: design validation framework
D4.2: demonstration report
Paper: validation outcomes paper

Version
03/05/2021 17:31

Figure 5: GEIGER Validation Schedule

Figure 5 provides an overview of the GEIGER WP4 Validation activities. This plan for the pilots is an initial view and will be adapted as the project evolves. UU, who leads WP4, will participate in all activities, often in collaboration with pilot partners SRA, BBB or ClujIT. In addition to the steps in this Figure, a few more descriptive details follow.

In phase 1, the organisational alignment is outlined in advance, with SRA as the launching use case partner. A validation walkthrough scenario for one Persona in the Accountancy domain is defined to illustrate the argument-based validation approach during the Y1 review. The framework validation arguments logic for later assessment of the GEIGER solution are created, as this is the core of GEIGER's validation. A validation walkthrough scenario in both Apprenticeship and Start-up domains is defined to illustrate the arguments as running cases. An SRA focus group is evaluated by discussing various use cases in the Accountancy domain, finetuning validation arguments where necessary. Two additional focus groups with BBB and ClujIT are evaluated by discussing various use cases in the Apprenticeship and Start-up domains, resp., finetuning validation arguments where necessary.

In phase 2, two early evaluation rounds are organised to evaluate walkthrough evaluations with intrinsically motivated end-user(s) using the GEIGER mockups to simulate the software to finetune and complement the arguments.

In phase 3, a first round of GEIGER Solution evaluation sanity checks is performed to catch remaining bugs and invalid or incoherent arguments, project internal. Then, a first functional GEIGER Solution evaluation on sanity checks to catch remaining bugs and invalid or incoherent arguments is performed with selected project-external potential end-users.

In phase 4, the GEIGER Solution is deployed for early adopter MSEs. Small-scale, with physically available support from partner to gather validation data and observe user experience (UX) (n = 30).

In phase 5, upscaling is carried out by letting MSEs use the GEIGER Solution independently, without physically available partner support (n > 50). Before the end of the GEIGER project, it will be ensured that results are integrated, consolidated, and secured.

Preparedness of countries/partners

Although it is too early to determine whether all partners are ready-as-should-be, WP4 is confident that with the WP4 planning overview, it is possible communicate early and clearly when calling upon each stakeholder.

Readiness of underlying technology

The GEIGER Solution development is on schedule.

Demonstration of viability and usefulness of our results

According to the GEIGER WP4 Planning overview, from M21 onward, GEIGER will be evaluated in daily practices by non-partner end-users.