

D9.14 E-SKILLS & TRAINING ASSESSMENT TOOLKIT

Lead author: HARRI RUOSLAHTI, LAU

Submission date: 31 January 2022

CONFIDENTIAL



The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830943



Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D9.14 E-SKILLS & TRAINING ASSESSMENT TOOLKIT

Work package	WP9 Dissemination, Exploitation, and Innovation Management
Lead author	Harri Ruoslahti (LAU)
Contributors	Jarmo Heinonen (LAU), Bríd Davis (NUIM), Eveliina Hytönen (LAU), Ilkka Tikanmäki (LAU)
Peer reviewers	Paolo Modica (AON), Jan Derkacz (AGH), Andrzej Dziech (AGH), Ewa Konieczna (VST)
Version	V1.0
Due date	31/01/2022
Submission date	31/01/2022

Dissemination level:

	PU: Public
X	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

Version history

Revision	Date	Editor	Comments
0.1	12/05/2021	Eveliina Hytönen (LAU), Bríd Davis (NUIM), Harri Ruoslahti (LAU), Jarmo Heinonen (LAU)	E-skills & Training Toolkit background and theory
0.2	11/10/2021	Harri Ruoslahti (LAU), Ilkka Tikanmäki (LAU)	E-skills from recruitment advertisements
0.3	11/10/2021	Harri Ruoslahti (LAU), Ilkka Tikanmäki (LAU)	E-skills & Training Toolkit concept
0.4	03/01/2022	Harri Ruoslahti (LAU), Ilkka Tikanmäki (LAU)	E-skills & Training Toolkit v1.0
0.5	20/01/2022	Harri Ruoslahti (LAU)	Final revisions based on internal peer reviews
0.6	27/01/2022	Ewa Konieczna (VST)	Minor adjustments and formatting
1.0	31/01/2022	Matteo Merialdo (RHEA)	Final QA, Document closed

Keywords

E-SKILLS, TRAINING, ASSESSMENT, CYBER SECURITY

Disclaimer

This document contains information which is proprietary to the ECHO consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or parts, except with the prior written consent of the ECHO consortium.

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Personal Data collected, used, and stored to produce the content of the deliverable were processed in compliance to requirements from the General Data Protection Regulation (GDPR), according to ECHO Data Management Plan and ECHO Ethics deliverables.

Executive summary

ECHO project task 9.5 ‘Societal Impact Assessment’ has delivered an E-Skills & Training Toolkit to identify e-skills that are relevant to cybersecurity, and related gaps in training. This deliverable provides an overview of how academic publications investigating approaches on organizational learning (OL), cyber skills gaps and cyber situation awareness have contributed to the development of this e-skills and training gaps assessment tool, and the process to develop the E-Skills & Training Toolkit.

Several academic papers have been and are published under T9.5, and five of these (Table 2) provide an overview of theoretical background that has guided the development of the E-Skills & Training Toolkit.

The E-Skills & Training Toolkit has been developed in steps during 2020 and 2021. The initial background and theory were explored and E-Skills & Training Toolkit concept was formulated to finalize the Toolkit to measure and identify e-skills and related training gaps to enhance the societal impact of cybersecurity.

The Toolkit is aimed for organizations and their managers to help them identify relevant skills gaps. Understanding skills gaps can bring structure and focus so that trainings and recruitment best address the gaps identified. The Toolkit is available as an electronic tool with the help of a qualified ECHO trained facilitator.

Table of contents

Version history	2
Keywords	2
Disclaimer	2
Executive summary	3
Table of contents	4
List of figures	5
List of tables	5
1. INTRODUCTION	6
1.1 PURPOSE AND SCOPE OF THE DOCUMENT	6
1.2 STRUCTURE OF THE DOCUMENT	6
1.3 RELATION TO OTHER WORK IN THE PROJECT	6
1.4 APPLICABLE AND REFERENCE DOCUMENTS	6
1.5 INTELLECTUAL PROPERTY RIGHTS	7
1.6 GLOSSARY OF ACRONYMS	7
2. BACKGROUND	9
2.1 ORGANIZATIONAL LEARNING	9
2.2 GAPS IN CYBERSECURITY RELATED E-SKILLS	9
2.3 TECHNICAL, SITUATION AWARENESS, AND PROBLEM-SOLVING E-SKILLS	10
3. ECHO METHOD	11
3.1 E-SKILLS FROM RECRUITMENT ADVERTISEMENTS	11
4. E-SKILLS AND TRAINING TOOLKIT	12
5. CONCLUSIONS	14

List of figures

Figure 1: Example excerpt of the technical e-skills Data Extraction Table (DET)	11
Figure 2: The E-skills and Training Toolkit concept	12
Figure 3: Screenshot of E-skills and Training Toolkit (phase 1)	13

List of tables

Table 1: Applicable ECHO documents	6
Table 2: Reference documents (relevant academic papers)	7
Table 3: Glossary of acronyms, initialisms, and abbreviations.....	8

1. Introduction

1.1 Purpose and scope of the document

A major purpose of the ECHO project task 9.5 is to deliver an E-Skills & Training Toolkit to identify e-skills relevant to cybersecurity and related training gaps.

Project ECHO has a networked approach through effective and efficient multi-sector collaboration that aims to strengthen proactive cyber security in the European Union. T9.5 developed the D9.13 Societal Impact Assessment Toolkit questionnaire and this D9.14 E-skills and Training Toolkit. This deliverable explains the work done in regards to the methodology behind the E-skills and Training Toolkit that can be used to identify e-skills relevant to cybersecurity and assess related training gaps, and provide the theoretical basis that has been the basis of this toolkit.

1.2 Structure of the document

This document is structured in five sections. Section one details general issues in relation to this ECHO project deliverable and the scope of this document. Section two provides theoretical and practical background that has guided the work of T9.5 to produce this D9.14. Section three describes the steps taken and work done to develop the E-skills and Training Toolkit, section four provides an overview of the use of the Toolkit, and section five is Conclusions.

1.3 Relation to other work in the project

The work in task 9.5 leading to the creation of this toolkit, has been conducted in relation to the work done in WP2 (Multi-sector needs analysis and Cyberskills Framework), WP4 (Transversal technical cybersecurity challenges) and WP8 (Demonstration Cases). A Societal Impact Assessment of the ECHO Assets (WP5, 6 and 7) was conducted as part of the development of the E-skills and Training Toolkit.

1.4 Applicable and reference documents

The following ECHO documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.42	1.42	20/10/2019
[PQP]	D1.3 Project Quality Plan	ECHO_D1.3_v1.4	1.4	23/04/2021

Table 1: Applicable ECHO documents

The following academic documents have been consulted for the generation of this document:

Reference	Authors	Document Title	Publication	Version	Date
[1]	Aaltola, K., Ruoslahti, H. & Heinonen, J.	Cyber Range (CR) capabilities, interactions and features in acquisition of cyber skills by experts – Empirical study	21st European Conference on Cyber Warfare and Security - ECCWS 2022	Accepted to ECCWS 2022	2022
[2]	Ruoslahti H., Coburn, J., Trent, A. & Tikanmäki, I.	Cyber Skills Gaps – a Systematic Literature Review of Academic Literature	Connections: The Quarterly Journal	Accepted for publication	2022
[3]	Ruoslahti, H.	From Classroom to Online Teaching – A Case during COVID19	Information & Security: An International Journal, 285-292	46, no. 3	2020
[4]	Ruoslahti, Harri, and Amir Trent.	Organizational Learning in the Academic Literature – Systematic Literature Review	Information & Security: An International Journal	46, no. 1: 65-78	2020
[5]	Pöyhönen, J., Rajamäki, J., Ruoslahti, H. & Lehto, M.	Cyber Situational Awareness in Critical Infrastructure Protection.	Annals of Disaster Risk Sciences: Special issue on cyber-security of critical infrastructure	Vol 3, No 1	2020

Table 2: Reference documents (relevant academic papers)

1.5 Intellectual Property Rights

Based on the legal framework provided in the ECHO Grant Agreement and the Consortium Agreement, ECHO specific Intellectual Property Rights (IPR) procedures have been established to protect the innovations and knowledge developed within this deliverable. The IPR Registry has been updated to reflect the innovation and knowledge generation developed by this deliverable.

1.6 Glossary of acronyms

Acronym	Description
CR	Cyber-Range
DET	Data Extraction Table
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
EU	European Union

Acronym	Description
GA	Grant Agreement
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
OL	Organizational Learning
WP	Work Package

Table 3: Glossary of acronyms, initialisms, and abbreviations

2. Background

Academic papers have been published and are submitted under T9.5 to provide a theoretical background for the development of the E-skills and Training Toolkit. The following text shows excerpts and an overview of the five most relevant academic papers (listed in Table 2) that have served as background and part of development activities in developing the E-skills and Training Toolkit.

Businesses, organizational communication and learning have become transformed by the Internet. Modern society is technology driven, where people in workplaces interact on cloud based social networking platforms and solutions. Besides many benefits, ICT technologies come with threats. Vulnerabilities in ICT applications and systems may become exploited in ways that require appropriate e-skills from their employees. E.g., in 2020, the Allianz Risk Barometer ranked cyber incidents as the greatest risk that threatens business continuity. Organizations face challenges that require technical, situation awareness and problem-solving related e-skills from a wide level of organizational actors.

2.1 Organizational Learning

The systematic literature review by Ruoslahti & Trent (2020) [4] looks at organizational learning in the academic literature to provide a theoretical basis for the work done in T9.5.

Ruoslahti & Trent (2020) [4] discuss that “organizational learning remains as a continuous process that requires a dedication to innovation and collaborative activities from the entire organization in order to take advantage of organizational learning benefits.” and that a supportive organizational culture and the right ICT tools need to be aligned as organizational culture and to produce the innovative culture, and ICT readiness being the other theme needed to strengthen organizational learning (OL) characteristics. The findings show that more attention should be placed on organizational culture because OL is impacted by the culture of the organization.

Ruoslahti & Trent (2020) [4] “... conclude organisational learning should not only be prioritized in order to build competitive advantage but primarily to instil essential skills, such as e-skills, which has become a requirement for modern organizations to thrive. Companies could further strengthen organisational learning by integrating a systematic learning package on ICT critical for business processes to address any discrepancy of e-skills competence among staff.”

Ruoslahti & Trent (2020) [4] propose that “learning package could be broken down into varying levels of e-skills literacy among personnel. This will provide appropriate training based on their level, in the form of theory trainings, and interactive sessions to further embed the information. Through this approach all personnel across the organization is tended to, which will help nurture employee confidence and contribute to the organisational learning culture.”

2.2 Gaps in Cybersecurity related E-skills

The systematic literature review by Ruoslahti et al. (2022) [2] on cyber skills gaps in academic literature provides understanding on how e-skills are viewed in academic papers discussing cybersecurity. This study shows “a general lack of established IT terms, there are ‘e-skills’, ‘cyber skills’, ‘computer skills’, ‘ICT skills’ and they all can mean different things to different authors”, and recommend further research to identify clearer definitions for these terms.

Ruoslahti et al. (2022) [2] find that “academic literature mostly discusses current cyber security issues, such as cyber threats, cyber related training and qualifications, and training, more work is proposed to define what e-skills, in addition to the very necessary cyber security related skills, are needed to effectively operate in modern society. Four major categories regarding e-skills emerge as results of this study.” and “these categories serve to understand the role of cyber and e-skills in modern society. It becomes apparent that users, be they private citizens, working professionals or ICT / cyber experts are a potential weak link regarding cyber issues. Thus, cyber skills are needed to protect people, organizations and society against disruptive cyber incidents and malicious cyber-attacks.”

Ruoslahti et al. (2022) [2] note that “When users have difficulties in distinguishing between legitimate requests and possible cyber-attacks there is a gap in having relevant cyber security training. Therefore, investing in cyber security awareness programs and cyber training to deal with cyber-threats should be priority for organizations.” The authors also identify a “need to invest in e-skills education and cyber security training in order to develop resilient societal, economical, and industrial systems. To address shortages in the workplace with ICT competence, there could be support from governments, organizations, and academic institutions regarding facilitating courses that develop cyber skills training and education in e-skills to continually cultivate growth and innovation in the European economies through ICT developments.”

2.3 Technical, Situation Awareness, and Problem-solving E-skills

Aaltola, Ruoslahti and Heinonen (2022) [1] conducted an empirical study on cyber range (CR) capabilities, interactions and features in acquisition of cyber skills. The authors find that expert respondents “valued cybersecurity very important or important, but there are several gaps in the organisational capabilities, awareness and employees’ skills to implement cybersecurity issues in everyday life. Preparedness and mitigation towards cybersecurity threats can be seen low, based on this survey responses.”

Aaltola, Ruoslahti and Heinonen (2022) [1] identify three main levels of e-skills as important for developing cybersecurity related capabilities among employees. These relevant e-skills are: A) Technical, B) Situation Awareness, and C) Problem-solving skills.

Pöyhönen et al. (2020) [5] write that the “Observe – Orient – Decide – Act (OODA) loop is examined as a way to promote collaboration towards a shared situational picture, awareness and understanding to meet challenges of forming CSA in relation to risk assessment (RA) and improving resilience.” The authors note that “Situation awareness is the main prerequisite towards cyber security. Without situation awareness, it is impossible to systematically prevent, identify, and protect the system from cyber incidents.”

Ruoslahti (2020) [3] finds on problem-solving that “... continuity requires human interaction and communication, and this calls for regular contacts and all parties having a willingness to collaborate and solve problems together. Thus, one critical element of continuity management that the results show is communication. Open communication was seen as a way to promote resilience, and results also show that it is important to raise awareness toward better collaboration between the many critical infrastructure actors.”

3. ECHO Method

In aiming to provide a gap measurement of e-skills and training related to cybersecurity, ECHO T9.5 has developed the E-skills and Training Toolkit. The Toolkit is based on a prior background research made public in academic papers published in relation to ECHO research activities. The E-skills and Training Toolkit has been developed in steps during 2020 and 2021, involving developing the initial concept that was digitalized as the final E-skills & Training Toolkit v1.0 that can identify relevant e-skills and measure related gap to identify training and recruitment needs that increase organisational cybersecurity.

3.1 E-skills from Recruitment Advertisements

The E-skills and Training Toolkit development has been based on the study of academic literature, and in relation to the work done in other ECHO WPs. An initial concept was first built and then digitalized as the E-skills & Training Toolkit v1.0 that is presented as this ECHO D9.14. European recruitment advertisements were analysed to create long lists of Technical, Situation awareness and Problem-solving skills that can serve as basis for the E-skills and Training Toolkit.

The Toolkit helps its users identify, based on the above mentioned long lists, the Technical, Situation awareness, and Problem-solving related e-skills, which the users feel are most relevant to their organization. The Toolkit then provides a target measure for a selected set of e-skills and self-assessment measures to the same set to show gaps in Technical, Situation awareness, and Problem-solving related e-skills. The gap analysis can be used to identify training and recruitment needs, which contribute to an overall increase organisational cybersecurity.

The division of Technical, Situation awareness, and Problem-solving related e-skills is based on reviews of academic literature and the ECHO CR study by Aaltola, Ruoslahti and Heinonen (2022).

The long lists of Technical, Situation awareness, and Problem-solving related e-skills have been collected by analysis of over 150 European recruitment advertisements (over 50 advertisements from three different markets each: Finland, Ireland and UK). Analysis of 50 recruitment advertisements was a KPI for T9.5 ‘Societal Impact Assessment’. These were analysed by using an Excel based Data Extraction Table (DET), which identifies job, company, technical field and sector, and most importantly, the relevant e-skills under the three categories of Technical, Situation awareness, and Problem-solving related e-skills for each individual recruitment ad. The three categories, Technical, Situation awareness, and Problem-solving, each have their own sheet.

Company	Country	Technical Field	Maritime	Healthcare	Energy	Other	Technical skills
			Strategic/Maal/Spe	gic/Maal/Spe	gic/Maal/Spe	gic/Maal/Specialist	
Visma Pay	Finland	Cybersecurity				x	Experience of cloud services (e.g. AWS, Azure)
Visma Pay	Finland	Cybersecurity				x	Experience of cloud service's information security (e.g. AWS, Azure)
Fastroi	Finland	Cybersecurity				x	Understanding of ITIL practices
Fastroi	Finland	Cybersecurity				x	Experience of Linux technology
Fastroi	Finland	Cybersecurity				x	Experience of AWS technology
Fastroi	Finland	Cybersecurity				x	Understanding of build-in security
Landis+Gyr	Finland	Cybersecurity			x		Develop the existing code base
Landis+Gyr	Finland	Cybersecurity			x		Contribute to system architecture definition

Figure 1: Example excerpt of the technical e-skills Data Extraction Table (DET)

From these long lists of Technical, Situation awareness, and Problem-solving related e-skills, organisational representatives can select the most relevant to the individual positions within their organization and prioritize them by assigning them target values on a five step Likert scale.

4. E-skills and Training Toolkit

The E-skills and Training Toolkit has five operational phases (Figure 2, below). In phase-1, the Toolkit provides its users with predetermined long lists of Technical, Situation awareness, and Problem-solving related e-skills. These long lists are based on prior analysis of European recruitment advertisements. In phase-2, the users select the Technical, Situation awareness, and Problem-solving related e-skills that they see being most important to their organization. Phase-3 provides organizational target values, as each of the selected e-skill is given a target value on a scale of one to five (Likert). The team manager can do this phase either alone or together with the team. Phase-4 constitutes a Self-assessment that is completed when individual task owners and team members rate their own skills against the skills selected in phase-2. Phase-5 provides reports that are given as both numbers (1 to 5) and as RADAR-graphs.

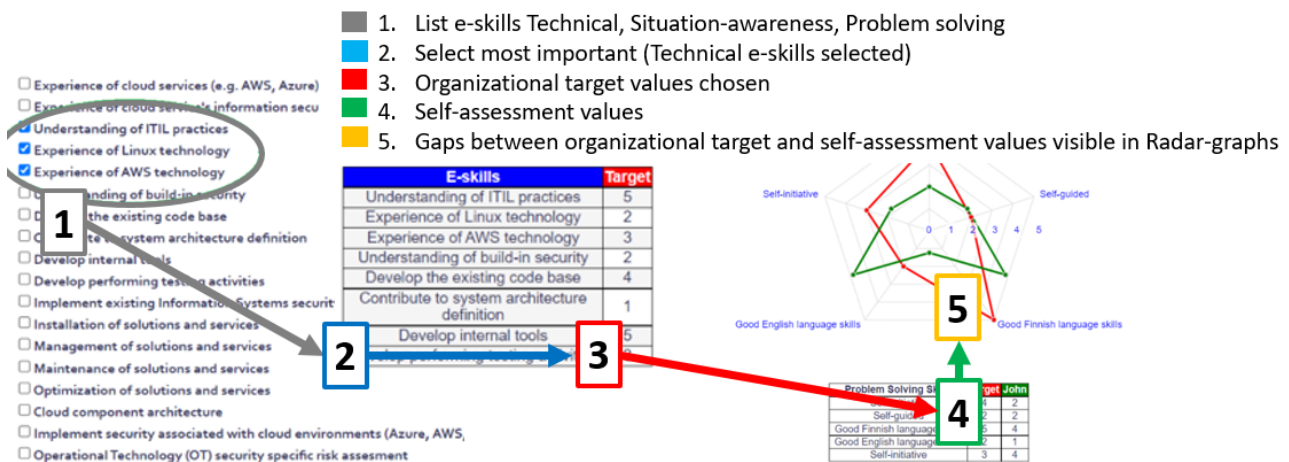
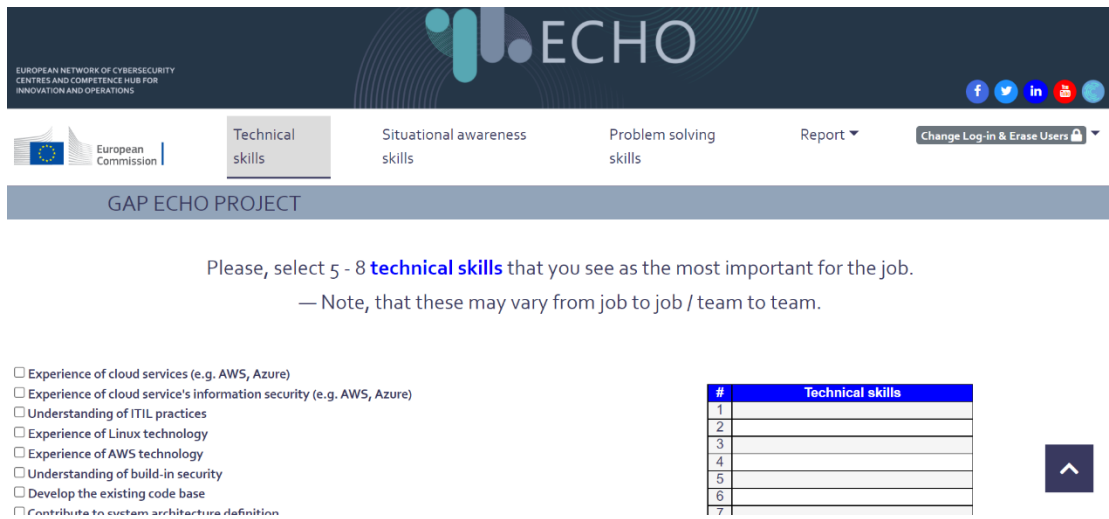


Figure 2: The E-skills and Training Toolkit concept

The gap reports that are provided in phase-5 help organization representatives compare the e-skills organizational target values against relevant self-assessment values that visualize on RADAR-graphs e-skills and training gaps. These gaps can be examined on an individual level as a tool to guide development discussions or prepare job descriptions and recruitment advertisements. On a team level, the Toolkit can provide an understanding of what training content is needed or how new recruits can most effectively help to close the identified e-skills gaps.



EUROPEAN NETWORK OF CYBERSECURITY
CENTRES AND COMPETENCE HUB FOR
INNOVATION AND OPERATIONS

European Commission

Technical skills

Situational awareness skills

Problem solving skills

Report

Change Log-in & Erase Users

GAP ECHO PROJECT

Please, select 5 - 8 **technical skills** that you see as the most important for the job.
— Note, that these may vary from job to job / team to team.

- Experience of cloud services (e.g. AWS, Azure)
- Experience of cloud service's information security (e.g. AWS, Azure)
- Understanding of ITIL practices
- Experience of Linux technology
- Experience of AWS technology
- Understanding of build-in security
- Develop the existing code base
- Contribute to custom architecture definition

#	Technical skills
1	
2	
3	
4	
5	
6	
7	

Figure 3: Screenshot of E-skills and Training Toolkit (phase 1)

This E-skills and Training Toolkit is recommended to be used by ECHO qualified facilitators.

5. Conclusions

One major aim for T9.5 “Societal Impact Assessment” was to deliver an E-skills and Training Toolkit. As the E-skills and Training Toolkit will include private information of individuals’ skills from self-assessments, so to protect this information the Toolkit is intended to be used with the help of qualified ECHO-trained facilitators. This is for the benefit of all organisations that wish to assess their e-skills and training gaps.

This toolkit addresses the cybersecurity related e-skills from three viewpoints: Technical, Situation awareness, and Problem-solving related e-skills. This approach aims to help organizations identify their most relevant e-skills gaps, providing a structured approach to identify and address their training, recruitment and development needs.

The Toolkit provides organizational users a systematic way to identify and prioritize which Technical, Situation awareness, and Problem-solving related e-skills are most important to them. By comparing these organisational target values of e-skills with individual employee self-assessment results, the organization can identify e-skills gaps that they can then address with appropriate trainings for their existing personnel or pinpoint their recruitment according to the identified gaps.

Understanding organizational and individual learning viewpoints, in part contributes to and expands the overall understanding of societal impacts on organizational cybersecurity.

The Toolkit is operational at: <https://echoproject1900413.azurewebsites.net/gap>. The toolkit is intended to be used by and with the aid of an ECHO qualified facilitator. **ECHO qualified facilitators Ilkka Tikanmäki (Ilkka.tikanmaki@laurea.fi) and/or Harri Ruoslahti (harri.ruoslahti@laurea.fi) may be contacted to assist you adopting the use this ECHO E-skills and Training Toolkit to assess the e-skills and training gaps of your team/organization!**