

NOVEMBER 2025

NEWSLETTER °2

GO CLOUD GO SECURE

 Say Hello to Go Cloud! Go Secure!

Dear Reader,

We are happy to see you again! You are reading the 2nd Newsletter of our Go Cloud! Go Secure! project.

There has been so much going on since our last Newsletter! We tested and finalized our CSI Matrix, met in person in Bulgaria in the wonderful city of Sofia and we deep dived into the development of the Go Cloud Training materials.

This issue is full of useful resources and information with the help of which you can further strengthen your cybersecurity level.

Thank you for being with us!

The Go Cloud Team



Co-funded by
the European Union

Highlights

A Message from the Go Cloud! Team
- page 1

Internal and External Testing of CSI Matrix
- page 2

The Matrix is Ready!
- page 3

Transnational Partner Meeting in Sofia - page 4

Projects Supporting Cybersecurity- page 5

Cybersecurity Fun Facts
- page 6



www.gocloudsecure.eu



[@gocloudgosecure](https://www.instagram.com/gocloudgosecure)



[gocloudgosecure](https://www.facebook.com/gocloudgosecure)



[gocloudgosecure](https://www.linkedin.com/company/gocloudgosecure)

INTERNAL AND EXTERNAL TESTING OF THE CSI MATRIX



As part of WP2-A5 “Test, evaluation and refinement of the digital CSI Matrix,” partners carried out real-life testing to check how useful, clear, and user-friendly the Cloud Security Implementation (CSI) Matrix is.

Internal Testing

For the internal testing, partner staff who hadn't been involved in developing the Matrix tried it out, providing fresh and unbiased feedback. Seven people with relevant experience took part, most of whom had previously worked with cloud security tools. They found the suggested vulnerabilities and mitigation actions suitable and appreciated the tool's practical value. Most testers said the Matrix was intuitive and easy to navigate and they especially liked the color-coded risk system. While the interface was generally user-friendly, a few users encountered minor issues like PDF export problems or occasional freezing. The overall feedback was very positive: the Matrix was seen as clear, well-structured and well-aligned with SME needs. All internal testers said they would use and recommend it.

External Testing

External testing also went very well. Every partner exceeded the target of five participants, gathering input from a wide mix of SME staff, IT/cloud security experts, VET trainers and other professionals. The group was split almost evenly between those with and without prior experience using cloud security tools, giving a balanced perspective. Participants found the Matrix clearly structured, relevant and detailed at the right level, although opinions varied by user experience. They confirmed that the vulnerability-mitigation pairings made sense and saw the Matrix as useful for both practical work and training. Over 90% said they would use it professionally, and all participants said they would recommend it to others. Users found the tool intuitive, the color-coded risk logic helpful, and the interface stable and easy to use. Only a few minor technical issues were reported, supporting the Matrix's reliability and strong overall acceptance.

THE MATRIX IS READY!



EXPLORE THE CSI MATRIX AND SECURE YOUR CLOUD ENVIRONMENT!



We're excited to share that the [Cloud Security Implementation Matrix](#), the very first result of the Go Cloud! Go Secure! Erasmus+ project, is now up and running on the [project's website](#).

The primary audience for the CSI Matrix is SMEs that are using or considering using cloud services but may not have own security teams or cloud-security expertise.

The tool is designed to be straightforward, flexible and SME-friendly without too much technical jargon and is a support for organisations that want to responsibly adopt cloud solutions and maintain security at the same time.

All the SMEs have to do is choose the cloud model they rely on and the Matrix reveals, assesses and mitigates the threats that are associated with the cloud model chosen.

The CSI Matrix works in four easy steps:

- 1** Choose which cloud service model you are using or planning to use (e.g. SaaS, PaaS, IaaS).
- 2** Based on your selections, you can check the security risks most relevant to your cloud environment.
- 3** The Matrix rates the level of risk each threat poses to your organisation — this means it prioritises what matters most for your business.
- 4** As a last step, you are presented with clear advice and tips guided by the well-known OWASP Top 10 framework.

At the end of the process, a personalised PDF can be downloaded with all the results and recommendations. Besides English, the tool is available in five more European languages.

16-17 October 2025,

Sofia

TRANSNATIONAL
PARTNER MEETING #2



The "Go Cloud! Go Secure!" project recently held its second international meeting in Sofia, Bulgaria, hosted by Acta Consulting. Partners from Hungary, Italy, Austria, and Cyprus gathered to review progress and plan next steps.

A key outcome of the project, the **Cloud Security Implementation (CSI) Matrix**, a digital self-assessment tool, has been thoroughly tested. During the external pilot, **38 professionals from five countries** provided feedback, with 100% recommending it to others. 81.1% found the risk-assessment logic "very useful," and participants confirmed the tool's stable performance. Internal testing with seven staff members also highlighted the tool's value, with only minor usability suggestions.

In the next phase, Work Package 3 will deliver the CSI implementation model in five steps:

1. Analysis (service inventory, risk map, compliance)
2. Definition (policy, roles, objectives)
3. Planning (measures, training)
4. Implementation (technical steps, awareness)
5. Verification (testing, feedback)

The CSI Model helps SMEs adopt secure cloud systems by guiding them through risk identification, security measures, and ongoing protection. This approach increases digital preparedness, reduces cyber risks, and builds customer trust.

Looking ahead, Work Package 4 will provide educational materials, including a pre-assessment questionnaire, CSI course curriculum, and an online portal. The curriculum will be available later this year, with microlearning videos based on real business examples coming in early 2026.



INTERESTING PROJECTS TO SUPPORT YOUR CYBERSECURITY

Cyber Security Training on Operational Technology Resilience

<https://csector.eu/>

CSeCTOR equips SMEs in manufacturing and other critical infrastructure sectors with OT-cybersecurity capabilities.

It focuses on **identifying vulnerabilities, implementing protective measures and developing incident-response plans** for operational-technology systems.

The project delivers a **tailored methodology, a self-assessment tool and a blended + e-training platform** to boost resilience in sectors like chemicals, plastics, textiles, utilities, oil & gas and transport.



Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

<https://encrypt40.eu/>

Encrypt 4.0 strengthens the capacity of manufacturing SMEs to **protect their data, systems and operations within the Industry 4.0 environment.**

The project **helps companies identify, analyse and address cyber-risks while supporting the development of a more skilled cybersecurity workforce.**

It delivers practical, easy-to-use tools such as the **Cyber Risk Audit Matrix, a hands-on Cybersecurity Training Lab and a collection of real-world cyber-incident case studies with defence strategies.**

Encrypt 4.0 promotes interactive, project-based learning, empowers SME managers to adopt proactive cybersecurity practices and encourages knowledge-sharing to enhance resilience and digital readiness across the industrial ecosystem.



THE FASCINATING WORLD OF CYBERSECURITY

There are cyber pirates!

The term "phishing" (fraudulent attempts to obtain sensitive information) comes from the idea of using a bait (like an email or website) to "hook" victims, much like fishermen use bait to attract fish. You will be able to learn more about phishing in our training material :)

The first virus wasn't a scam.

The first known computer virus was called Creeper, and it was created in the early 1970s as a self-replicating program. It didn't cause damage—it just displayed the message, "I'm the Creeper, catch me if you can!" It was more of a proof-of-concept than a malicious attack.

Passwords are still a major weak spot.

The most common password in the world is still "123456," despite years of warnings about weak passwords. In fact, around 80% of data breaches are caused by weak or stolen passwords.

There are more cyberattacks than you might expect.

The average number of cyberattacks every day is staggering: around 30,000 websites are hacked daily. That's more than 20 websites per minute!

did

you

know

?



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.