

MAY 2026

NEWSLETTER °3

GO CLOUD GO SECURE

Check out our new security contents and tools with Go Cloud! Go Secure!

Dear Reader,

We are happy to see you again! You are reading the 3rd Newsletter of our Go Cloud! Go Secure! project.

We have exciting updates to share: three key project results are now available on our website:

- The CSI Self-Assessment tool allows users to check their own knowledge and identify areas for improvement.
- The CSI Course offers practical, easy-to-follow learning materials on cloud security.
- The CSI Model helps SMEs understand how to use cloud services more securely and what steps they can take to improve.

At the moment, all three resources are available in English, but the translated versions will be ready soon.

This issue brings you useful updates, fresh resources and practical information to help you 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

Cloud Security Journey
- page 2

CSI Self-Assessment tool
- page 3

CSI Course
- page 4

CSI Implementation Model
- page 5

Testers wanted!
- page 6

Multiplier events coming soon!
- page 7

Cybersecurity Fun Facts
- page 8



www.gocloudsecure.eu



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



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



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



Cloud Security Journey

A practical pathway for SMEs and VET providers: assess your current situation, build cloud-security skills, and turn knowledge into action.

How can my organisation improve cloud security step by step?



1 Start with self-assessment

Use the CSI Self-Assessment to reflect on your current cloud-security awareness, everyday practices and decision-making. It helps identify strengths, gaps and priority areas.

2 Identify needs and gaps

Review the results to understand where support is needed most - from cloud basics and shared responsibility to common threats and weak points.



3 Build skills with the course

Learn how to understand cloud risks, recognise common threats, design safer cloud environments and apply effective governance practices.



4 Apply the CSI Model

Use the CSI Model to turn learning into action. Map services, risks and compliance needs, then define priorities, roles, policies and suitable security controls.



5 Improve and grow securely

Monitor progress, refine your practices and keep strengthening resilience. Our tools support ongoing improvement, staff awareness and confident digital transformation.



Success!





CSI SELF-ASSESSMENT TOOL

CLOUD SECURITY CHECK-UP

ANSWER 15 QUESTIONS - GET IMMEDIATE RESULTS



AVAILABLE ONLINE NOW



TEST YOUR CLOUD SECURITY STATUS

How secure is your approach to cloud computing? The **CSI Self-Assessment** helps SMEs, trainers and learners reflect on real-life cloud security situations in a simple and practical way.

The questionnaire covers key topics such as cloud service models, shared responsibility, data protection, ransomware prevention, Zero Trust, access control, governance and incident response.

There are no “scary exam” moments here — only useful questions that help you see what you already know and where you may want to improve.

FROM EVERYDAY RISKS TO BETTER DECISIONS

Cloud security can feel complex, especially for smaller businesses with limited time and resources. The **CSI Self-Assessment** breaks this topic into practical questions that connect directly to everyday business decisions.

It helps users think about password security, multi-factor authentication, backups, data leakage, secure cloud design and clear responsibilities. By going through the questions, SMEs can better understand which areas need more attention and what kind of knowledge can support safer cloud use.

A SIMPLE FIRST STEP TOWARDS STRONGER CLOUD SECURITY

The **CSI Self-Assessment** is not about pressure — it is about awareness. It gives users a quick and useful way to check their understanding, identify learning needs and become more confident in cloud security topics.

For SMEs, trainers and learners, it is a practical starting point for building stronger cybersecurity habits and preparing for safer cloud adoption.

BOOST YOUR CLOUD SECURITY SKILLS

The CSI Course helps SMEs strengthen their cloud security knowledge through practical, easy-to-follow training. It shows how to recognise risks, protect data, improve daily security decisions and use the CSI Model with more confidence.

22
SELF-PACED HOURS

06
PRACTICAL
MODULES

06
LANGUAGES

Yes
CERTIFICATE

WHAT YOU'LL ACHIEVE

Walk out with a security posture you can defend.

Each module ends with a practical artefact – a policy, a configuration, or a decision log – that you keep for your business.

01

Understand the main cloud security risks affecting SMEs and how to recognise weak points before they become serious issues.

02

Apply practical controls for safer cloud use, including access management, data protection, backup planning, and secure configuration.

03

Use the CSI Model to assess your current situation, prioritise improvements, and make clearer security decisions.

04

Build confidence to support staff awareness, training delivery, compliance readiness, and long-term secure digital transformation.

[CLICK HERE >](#)

CSI COURSE

Six modules, designed for busy founders

- **Module 1 – Cloud Security Essentials for SMEs:**
 - Introduces cloud computing, service and deployment models, their benefits and challenges for SMEs, and the fundamental principles of secure cloud adoption and shared responsibility.
- **Module 2 – Threat Landscape & SME-Specific Challenges:**
 - Explores common cybersecurity threats affecting SMEs, including phishing, ransomware, insider threats and shadow IT, together with practical and cost-effective prevention measures.
- **Module 3 – Designing Secure Cloud Environments:**
 - Presents the principles and controls needed to design secure cloud architectures, including identity and access management, encryption, defence in depth, segmentation, monitoring and secure-by-design practices.
- **Module 4 – Cloud Security Governance:**
 - Covers cloud security governance through encryption and key management, data protection, risk assessment, regulatory compliance, privacy by design, business continuity and recognised cybersecurity frameworks.
- **Module 5 – The CSI Model: From Theory to Practice:**
 - Explains how SMEs can apply the Cloud Security Implementation Model to assess risks, define priorities, plan and implement security measures, and verify their effectiveness through continuous monitoring and improvement.
- **Module 6 – Capacity Building for VET Providers:**
 - Supports VET providers in developing SME-oriented cloud security training through tailored learner profiles, practical teaching methods, digital assessment tools and cooperation with industry partners.

Structure of the Course

The CSI Course guides learners through cloud security essentials, threat awareness, secure cloud design, governance, the CSI Model and capacity building. It supports safer decisions, stronger staff awareness, better compliance readiness and more confident digital transformation.

CSI IMPLEMENTATION MODEL

PRACTICAL ROADMAP FOR SAFER CLOUD USE

Cloud services can make SMEs faster, more flexible and more competitive — but only if they are used securely. The CSI Implementation Model helps businesses understand their cloud risks, set clear priorities and take practical steps towards stronger cybersecurity.

CSI Implementation Model

Phase 1: ANALYSE

Phase 2: DEFINE

Phase 3: PLAN

Phase 4: IMPLEMENT

Phase 5: VERIFY

From Risks to Action

The CSI Model starts with a clear analysis of cloud services, possible risks and compliance needs. This helps SMEs see where they are most vulnerable and what should be improved first.

Built for SMEs

The model is designed to be practical and easy to follow. It supports smaller organisations in creating policies, assigning responsibilities and choosing realistic security actions without unnecessary complexity.

Five Phases to Stronger Cloud Security

The CSI Implementation Model guides organisations through five key phases: Analyse, Define, Plan, Implement and Verify. Step by step, it helps businesses move from understanding risks to applying real security measures.

The model also highlights the importance of training, monitoring and feedback. This means cloud security does not stop after implementation — it becomes a continuous process of learning, checking and improving.

[CLICK HERE](#)



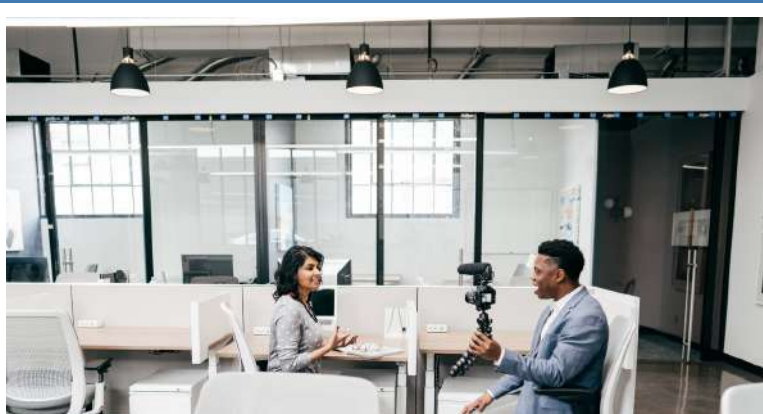
With the CSI Model, SMEs receive a practical framework for making safer decisions, protecting data, improving compliance and building long-term confidence in cloud technologies.

TESTERS WANTED!



GO CLOUD! GO SECURE PROJECT ENTERS ITS TESTING PHASE

The Go Cloud! Go Secure! project has reached another important milestone: the testing of the Cloud Security Implementation Model and the related training programme is now beginning. The purpose of this phase is to assess how useful, clear and relevant the developed tools are for businesses, trainers and cloud security professionals.



EXPERT FEEDBACK FOR PRACTICAL RESULTS

The testing process and the evaluation of the results are expected to be completed by September 2026. Following the final refinements, the Cloud Security Implementation Model and the training programme will be available in all five project languages.

WE WANT YOUR
FEEDBACK!

External Experts Join the Testing

Alongside staff members of the project partners, external experts and representatives of the target groups will also participate. Their feedback will help the consortium refine the model and the training materials so that they respond as closely as possible to the practical needs of small and medium-sized enterprises.

Expected Results by September 2026

Pilot testing completed

Model and course refined

Available in five languages



Contribute to the final versions of the Go Cloud products by sharing your valuable inputs BELOW:
[Link for the testing](#)

MULTIPLIER EVENTS COMING SOON!

September-October 2026 |
Across 5 European Countries

**SEPTEMBER-
OCTOBER
2026**

MULTIPLIER EVENTS IN

**AUSTRIA
HUNGARY
ITALY
BULGARIA
CYPRUS**

What to expect?

- Discover project results and innovative tools
- Learn practical cloud security strategies
- Exchange with experts and local stakeholders
- Get inspired and build valuable connections

Join your local event if you are:

- an SME owner or manager
- an IT professional
- a cybersecurity practitioner
- a consultant
- a trainer
- interested in cloud security

Stay Tuned!

Detailed agendas, dates and registration info will be announced soon on the project's website and social media.

Don't miss the opportunity to be part of a stronger and more secure digital Europe!

THE FASCINATING WORLD OF CYBERSECURITY

Cybersecurity uses honey as a trap!

A “honeypot” is a deliberately tempting fake system designed to attract cyber attackers. While intruders believe they have discovered a valuable target, security experts can quietly observe their methods and learn how to defend real systems more effectively.

Every file has a digital fingerprint!

A cryptographic hash acts like a unique fingerprint for a file. Changing even a single letter can create a completely different fingerprint, making it possible to detect whether data has been secretly modified.

A photograph can carry a secret passenger!

Steganography is the art of hiding information inside an ordinary-looking image, audio recording or video. The file may appear completely normal, while secretly carrying a hidden message or malicious code.

Some computers live on digital islands!

Highly sensitive computers are sometimes “air-gapped”, meaning they are physically disconnected from the internet and other networks. However, even a digital island can be reached through an infected USB drive or another removable device.

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.