

MAI 2026

NEWSLETTER °3

GO CLOUD GO SECURE

**Entdecken Sie unsere neuen Inhalte und Tools
zum Thema Sicherheit mitGo Cloud! Go Secure!**

Liebe Leserinnen und Leser,

wir freuen uns, Sie wiederzusehen! Sie lesen gerade den dritten Newsletter unseres Projekts „Go Cloud! Go Secure!“.

Wir haben spannende Neuigkeiten für Sie: Drei wichtige Projektergebnisse sind nun auf unserer Website verfügbar:

- Mit dem CSI-Selbstbewertungstool können Nutzer ihr eigenes Wissen überprüfen und Verbesserungsmöglichkeiten identifizieren.
- Der CSI-Kurs bietet praktische, leicht verständliche Lernmaterialien zum Thema Cloud-Sicherheit.
- Das CSI-Modell hilft KMU zu verstehen, wie sie Cloud-Dienste sicherer nutzen können und welche Schritte sie zur Verbesserung unternehmen können.

Derzeit sind alle drei Ressourcen auf Englisch verfügbar, die übersetzten Versionen werden jedoch in Kürze bereitstehen.

Diese Ausgabe bietet Ihnen nützliche Neuigkeiten, aktuelle Ressourcen und praktische Informationen, die Ihnen helfen, Ihr Cybersicherheitsniveau zu stärken.

Vielen Dank, dass Sie dabei sind!

Das Go Cloud-Team



Co-funded by
the European Union

Highlights

Ein Nachricht vom Go
Cloud! Team
- Seite 1

Cloud Security Journey
- Seite 2

CSI Self-Assessment tool
- Seite 3

CSI Course
- Seite 4

CSI Implementation
Model
- Seite 5

Tester:innen gesucht!
- Seite 6

Multiplier events coming
soon!
- Seite 7

Cybersecurity Fun Facts
- Seite 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

Ein praktischer Leitfaden für KMU und Anbieter beruflicher Bildung: Bewerten Sie Ihre aktuelle Situation, bauen Sie Kompetenzen im Bereich Cloud-Sicherheit auf und setzen Sie Ihr Wissen in die Praxis um.

Wie kann mein Unternehmen die Cloud-Sicherheit Schritt für Schritt verbessern?



1 Start mit self-assessment

Nutzen Sie das CSI-Self-Assessment Tool (Einschätzung), um Ihre derzeitigen Kenntnisse im Bereich Cloud-Sicherheit, Ihre täglichen Arbeitsabläufe und Ihre Entscheidungsfindung zu reflektieren. Es hilft Ihnen dabei, Stärken, Lücken und vorrangige Bereiche zu identifizieren.

2 Bedarf und Lücken ermitteln

Sehen Sie sich die Ergebnisse an, um zu erkennen, wo Unterstützung am dringendsten benötigt wird – von den Grundlagen der Cloud über die geteilte Verantwortung bis hin zu häufigen Bedrohungen und Schwachstellen.



3 Erwerben Sie neue Fähigkeiten

Erfahren Sie, wie Sie Cloud-Risiken verstehen, häufige Bedrohungen erkennen, sicherere Cloud-Umgebungen gestalten und wirksame Governance-Maßnahmen umsetzen können.



4 Wenden Sie das CSI Modell an

Nutzen Sie das CSI-Modell, um das Gelernte in die Praxis umzusetzen. Erfassen Sie Dienste, Risiken und Compliance-Anforderungen und legen Sie anschließend Prioritäten, Rollen, Richtlinien und geeignete Sicherheitsmaßnahmen fest.



5 Sich verbessern und sicher wachsen

Unsere Tools unterstützen die kontinuierliche Verbesserung, die Sensibilisierung der Mitarbeiter und eine erfolgreiche digitale Transformation.



Success!





CSI SELF-ASSESSMENT TOOL

CLOUD SECURITY CHECK-UP

BEANTWORTEN SIE 15 FRAGEN - ERHALTEN SIE SOFORTIGE ERGEBNISSE

AVAILABLE ONLINE NOW

CLICK HERE >

TESTEN SIE IHREN CLOUD SECURITY STATUS

Wie sicher ist Ihr Ansatz beim Cloud-Computing? Die CSI-Selbsteinschätzung hilft KMU, Ausbildern und Lernenden dabei, sich auf einfache und praktische Weise mit realen Situationen im Bereich der Cloud-Sicherheit auseinanderzusetzen.

Der Fragebogen deckt wichtige Themen wie Cloud-Servicemodelle, geteilte Verantwortung, Datenschutz, Ransomware-Prävention, Zero Trust, Zugriffskontrolle, Governance und Reaktion auf Vorfälle ab. Hier gibt es keine „beängstigenden Prüfungsmomente“ – nur nützliche Fragen, die Ihnen helfen zu erkennen, was Sie bereits wissen und wo Sie sich möglicherweise verbessern möchten.

VON ALLTÄGLICHEN RISIKEN ZU BESSEREN ENTSCHEIDUNGEN

Cloud-Sicherheit kann komplex erscheinen, insbesondere für kleinere Unternehmen mit begrenzten Zeit- und Ressourcenkapazitäten. Die CSI-Selbstbewertung gliedert dieses Thema in praktische Fragen, die einen direkten Bezug zu alltäglichen Geschäftsentscheidungen haben. Sie hilft, sich mit Passwortsicherheit, Multi-Faktor-Authentifizierung, Datensicherungen, Datenlecks, sicherer Cloud-Gestaltung und klaren Zuständigkeiten auseinanderzusetzen. Durch das Durcharbeiten der Fragen können KMU besser verstehen, welche Bereiche mehr Aufmerksamkeit erfordern und welches Wissen zu einer sichereren Cloud-Nutzung beitragen kann.

EIN EINFACHER ERSTER SCHRITT ZU MEHR SICHERHEIT IN DER CLOUD

Bei der CSI-Selbsteinschätzung geht es nicht um Druck – es geht um Bewusstseinsbildung. Sie bietet den Nutzern eine schnelle und nützliche Möglichkeit, ihr Verständnis zu überprüfen, Lernbedarf zu ermitteln und mehr Sicherheit im Umgang mit Themen der Cloud-Sicherheit zu gewinnen. Für KMU, Schulungsleiter und Lernende ist sie ein praktischer Ausgangspunkt, um solidere Cybersicherheitsgewohnheiten zu entwickeln und sich auf eine sicherere Cloud-Einführung vorzubereiten.



VERBESSERN SIE IHRE CLOUD-SECURITY SKILLS

Der CSI-Kurs hilft KMU dabei, ihr Wissen über Cloud-Sicherheit durch praktische, leicht verständliche Schulungen zu vertiefen. Er zeigt, wie man Risiken erkennt, Daten schützt, die täglichen Sicherheitsentscheidungen verbessert und das CSI-Modell sicherer anwendet.

 **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.

CLICK HERE >

CSI COURSE

Sechs Module, speziell für vielbeschäftigte Gründer konzipiert

- **Modul 1 – Grundlagen der Cloud-Sicherheit für KMU:**
 - Bietet eine Einführung in Cloud-Computing, Service- und Bereitstellungsmodelle, deren Vorteile und Herausforderungen für KMU sowie die Grundprinzipien einer sicheren Cloud-Einführung und der geteilten Verantwortung.
- **Modul 2 – Bedrohungslandschaft und KMU-spezifische Herausforderungen:**
 - Behandelt häufige Cybersicherheitsbedrohungen für KMU, darunter Phishing, Ransomware, Insider-Bedrohungen und Schatten-IT, sowie praktische und kosteneffiziente Präventionsmaßnahmen.
- **Modul 3 – Gestaltung sicherer Cloud-Umgebungen:**
 - Stellt die Grundsätze und Kontrollmaßnahmen vor, die für die Gestaltung sicherer Cloud-Architekturen erforderlich sind, darunter Identitäts- und Zugriffsmanagement, Verschlüsselung, mehrschichtige Verteidigung, Segmentierung, Überwachung und „Secure-by-Design“-Praktiken.
- **Modul 4 – Cloud-Sicherheits-Governance:**
 - Behandelt das Thema Cloud-Sicherheits-Governance anhand von Verschlüsselung und Schlüsselverwaltung, Datenschutz, Risikobewertung, Einhaltung gesetzlicher Vorschriften, „Privacy by Design“, Geschäftskontinuität und anerkannten Cybersicherheits-Rahmenwerken.
- **Modul 5 – Das CSI-Modell: Von der Theorie zur Praxis:**
 - Erläutert, wie KMU das Cloud-Sicherheits-Implementierungsmodell anwenden können, um Risiken zu bewerten, Prioritäten festzulegen, Sicherheitsmaßnahmen zu planen und umzusetzen sowie deren Wirksamkeit durch kontinuierliche Überwachung und Verbesserung zu überprüfen.
- **Modul 6 – Kapazitätsaufbau für Berufsbildungsanbieter:**
 - Unterstützt Berufsbildungsanbieter bei der Entwicklung von KMU-orientierten Schulungen zur Cloud-Sicherheit durch maßgeschneiderte Lernendenprofile, praxisorientierte Lehrmethoden, digitale Bewertungsinstrumente und die Zusammenarbeit mit Partnern aus der Industrie.



Struktur des Kurses

Der CSI-Kurs vermittelt den Teilnehmer:innen die Grundlagen der Cloud-Sicherheit, das Bewusstsein für Bedrohungen, die sichere Cloud-Gestaltung, Governance, das CSI-Modell und den Aufbau von Kompetenzen. Er trägt zu sichereren Entscheidungen, einem stärkeren Bewusstsein der Mitarbeiter:innen, einer besseren Compliance-Bereitschaft und einer selbstbewussteren digitalen Transformation bei.

CSI IMPLEMENTATION MODEL

PRAKTISCHER LEITFADEN FÜR EINE SICHERERE CLOUD-NUTZUNG

Cloud-Dienste können KMU schneller, flexibler und wettbewerbsfähiger machen – allerdings nur, wenn sie sicher genutzt werden. Das CSI-Implementierungsmodell hilft Unternehmen dabei, ihre Cloud-Risiken zu verstehen, klare Prioritäten zu setzen und praktische Maßnahmen für eine stärkere Cybersicherheit zu ergreifen.

CSI Implementation Model

Phase 1: ANALYSE

Phase 2: DEFINE

Phase 3: PLAN

Phase 4: IMPLEMENT

Phase 5: VERIFY

Von Risiken zu Handlungen

Das CSI-Modell beginnt mit einer klaren Analyse der Cloud-Dienste, möglicher Risiken und Compliance-Anforderungen. Dies hilft KMU dabei, zu erkennen, wo ihre größten Schwachstellen liegen und was zuerst verbessert werden sollte.

Für KMUs entwickelt

Das Modell ist praxisorientiert und leicht umsetzbar konzipiert. Es unterstützt kleinere Organisationen dabei, Richtlinien zu erstellen, Zuständigkeiten zuzuweisen und realistische Sicherheitsmaßnahmen auszuwählen, ohne dabei unnötige Komplexität zu erzeugen.

Fünf Phasen zur stärkeren Cloud Security

Das CSI-Implementierungsmodell führt Organisationen durch fünf Schlüsselphasen: Analyse, Definition, Planung, Umsetzung und Überprüfung. Schritt für Schritt unterstützt es Unternehmen dabei, vom Verständnis der Risiken zur Umsetzung konkreter Sicherheitsmaßnahmen zu gelangen.

Das Modell unterstreicht zudem die Bedeutung von Schulungen, Überwachung und Feedback. Das bedeutet, dass Cloud-Sicherheit nicht mit der Implementierung endet – sie wird zu einem kontinuierlichen Prozess des Lernens, Überprüfens und Verbesserns.

[CLICK HERE](#)



Mit dem CSI-Modell erhalten KMU einen praktischen Rahmen, um sicherere Entscheidungen zu treffen, Daten zu schützen, die Einhaltung von Vorschriften zu verbessern und langfristiges Vertrauen in Cloud-Technologien aufzubauen.

TESTER:INNEN GESUCHT!



GO CLOUD! GO SECURE PROJEKT TRITT IN DIE TESTPHASE EIN

Das Go Cloud! Go Secure! Projekt hat einen weiteren wichtigen Meilenstein erreicht: Die Erprobung des Cloud-Sicherheits-Implementierungsmodells und des dazugehörigen Schulungsprogramms beginnt nun. Ziel dieser Phase ist es, zu beurteilen, wie nützlich, verständlich und relevant die entwickelten Instrumente für Unternehmen, Schulungsleiter und Cloud-Sicherheitsexperten sind.



EXPERT FEEDBACK FOR PRACTICAL RESULTS

Der Testprozess und die Auswertung der Ergebnisse werden voraussichtlich bis September 2026 abgeschlossen sein.

Nach den abschließenden Feinabstimmungen werden das Cloud-Sicherheits-Implementierungsmodell und das Schulungsprogramm in allen fünf Projektsprachen verfügbar sein.

WE WANT YOUR
FEEDBACK!

Externe Experten beteiligen sich an den Tests

Neben den Mitarbeiter:innen der Projektpartner werden auch externe Expert:innen und Vertreter der Zielgruppen teilnehmen. Ihr Feedback wird dem Konsortium dabei helfen, das Modell und die Schulungsunterlagen so weiterzuentwickeln, dass sie so genau

wie möglich auf die praktischen Bedürfnisse kleiner und mittlerer Unternehmen zugeschnitten sind.

Erwartete Ergebnisse bis September 2026

Pilot testing abgeschlossen

Model und Kurs optimiert

In fünf Sprachen erhältlich



Tragen Sie zur Fertigstellung der Go Cloud-Produkte bei, indem

Sie UNTEN Ihre wertvollen Anregungen mitteilen:

[Link für den Test](#)

MULTIPLIER EVENTS COMING SOON!

September-Oktober 2026 |
In 5 europäischen Ländern

SEPTEMBER-
OKTOBER
2026

MULTIPLIER EVENTS IN

AUSTRIA
HUNGARY
ITALY
BULGARIA
CYPRUS

Was erwartet Sie?

- Entdecken Sie Projektergebnisse und innovative Tools
- Lernen Sie praktische Strategien zur Cloud-Sicherheit kennen
- Tauschen Sie sich mit Expert:innen und lokalen Akteuren aus
- Lassen Sie sich inspirieren und knüpfen Sie wertvolle Kontakte

Nehmen Sie an Ihrer lokalen Veranstaltung teil, wenn Sie:

- Inhaber:in oder Geschäftsführer:in eines KMU
- IT-Fachkraft
- Experte für Cybersicherheit
- Berater:in
- Ausbilder:in
- Interesse an Cloud-Sicherheit haben

Stay Tuned!

Detaillierte Tagesordnungen, Termine und Informationen zur Anmeldung werden in Kürze auf der Website des Projekts und in den sozialen Medien bekannt gegeben.

Verpassen Sie nicht die Gelegenheit, Teil eines stärkeren und sichereren digitalen Europas zu werden!

DIE FASZINIERENDE WELT DER CYBERSICHERHEIT

Die Cybersicherheit nutzt Honig als Köder!

Ein „Honeypot“ ist ein bewusst verlockend gestaltetes Scheinsystem, das dazu dient, Cyberangreifer anzulocken. Während die Angreifer glauben, ein wertvolles Ziel entdeckt zu haben, können Sicherheitsexperten ihre Vorgehensweisen unbemerkt beobachten und daraus lernen, wie sich echte Systeme wirksamer schützen lassen.

Jede Datei hat einen digitalen Fingerabdruck!

Ein kryptografischer Hash fungiert wie ein eindeutiger Fingerabdruck einer Datei. Schon die Änderung eines einzigen Buchstabens kann einen völlig anderen Fingerabdruck erzeugen, wodurch sich feststellen lässt, ob Daten heimlich verändert wurden.

Ein Foto kann einen blinden Passagier enthalten!

Steganografie ist die Kunst, Informationen in einem ganz normal aussehenden Bild, einer Audioaufnahme oder einem Video zu verstecken. Die Datei mag völlig normal erscheinen, enthält jedoch heimlich eine versteckte Botschaft oder bösartigen Code.

Manche Computer leben auf digitalen Inseln!

Besonders sensible Computer sind manchmal „air-gapped“, das heißt, sie sind physisch vom Internet und anderen Netzwerken getrennt. Doch selbst eine digitale Insel kann über einen infizierten USB-Stick oder ein anderes Wechseldatenträger-Gerät angegriffen werden.

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.