

МАЙ 2026

ИНФОРМАЦИОНЕН БЮЛЕТИН №3

GO CLOUD GO SECURE

Представяме Ви готовите ресурси и инструменти за сигурност Go Cloud! Go Secure!

Здравейте,

Радваме се да Ви видим отново!

Представяме Ви информационен бюлетин 3 по проект Go Cloud! Go Secure!

Имаме вълнуващи новини за споделяне: три основни резултата от проекта вече са напълно завършени и достъпни на нашия уебсайт:

- **Инструментът за самооценка** (CSI Cloud Security Self-Assessment) позволява на потребителите да проверят собствените си знания и да определят областите, в които могат да се подобрят.
- **Курсът за прилагане на облачна сигурност** (CSI Course) предлага практични и лесни за следване учебни материали по темата за облачната сигурност.
- **Моделът за прилагане на облачна сигурност** (CSI Model) помага на МСП да разберат как да използват облачните услуги по-сигурно и какви стъпки могат да предприемат, за да се подобрят.

Към момента и трите ресурса са достъпни на английски език, но преведените версии ще бъдат готови скоро.

Настоящият бюлетин Ви поднася полезни новини, свежи ресурси и практическа информация, които ще ви помогнат да повишите нивото си на киберсигурност.

Благодарим Ви, че сте с нас!



Co-funded by
the European Union

Акценти

Съобщение от екипа на Go Cloud! - стр. 1

Пътят към облачна сигурност - стр. 2

Инструмент за самооценка (CSI) - стр. 3

Курс за прилагане на облачна сигурност (CSI) - стр. 4

Модел за прилагане на облачна сигурност (CSI) - стр. 5

Търсим тестери! - стр. 6

Предстоящи събития за разпространение на резултатите - стр. 7

Интересни факти за киберсигурността - стр. 8



www.gocloudsecure.eu



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



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



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



Пътят към облачна сигурност

Как моята организация може да подобри облачната си сигурност стъпка по стъпка?

Практически маршрут за МСП и доставчици на ПОО: оценете текущото си състояние, изградете умения за облачна сигурност и превърнете знанието в действие.

1 Започнете със самооценка

Използвайте инструмента за самооценка (CSI Self-Assessment), за да прецените текущата си осведоменост за облачната сигурност, ежедневните си практики и начина, по който вземате решения. Той помага да определите силните си страни, пропуските и приоритетните области.

2 Идентифицирайте нуждите и пропуските

Прегледайте резултатите, за да разберете къде подкрепата е най-необходима – от основите на облака и споделяната отговорност до често срещаните заплахи и слабите места.

3 Изградете умения с курса

Научете как да разбирате облачните рискове, да разпознавате често срещаните заплахи, да проектирате по-сигурни облачни среди и да прилагате ефективни практики за управление.

4 Приложете Модела CSI

Използвайте Модела CSI, за да превърнете наученото в действие. Картографирайте услугите, рисковете и изискванията за съответствие, след което определете приоритети, роли, политики и подходящи мерки за сигурност.

5 Подобрявайте се сигурно

Наблюдавайте напредъка си, усъвършенствайте практиките и продължавайте да укрепвате устойчивостта си. Нашите инструменти подпомагат постоянното подобрене, осведомеността на служителите и увереното преминаване към дигитална трансформация.

Success!



ИНСТРУМЕНТ ЗА САМООЦЕНКА

CLICK HERE >

**ПРОВЕРКА НА ОБЛАЧНАТА
СИГУРНОСТ
ОТГОВОРЕТЕ НА 15 ВЪПРОСА И
ПОЛУЧЕТЕ НЕЗАБАВНИ РЕЗУЛТАТИ.**

ИНСТРУМЕНТЪТ Е ДОСТЪПЕН ОНЛАЙН



ПРОВЕРЕТЕ СЪСТОЯНИЕТО НА ОБЛАЧНАТА СИ СИГУРНОСТ

Колко сигурен е подходът ви към облачните технологии? Инструментът за самооценка (CSI Self-Assessment) помага на МСП, обучители и обучаеми да осмислят реални ситуации, свързани с облачната сигурност, по достъпен и практичен начин.

Въпросникът обхваща ключови теми като модели на облачни услуги, споделена отговорност, защита на данните, превенция на рансъмуер атаки, Zero Trust, контрол на достъпа, управление и реакция при инциденти.

Тук няма „страшни изпитни“ моменти - само полезни въпроси, които ви помагат да видите какво вече знаете и къде бихте могли да се подобрите.

ОТ ЕЖЕДНЕВНИТЕ РИСКОВЕ КЪМ ПО-ДОБРИ РЕШЕНИЯ

Облачната сигурност може да изглежда сложна, особено за по-малките дружества с ограничено време и ресурси. Инструментът за самооценка (CSI Self-Assessment) предлага достъпност чрез практични въпроси по темата, които са пряко свързани с ежедневиите бизнес решения. Той помага на потребителите да се замислят за сигурността на паролите, многофакторната автентикация, резервните копия, изтичането на данни, сигурния дизайн на облака и ясното разпределение на отговорностите. Преминавайки през въпросите, МСП могат по-добре да разберат кои области се нуждаят от повече внимание и какви знания могат да подпомогнат по-сигурното използване на облака.

ПРАКТИЧНА ПЪРВА СЪПКА КЪМ ПО-СИЛНА ОБЛАЧНА СИГУРНОСТ

Инструментът за самооценка (CSI Self-Assessment) служи основно за осведоменост. Дава на потребителите бърз и полезен начин да проверят разбирането си, да определят нуждите си от обучение и да станат по-уверени по темите за облачната сигурност.

За МСП, обучители и обучаеми той е практична отправна точка за изграждане на по-силни навици за киберсигурност.

РАЗВИЙТЕ УМЕНИЯТА СИ ЗА ОБЛАЧНА СИГУРНОСТ

Курсът за прилагане на облачна сигурност (CSI Course) помага на МСП да укрепят знанията си за облачната сигурност чрез практично и лесно за следване обучение. Той показва как да разпознавате рисковете, да защитавате данни, да подобрявате ежедневните си решения за сигурност и да използвате Модела CSI с повече увереност.

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 КУРС

Шест модула, създадени за заети ръководители

- **Модул 1 – Основи на облачната сигурност за МСП:**
 - Въвежда облачните изчисления, моделите на услуги и внедряване, техните предимства и предизвикателства за МСП, както и основните принципи на сигурното навлизане в облака и споделяната отговорност.
- **Модул 2 – Средата на заплахите и специфичните предизвикателства за МСП:**
 - Разглежда често срещаните киберзаплахи, засягащи МСП, включително фишинг, рансъмуер и др.
- **Модул 3 – Проектиране на сигурни облачни среди:**
 - Представя принципите и мерките, необходими за проектиране на сигурни облачни архитектури, включително управление на идентичността и достъпа, криптиране, защита в дълбочина и др.
- **Модул 4 – Управление на облачната сигурност:**
 - Обхваща управлението на облачната сигурност чрез криптиране и управление на ключове, защита на данните, оценка на риска, регулаторно съответствие, защита на личните данни.
- **Модул 5 – Моделът CSI: от теория към практика:**
 - Обяснява как МСП могат да приложат Модела за прилагане на облачна сигурност, за да оценят рисковете, да определят приоритети, да планират и внедрят мерки за сигурност и да проверят тяхната ефективност чрез непрекъснато наблюдение и подобрение.
- **Модул 6 – Изграждане на капацитет за доставчици на ПОО:**
 - Подпомага доставчиците на ПОО в разработването на обучение по облачна сигурност, ориентирано към МСП, чрез съобразени профили на обучаемите, практически методи на преподаване и инструменти за дигитално оценяване.



Структура на курса

ТКурсът CSI води обучаемите през основите на облачната сигурност, осведомеността за заплахите, сигурния дизайн на облака, управлението, Модела CSI и изграждането на капацитет. Той подпомага по-сигурните решения, по-силната осведоменост на служителите, по-добрата готовност за съответствие и по-уверената дигитална трансформация.

CSI МОДЕЛ ЗА ПРИЛАГАНЕ НА ОБЛАЧНА СИГУРНОСТ

ПРАКТИЧЕСКИ МАРШРУТ ЗА ПО-ЕФЕКТИВНА ОБЛАЧНА СИГУРНОСТ

Облачните услуги могат да направят МСП по-бързи, по-гъвкави и по-конкурентоспособни, но само ако се използват сигурно. Моделът за прилагане на облачна сигурност CSI помага на бизнеса да разбере своите облачни рискове, да зададе ясни приоритети и да предприеме практически стъпки към по-силна киберсигурност.

CSI Implementation Model

Phase 1: ANALYSE

Phase 2: DEFINE

Phase 3: PLAN

Phase 4: IMPLEMENT

Phase 5: VERIFY

От рискове към действие

Моделът CSI започва с ясен анализ на облачните услуги, възможните рискове и нуждите от съответствие. Това помага на МСП да видят къде са най-уязвими и какво трябва да бъде подобро първо.

Създаден за МСП

Моделът е проектиран да бъде практичен и лесен за следване. Той подпомага по-малките организации в изготвянето на политики, разпределянето на отговорности и избора на реалистични мерки за сигурност без излишна сложност.

Пет фази към по-силна облачна сигурност

Моделът CSI води организацията през пет ключови фази: Анализ, Дефиниране, Планиране, Внедряване и Проверка. Стъпка по стъпка той помага на бизнеса да премине от разбирането на рисковете към прилагането на реални мерки за сигурност.

Моделът също така подчертава значението на обучението, наблюдението и обратната връзка. Това означава, че облачната сигурност не спира след внедряването — тя се превръща в непрекъснат процес на учене, проверка и подобрене.

[CLICK HERE](#)



С Модела CSI МСП получават практическа рамка за вземане на по-сигурни решения, защита на данните, подобряване на съответствието и изграждане на дългосрочна увереност в облачните технологии.

ТЪРСИМ ТЕСТЕРИ!



**GO CLOUD!
GO SECURE**

НАВЛИЗА В СВОЯТА ФАЗА НА ТЕСТВАНЕ

Проектът Go Cloud! Go Secure! достигна поредна важна фаза: започва тестването на Модела за прилагане на облачна сигурност и свързаната с него обучителна програма. Целта на тази фаза е да се оцени доколко полезни, ясни и приложими са разработените инструменти за бизнеса, обучителите и специалистите по облачна сигурност.



EXPERT FEEDBACK FOR PRACTICAL RESULTS

Процесът на тестване и оценката на резултатите се очаква да приключат до м. септември 2026г. След финалните подобрения Моделът за прилагане на облачна сигурност и обучителната програма ще бъдат достъпни на всички пет езика на проекта.

**WE WANT YOUR
FEEDBACK!**

Външни експерти се включват в тестването

Наред със служителите на партньорските организации в тестването ще участват и външни експерти - представители на целевите групи. Тяхната обратна връзка ще помогне на консорциума да усъвършенства модела и обучителните материали, така че те да отговарят възможно най-точно на практическите нужди на бизнеса.

Очаквани резултати до м. септември 2026

Приключено пилотно тестване

Усъвършенствани модел и курс

Достъпни на пет езика



Искаме вашата обратна връзка! Допринесете за финалните версии на продуктите на Go Cloud, като споделите Вашето мнение

Линк към анкетата за обратна връзка

ПРЕДСТОЯЩИ СЪБИТИЯ ПО ПРОЕКТА

м. септември - м. октомври 2026г.
В 5 европейски държави

**М. СЕПТЕМВРИ -
М. ОКТОМВРИ
2026Г.**

**СЪБИТИЯ ЗА
РАЗПРОСТРАНЕНИЕ НА
РЕЗУЛТАТИТЕ В:**

- АВСТРИЯ
- УНГАРИЯ
- ИТАЛИЯ
- БЪЛГАРИЯ
- КИПЪР

Какво да очаквате?

- Открийте резултатите от проекта и иновативните инструменти
- Научете практически стратегии за облачна сигурност
- Обменете опит с експерти и местни заинтересовани страни
- Вдъхновете се

Присъединете се към местното събитие, ако сте:

- собственик или управител на МСП
- ИТ специалист
- специалист по киберсигурност
- консултант
- учител
- човек, който се интересува от облачна сигурност

Следете за новини!

Подробности за събитията, дати и информация за регистрация ще бъдат обявени скоро на уебсайта на проекта и в социалните мрежи на всяка от партньорските организации.

Не пропускайте възможността да бъдете част от една по-силна и по-сигурна дигитална Европа!

ИНТЕРЕСНИ ФАКТИ ЗА КИБЕРСИГУРНОСТТА

Киберсигурността използва мед като капан!

„Honeyrot“ (медено гърне) е умишлено примамлива фалшива система, създадена да привлича кибератакуващи. Докато нарушителите смятат, че са открили ценна цел, експертите по сигурност могат незабелязано да наблюдават методите им и да се научат как да защитават реалните системи по-ефективно.

Всеки файл има дигитален отпечатък!

Криптографският хеш действа като уникален пръстов отпечатък на файл. Промяната дори на една буква може да създаде напълно различен отпечатък, което прави възможно да се установи дали данните са били тайно променени.

Една снимка може да носи скрита информация

Стеганографията е изкуството да се скрива информация в обикновено на пръв поглед изображение, аудиозапис или видео. Файлът може да изглежда напълно нормален, а тайно да носи скрито съобщение или зловреден код.

Някои компютри живеят на дигитални острови!

Особено чувствителните компютри понякога са „air-gapped“, което означава, че са физически откъснати от интернет и другите мрежи. Въпреки това дори до един дигитален остров може да се достигне чрез заразено USB устройство или друг преносим носител.

did

you

know

?



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093



**Co-funded by
the European Union**

Съфинансиран от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.