Co-funded by the European Union

GO CLOUD GO SECURE

AUXILIARY IMPLEMENTATION GUIDE

How to apply the Cloud Security Implementation (CSI) Model in your organisation

*Companion to the **"Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs"** (Erasmus+ Project 2024-1-AT01-KA220-VET-000245093). Source materials and interactive tools: gocloudsecure.eu*

1. Purpose of This Guide

The CSI Model is a five-phase framework that helps small and medium-sized enterprises (SMEs) secure their cloud operations, whether they use Software-, Platform- or Infrastructure-as-a-Service. This auxiliary guide is a practical companion to the official CSI Model documentation: it summarises what each phase requires, and walks through one worked example so a company can see the model applied step by step before adapting it to their own cloud environment. Use this guide to understand and follow the overall implementation process. Refer to the detailed Phase 1-5 documents for additional guidance, templates and implementation details.

Use this guide alongside the two other CSI tools:

- CSI Matrix — an interactive tool that maps cloud services to their threats, vulnerabilities and risks, and scores them against the OWASP Top 10; used throughout Phases 1–3. www.gocloudsecure.eu
- CSI Self-Assessment & CSI Course (SecureCloud SME) — reflection questions and training material covering cloud fundamentals, the threat landscape, secure design and governance; used to prepare and deliver the training in Phases 3–4.

> *Tip Keep this guide open alongside the CSI Matrix while working through Phases 1-3. Open the CSI Matrix, follow the instructions provided there, complete the assessment and use the resulting risks and scores in the next phases.*

2. The CSI Model at a Glance

The model runs as a continuous cycle of five phases. Each phase has a clear objective, a short sequence of steps, and a defined output that feeds the next phase.

Phase	Objective	Key steps	Main output
1. Analyse	Understand cloud usage, threat exposure and compliance duties.	Cloud services list • Risk mapping (CSI Matrix) • Compliance check	Cloud service inventory, CSI Matrix baseline, list of applicable regulations.
2. Define	Set governance, prioritise risk	Policy development • Risk	Cloud Security Policy,

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

Phase	Objective	Key steps	Main output
	and define control objectives.	prioritisation • Control objectives • Roles & responsibilities	prioritised risk list, control objectives, governance map.
3. Plan	Turn risks and objectives into a concrete implementation plan.	Mitigation actions • Control mapping • Documentation • Training programme	Mitigation action list, control mapping table, templates/checklists, training plan.
4. Implement	Apply the controls and train staff.	Technical actions • Training & awareness	Implemented controls, completed training, a more secure, policy-compliant environment.
5. Verify	Test effectiveness and continuously improve.	Testing • Monitoring (KPIs) • Feedback (incident registry)	Validated controls, monitoring dashboard, lessons learned, refined policy & training.

3. Step-by-Step Instructions

Complete the phases in sequence, as the outputs of each phase provide the inputs for the next.

Phase 1 — Analyse

Objective: understand your organisation's cloud usage, its exposure to threats and vulnerabilities, and its compliance obligations.

1. Cloud Services List — list every cloud service in use (IaaS, PaaS, SaaS, storage, databases, networking, security services). Note what is critical to the business.
2. Risk Mapping — for each service, use the CSI Matrix to identify threats (e.g. data breaches, DDoS), vulnerabilities (e.g. weak authentication) and resulting risks (e.g. data loss, account hijacking).
3. Compliance — check alignment with EU regulations (GDPR, DORA, NIS2) and any relevant standard you hold or target (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

Output: Cloud service inventory, completed CSI Matrix assessment and list of applicable compliance requirements.

Phase 2 — Define

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

Objective: establish governance rules, clarify risks and define control objectives tailored to your organisation.

1. Policy Development — draft a Cloud Security Policy covering secure use, access and data protection.
2. Risk Prioritisation — score each risk from the CSI Matrix by likelihood and impact to focus effort on what matters most.
3. Define Control Objectives — for each high-priority risk, set a mitigation objective (e.g. risk "weak authentication" → objective "strengthen identity").
4. Roles & Responsibilities — assign functions such as Cloud Administrator, Data Owner, Security Officer and Compliance Manager (roles may be combined in smaller SMEs).

Output: Cloud Security Policy, prioritised risks, defined control objectives and assigned roles.

Phase 3 — Plan

Objective: translate risks and control objectives into a detailed implementation plan with mitigation actions, documentation and training.

1. Mitigation Actions — define a specific, actionable measure for each control objective (e.g. "strengthen identity" → "implement multi-factor authentication").
2. Control Mapping — build a table linking each mitigation action to the cloud service it protects.
3. Documentation — prepare an Implementation Checklist, Incident Response Template and Audit Log Review form.
4. Training Programme — design short, practical modules using the CSI training material, matched to your team's technical reality.

Output: Mitigation action list, control mapping, implementation documentation and training plan.

Phase 4 — Implement

Objective: apply the planned controls across all relevant cloud services and train personnel.

1. Technical Actions — execute the roadmap from Phase 3 (e.g. enable MFA, encryption, IAM policies, RBAC). Start with quick wins using built-in tools such as AWS Config or Azure Security Center.
2. Training & Awareness — deliver the training plan, focused on the CSI Matrix findings and CSI training material.

Output: Implemented controls, completed training and implementation evidence.

Phase 5 — Verify

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

Objective: evaluate the effectiveness of implemented measures and continuously improve.

1. Testing — run simulated attacks, control checks and security assessments.
2. Monitoring — track KPIs such as failed logins, misconfiguration alerts and outdated patches, e.g. via a simple dashboard.
3. Feedback — log incidents in an incident registry (what happened, why, impact, mitigation) and feed lessons back into Phases 1–2.

Output: Verified controls, KPI results, corrective actions and lessons learned for the next CSI cycle.

4. Worked Example

Fictional company: NordicCraft Handicrafts — a 25-employee e-commerce SME selling handmade goods online. This walkthrough shows how NordicCraft applied each phase of the CSI Model; the figures and findings are illustrative.

Phase 1 — Analyse: cloud inventory and risk mapping

Cloud service	Service model	Business use
Shopify	SaaS	Online storefront, order capture, customer PII, payment handoff
Google Workspace	SaaS	Company email, shared drives, calendars
AWS S3	IaaS / Storage	Product photography, nightly backups of order exports
Azure App Service	PaaS	Custom order-management web app (integrates Shopify + warehouse)

CSI Matrix output (excerpt):

Service	Threat	Vulnerability	Risk	Priority
Shopify admin panel	Account takeover / phishing	No MFA on admin accounts	Unauthorised changes, customer data breach	High
AWS S3 bucket	Data exposure	Bucket permissions set to public-read	Leakage of customer images & backup files	High
Azure order-management app	Injection / exploitation of known CVE	Outdated third-party libraries, no WAF	Order & customer data breach, downtime	Medium
Google Workspace	Business email compromise	Weak/reused passwords, no MFA enforcement	Data loss, fraudulent payment requests	Medium

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

Compliance check: customer personal data is processed → GDPR applies. NordicCraft is not directly in scope of DORA or NIS2, but has chosen to align voluntarily with ISO/IEC 27001 good practice.

Phase 2 — Define: policy, priorities, roles

A one-page Cloud Security Policy was drafted covering account access, data classification and backup rules. The two "High" risks above (Shopify admin, S3 bucket) were prioritised for immediate action. Roles were assigned as follows:

- Cloud Administrator — IT Manager (configures and manages all cloud platforms)
- Data Owner — Operations Lead (customer data classification and access rules)
- Security Officer — IT Manager, supported by an external IT partner (monitoring, incidents, policy updates)
- Compliance Manager — Managing Director (GDPR and ISO/IEC 27001 alignment)

Phase 3 — Plan: mitigation actions and control mapping

Risk	Control objective	Mitigation action	Owner
Weak identity on Shopify admin	Strengthen identity	Enforce MFA on all Shopify admin accounts	IT Manager
Public AWS S3 bucket	Enforce least-privilege storage access	Set bucket to private; apply bucket policy + access logging	IT Manager
Outdated Azure app dependencies	Reduce attack surface	Patch libraries; enable Azure WAF and auto-updates	External IT Partner
No MFA on Google Workspace	Strengthen identity	Enforce org-wide MFA; enable login alerts	IT Manager

Supporting documents prepared: Cloud Security Policy, an Implementation Checklist (one row per action above), an Incident Response Template, and an Audit Log Review form. Training plan: two 45-minute sessions — "MFA & password hygiene" and "Spotting phishing & reporting incidents" — built from the CSI training material.

Phase 4 — Implement: technical actions and training

- MFA enforced on all Shopify and Google Workspace admin accounts (quick win, completed in week 1).
- AWS S3 bucket switched to private, bucket policy and access logging enabled.
- Azure App Service dependencies patched and Azure WAF enabled in front of the order-management app.
- Both training sessions delivered to all 25 staff; completion tracked in a shared spreadsheet.

Phase 5 — Verify: testing, monitoring, feedback

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

NordicCraft's external IT partner ran a simulated phishing test and a basic vulnerability scan of the Azure app one month after implementation. A lightweight KPI dashboard was set up in a spreadsheet:

KPI	How it's measured	Alert threshold
Failed login attempts (all platforms)	Weekly export from admin consoles	> 10 per account / week
% of admin accounts with MFA enabled	Monthly review of identity settings	< 100%
Days since last dependency/patch update (Azure app)	Monthly patch log	> 30 days
Open items in incident registry	Continuous	Any item open > 14 days

An incident registry was created to record what happened, why it happened, its impact and the mitigation applied. Verification findings and lessons learned are fed back into the CSI Matrix, policies, controls and training as appropriate and inform the next CSI Model cycle beginning again with Phase 1.

5. Getting Started Checklist

Before your first cycle through the CSI Model, make sure you have:

- Named an owner for the overall roll-out (does not need to be a dedicated security role in a small SME).
- Blocked time to complete the CSI Self-Assessment as a team baseline.
- Access to the CSI Matrix ready for Phase 1's risk mapping step.
- A shared location (drive folder) for the Cloud Security Policy, checklists and incident registry.
- A recurring calendar reminder to re-enter Phase 1 (e.g. every 6–12 months, or after any significant cloud change).

6. Resources

All tools referenced in this guide are available at gocloudsecure.eu:

- **CSI Model** - Full documentation for all five CSI Model phases. Read the CSI Model documentation
- **CSI Matrix** - Interactive tool for identifying and assessing cloud security threats and risks. Open the CSI Matrix
- **CSI Self-Assessment** - Tool for assessing the team's cloud security knowledge. Take the CSI Self-Assessment

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.

- **CSI Course: SecureCloud SME** - Training material for developing practical cloud security knowledge and skills. Access the SecureCloud SME course

This guide is an auxiliary, non-official companion document prepared to support adoption of the CSI Model; it does not replace the official "Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs" publication (Erasmus+ 2024-1-AT01-KA220-VET-000245093), released under CC BY-NC-ND 4.0.

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 OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project Number: 2024-1-AT01-KA220-VET-000245093.