



ERGÄNZENDER LEITFADEN ZUR UMSETZUNG

So setzen Sie das CSI-Modell für Cloud-Sicherheit in Ihrer Organisation ein

Begleitender Leitfaden zum Projekt „Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs“
(Erasmus+ 2024-1-AT01-KA220-VET-000245093).

Schulungsmaterialien und interaktive Tools: gocloudsecure.eu

1. Ziel dieses Leitfadens

Das CSI-Modell umfasst fünf Phasen und hilft kleinen und mittleren Unternehmen (KMU), ihre Cloud-Dienste sicherer zu nutzen – unabhängig davon, ob sie Software (SaaS), Plattformen (PaaS) oder Infrastruktur (IaaS) einsetzen.

Dieser Leitfaden ergänzt die offizielle Dokumentation zum CSI-Modell. Er erläutert die fünf Phasen kompakt und zeigt anhand eines Praxisbeispiels, wie Unternehmen die einzelnen Schritte umsetzen und an ihre Bedürfnisse anpassen können.

Weitere Hinweise, Vorlagen und detaillierte Anleitungen finden Sie in den Unterlagen zu den fünf Phasen des CSI-Modells.

Nutzen Sie diesen Leitfaden zusammen mit den beiden zentralen CSI-Werkzeugen:

- **CSI Matrix:** Ein interaktives Werkzeug, das Bedrohungen, Schwachstellen und Risiken von Cloud-Diensten erfasst und anhand der OWASP Top 10 bewertet. Es kommt in den Phasen 1–3 zum Einsatz.
- **CSI-Umsetzungsmodell & CSI-Kurs:** Selbsteinschätzung und Lernmaterialien zu Cloud-Grundlagen, Cyberbedrohungen, sicherer Gestaltung und Governance. Sie unterstützen die Vorbereitung und Durchführung der Schulungen in den Phasen 3–4.

Tipp: Lassen Sie diesen Leitfaden und die CSI Matrix während der Phasen 1–3 geöffnet. Folgen Sie den Anweisungen, führen Sie die Bewertung durch und nutzen Sie die Ergebnisse in den nächsten Phasen.

2. Das CSI-Modell im Überblick

Das CSI-Modell ist als fortlaufender Zyklus mit fünf Phasen aufgebaut. Jede Phase hat ein klares Ziel, zentrale Arbeitsschritte und Ergebnisse, auf denen die nächste Phase aufbaut.

Phase	Ziel	Wichtige Schritte	Ergebnisse
1. Analysieren	Cloud-Nutzung, Bedrohungen und Compliance-Pflichten verstehen.	Cloud-Dienste erfassen · Risiken mit der CSI Matrix bewerten · Compliance prüfen	Dienstverzeichnis, erste CSI-Matrix-Bewertung, geltende Vorschriften.
2. Definieren	Sicherheitsregeln und Schutzziele festlegen, Risiken priorisieren.	Sicherheitsrichtlinie · Risikoprioritäten · Schutzziele · Zuständigkeiten	Cloud-Sicherheitsrichtlinie, priorisierte Risiken, Schutzziele und Rollen.
3. Planen	Risiken und Ziele in einen konkreten Maßnahmenplan übertragen.	Risikominderung · Maßnahmen zuordnen · Dokumentation · Schulung	Maßnahmenplan, Zuordnungstabelle, Vorlagen, Checklisten und Schulungsplan.
4. Umsetzen	Schutzmaßnahmen umsetzen und Mitarbeitende schulen.	Technische Maßnahmen · Schulung und Sensibilisierung	Umgesetzte Maßnahmen, Schulungen und ein sichereres, richtlinienkonformes Umfeld.
5. Überprüfen	Wirksamkeit prüfen und laufend verbessern.	Tests · KPI-Überwachung · Vorfallregister und Rückmeldungen	Geprüfte Maßnahmen, Dashboard, Erkenntnisse und verbesserte Richtlinien und Schulungen.

3. Schritt-für-Schritt-Anleitung

Durchlaufen Sie die fünf Phasen nacheinander. Die Ergebnisse einer Phase bilden jeweils die Grundlage für die nächste.

Phase 1 – Analysieren

Ziel: Ermitteln, welche Cloud-Dienste Ihr Unternehmen nutzt, welchen Bedrohungen und Schwachstellen es ausgesetzt ist und welche Compliance-Anforderungen gelten.

- **Cloud-Dienste erfassen:** Listen Sie alle genutzten Dienste auf (IaaS, PaaS, SaaS, Speicher, Datenbanken, Netzwerke und Sicherheitsdienste). Kennzeichnen Sie geschäftskritische Dienste.
- **Risiken bewerten:** Ermitteln Sie mit der CSI Matrix für jeden Dienst die Bedrohungen (z. B. Datenlecks, DDoS-Angriffe), Schwachstellen (z. B. unzureichende Authentifizierung) und möglichen Folgen (z. B. Datenverlust, Kontoübernahme).
- **Compliance prüfen:** Prüfen Sie die einschlägigen EU-Vorschriften (DSGVO, DORA, NIS2) sowie Standards, die Sie bereits anwenden oder anstreben (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen der Autorin oder des Autors bzw. der Autorinnen oder Autoren und spiegeln nicht zwingend die der Europäischen Union oder der OeAD-GmbH wider. Weder die Europäische Union noch die OeAD-GmbH können dafür verantwortlich gemacht werden.

Projektnummer: 2024-1-AT01-KA220-VET-000245093.



Ergebnis: Verzeichnis der Cloud-Dienste, abgeschlossene Bewertung mit der CSI Matrix und Übersicht der geltenden Compliance-Anforderungen.

Phase 2 – Definieren

Ziel: Sicherheitsregeln festlegen, Risiken priorisieren und passende Schutzziele für Ihr Unternehmen definieren.

- **Sicherheitsrichtlinie:** Erarbeiten Sie eine Cloud-Sicherheitsrichtlinie zur sicheren Nutzung von Diensten, zur Zugriffsverwaltung und zum Datenschutz.
- **Risiken priorisieren:** Bewerten Sie jedes Risiko aus der CSI Matrix nach Eintrittswahrscheinlichkeit und Auswirkungen. Konzentrieren Sie sich auf die wichtigsten Risiken.
- **Schutzziele festlegen:** Definieren Sie für jedes vorrangige Risiko ein klares Ziel. Beispiel: Aus „unzureichender Authentifizierung“ wird das Ziel „Kontosicherheit stärken“.
- **Rollen und Zuständigkeiten:** Legen Sie fest, wer für Cloud-Betrieb, Daten, Sicherheit und Compliance verantwortlich ist. In kleinen Unternehmen kann eine Person mehrere Rollen übernehmen.

Ergebnis: Cloud-Sicherheitsrichtlinie, priorisierte Risiken, definierte Schutzziele und klar verteilte Zuständigkeiten.

Phase 3 – Planen

Ziel: Risiken und Schutzziele in einen konkreten Umsetzungsplan mit technischen Maßnahmen, Dokumentation und Schulungen übertragen.

- **Risikomindernde Maßnahmen:** Legen Sie für jedes Schutzziel eine konkrete Maßnahme fest. Beispiel: Für „Kontosicherheit stärken“ führen Sie die Multi-Faktor-Authentifizierung (MFA) ein.
- **Maßnahmen zuordnen:** Erstellen Sie eine Tabelle, aus der hervorgeht, welche Cloud-Dienste durch welche Maßnahme geschützt werden.
- **Dokumentation:** Bereiten Sie eine Umsetzungscheckliste, eine Vorlage zur Reaktion auf Sicherheitsvorfälle und ein Formular zur Prüfung von Audit-Protokollen vor.
- **Schulungsprogramm:** Planen Sie kurze, praxisnahe Lerneinheiten auf Basis des CSI-Materials, abgestimmt auf die Kenntnisse und Bedürfnisse Ihres Teams.

Ergebnis: Maßnahmenliste, Zuordnungstabelle, Umsetzungsdokumente und Schulungsplan.

Phase 4 – Umsetzen

Ziel: Die geplanten Schutzmaßnahmen für alle betroffenen Cloud-Dienste umsetzen und Mitarbeitende schulen.

- **Technische Maßnahmen:** Setzen Sie den Plan aus Phase 3 um, etwa MFA, Verschlüsselung sowie Richtlinien zur Identitäts- und Zugriffsverwaltung (IAM, RBAC). Beginnen Sie mit einfach umsetzbaren Verbesserungen und nutzen Sie integrierte Tools wie AWS Config oder Azure Security Center.
- **Schulung und Sensibilisierung:** Führen Sie die Schulungen durch. Nutzen Sie die Erkenntnisse aus der CSI Matrix und die CSI-Lernmaterialien als Grundlage.

Ergebnis: Umgesetzte Schutzmaßnahmen, geschulte Mitarbeitende und Nachweise über die Umsetzung.

Phase 5 – Überprüfen

Ziel: Die Wirksamkeit der Sicherheitsmaßnahmen prüfen und den Schutz des Unternehmens laufend verbessern.

- **Tests:** Führen Sie simulierte Angriffe, Kontrollprüfungen und Sicherheitsbewertungen durch.
- **Überwachung:** Verfolgen Sie Kennzahlen (KPIs) wie fehlgeschlagene Anmeldungen, Warnungen zu Fehlkonfigurationen und ausstehende Sicherheitsupdates, beispielsweise in einem einfachen Dashboard.
- **Rückmeldungen nutzen:** Dokumentieren Sie Sicherheitsvorfälle mit Ursache, Auswirkungen und Gegenmaßnahmen. Nutzen Sie die gewonnenen Erkenntnisse zur Verbesserung der Phasen 1 und 2.

Ergebnis: Geprüfte Schutzmaßnahmen, KPI-Ergebnisse, Korrekturmaßnahmen und Erkenntnisse für den nächsten CSI-Zyklus.

4. Praxisbeispiel

Fiktives Unternehmen: NordicCraft Handicrafts

NordicCraft ist ein E-Commerce-Unternehmen mit 25 Beschäftigten, das handgefertigte Produkte online verkauft.

Das Beispiel zeigt die Anwendung aller fünf Phasen des CSI-Modells. Zahlen und Ergebnisse dienen nur der Veranschaulichung.

Phase 1 – Analysieren: Cloud-Dienste erfassen und Risiken bewerten

Cloud-Dienst	Dienstmodell	Nutzung im Unternehmen
Shopify	SaaS	Onlineshop, Bestellungen, personenbezogene Kundendaten und Zahlungsweiterleitung.
Google Workspace	SaaS	Firmen-E-Mail, gemeinsame Dateien und Kalender.
AWS S3	IaaS / Speicher	Produktfotos und tägliche Backups der Bestelldaten.
Azure App Service	PaaS	Eigene Webanwendung zur Bestellverwaltung, die Shopify mit dem Lager verbindet.

Ergebnisse der CSI Matrix (Auszug):

Dienst	Bedrohung	Schwachstelle	Risiko	Priorität
Shopify-Adminbereich	Kontoübernahme / Phishing	Keine MFA für Administratorkonten.	Unbefugte Änderungen und Abfluss von Kundendaten.	Hoch
AWS S3	Offenlegung von Daten	S3-Bucket erlaubt öffentlichen Lesezugriff.	Abfluss von Kundenbildern und Sicherungsdateien.	Hoch
Azure-Bestell-App	Code-Injection / Ausnutzung bekannter Schwachstellen (CVE)	Veraltete Bibliotheken, keine WAF.	Datenabfluss und Ausfall der Anwendung.	Mittel

Dienst	Bedrohung	Schwachstelle	Risiko	Priorität
Google Workspace	Kompromittierung von Firmen-E-Mails	Schwache oder wiederverwendete Passwörter, MFA nicht verpflichtend.	Datenverlust und gefälschte Zahlungsaufforderungen.	Mittel

Compliance-Prüfung:

NordicCraft verarbeitet personenbezogene Kundendaten. Daher gilt die DSGVO.

DORA und NIS2 sind auf das Unternehmen nicht unmittelbar anwendbar. NordicCraft orientiert sich jedoch freiwillig an bewährten Verfahren nach ISO/IEC 27001.

Phase 2 – Definieren: Richtlinie, Prioritäten und Rollen

NordicCraft erstellte eine einseitige Cloud-Sicherheitsrichtlinie zu Kontozugriffen, Datenklassifizierung und Backups.

Die beiden Risiken mit hoher Priorität – Shopify-Administratorkonten und öffentlich zugänglicher AWS-S3-Speicher – sollten sofort behoben werden.

Die Verantwortlichkeiten wurden wie folgt verteilt:

- **Cloud-Administrator:** IT-Leiter – konfiguriert und verwaltet alle Cloud-Plattformen.
- **Datenverantwortlicher:** Betriebsleiter – legt die Klassifizierung der Kundendaten und die Zugriffsregeln fest.
- **Sicherheitsbeauftragter:** IT-Leiter mit Unterstützung eines externen IT-Partners – überwacht die Sicherheit, bearbeitet Vorfälle und aktualisiert die Richtlinie.
- **Compliance-Verantwortlicher:** Geschäftsführer – sorgt für die Einhaltung der DSGVO und die Orientierung an ISO/IEC 27001.

Phase 3 – Planen: Maßnahmen zur Risikominderung

Risiko	Schutzziel	Gegenmaßnahme	Verantwortlich
Schwache Absicherung von Shopify-Adminkonten	Kontosicherheit stärken	MFA für alle Shopify-Administratorkonten verpflichtend aktivieren.	IT-Leiter
Öffentliches AWS-S3-Bucket	Zugriff auf notwendige Rechte beschränken	Bucket auf privat setzen, Zugriffsrichtlinie und Protokollierung aktivieren.	IT-Leiter
Veraltete Azure-App-Bibliotheken	Angriffsfläche verringern	Bibliotheken aktualisieren, Azure WAF und Auto-Updates aktivieren.	Externer IT-Partner
Keine MFA in Google Workspace	Kontosicherheit stärken	MFA für das gesamte Unternehmen und Anmeldewarnungen aktivieren.	IT-Leiter

Erstellte Unterlagen:

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen der Autorin oder des Autors bzw. der Autorinnen oder Autoren und spiegeln nicht zwingend die der Europäischen Union oder der OeAD-GmbH wider. Weder die Europäische Union noch die OeAD-GmbH können dafür verantwortlich gemacht werden.

Projektnummer: 2024-1-AT01-KA220-VET-000245093.

- Cloud-Sicherheitsrichtlinie.
- Umsetzungskheckliste mit einem Eintrag pro Maßnahme.
- Vorlage zur Reaktion auf Sicherheitsvorfälle.
- Formular zur Prüfung von Audit-Protokollen (Audit Logs).

Schulungsprogramm:

Auf Basis der CSI-Lernmaterialien wurden zwei 45-minütige Schulungen geplant:

- „MFA und sicherer Umgang mit Passwörtern“
- „Phishing erkennen und Sicherheitsvorfälle melden“

Phase 4 – Umsetzen: Technische Maßnahmen und Schulung

NordicCraft setzte folgende Maßnahmen um:

- Für alle Administratorkonten von Shopify und Google Workspace wurde MFA verpflichtend aktiviert. Diese schnelle Verbesserung war in der ersten Woche abgeschlossen.
- Der AWS-S3-Speicher wurde auf privat umgestellt. Zugriffsrichtlinien und Zugriffsprotokollierung wurden aktiviert.
- Die Bibliotheken der Azure-App wurden aktualisiert und Azure WAF zum Schutz der Bestellverwaltungsanwendung aktiviert.
- Beide Schulungen wurden für alle 25 Mitarbeitenden durchgeführt. Die Teilnahme wurde in einer gemeinsamen Tabelle erfasst.

Phase 5 – Überprüfen: Tests, Überwachung und Rückmeldungen

Einen Monat nach der Umsetzung führte der externe IT-Partner einen simulierten Phishing-Test und einen einfachen Schwachstellenscan der Azure-Anwendung durch.

Außerdem wurde in einer Tabelle ein übersichtliches KPI-Dashboard eingerichtet.

Kennzahl (KPI)	Messung	Warnschwelle
Fehlgeschlagene Anmeldungen (alle Plattformen)	Wöchentlicher Export aus den Admin-Konsolen.	Über 10 Versuche pro Konto und Woche.
Anteil der Administratorkonten mit MFA	Monatliche Prüfung der Kontoeinstellungen.	Unter 100 %.
Tage seit dem letzten Bibliotheks- oder Sicherheitsupdate (Azure-App)	Monatliches Update-Protokoll.	Über 30 Tage.
Offene Sicherheitsvorfälle	Laufende Überwachung.	Ein Vorfall ist länger als 14 Tage offen.

Ein Vorfallregister dokumentiert nun Ereignisse, Ursachen, Auswirkungen und getroffene Gegenmaßnahmen.

Die Ergebnisse der Kontrollen fließen in die Aktualisierung der CSI Matrix, der Richtlinien, der Schutzmaßnahmen und der Schulungen ein.

So kann NordicCraft einen neuen CSI-Zyklus mit Phase 1 beginnen und die Sicherheit kontinuierlich verbessern.

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen der Autorin oder des Autors bzw. der Autorinnen oder Autoren und spiegeln nicht zwingend die der Europäischen Union oder der OeAD-GmbH wider. Weder die Europäische Union noch die OeAD-GmbH können dafür verantwortlich gemacht werden.
Projektnummer: 2024-1-AT01-KA220-VET-000245093.



5. Checkliste für den Einstieg

Bevor Sie das CSI-Modell zum ersten Mal anwenden, sollten Sie Folgendes vorbereiten:

- Eine Person bestimmen, die die gesamte Umsetzung koordiniert. In einem kleinen Unternehmen ist dafür keine eigene Sicherheitsstelle nötig.
- Zeit für die gemeinsame CSI-Selbsteinschätzung einplanen, um den Wissensstand des Teams zu erfassen.
- Den Zugang zur CSI Matrix für die Risikobewertung in Phase 1 sicherstellen.
- Einen gemeinsamen Ordner für Cloud-Sicherheitsrichtlinie, Checklisten und Vorfallregister anlegen.
- Eine regelmäßige Erinnerung für Phase 1 einrichten, z. B. alle 6–12 Monate oder nach größeren Änderungen an Cloud-Diensten.

6. Weiterführende Ressourcen

Alle in diesem Leitfaden genannten Tools finden Sie auf gocloudsecure.eu.

- [CSI-Umsetzungsmodell](#): Vollständige Dokumentation aller fünf Phasen des CSI-Modells.
- [CSI Matrix](#): Interaktives Werkzeug zur Erkennung und Bewertung von Cloud-Sicherheitsbedrohungen und -risiken.
- [CSI-Selbsteinschätzung](#): Werkzeug zur Einschätzung des Cloud-Sicherheitswissens Ihres Teams.
- [CSI-Kurs](#): Lernmaterialien für praxisbezogene Kenntnisse und Fähigkeiten zur Cloud-Sicherheit.

Hinweis zum Leitfaden

Dieser Leitfaden ist ein inoffizielles ergänzendes Dokument, das die Anwendung des CSI-Modells erleichtern soll.

Er ersetzt nicht die offizielle Publikation „Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs“ (Erasmus+ 2024-1-AT01-KA220-VET-000245093), die unter CC BY-NC-ND 4.0 veröffentlicht wurde.