

VISCHER CCRA-FI Light: Die effiziente IT/Cloud-Compliance-Prüfung.

Mit diesem Werkzeug prüft das Business einfache IT- und Cloud-Projekte zunächst einmal selbst – und entlastet so sich und die 2nd Line.

- CCRA-FI Light ist ein **automatisierter Fragebogen**, der die für eine Compliance-Prüfung von IT- und Cloud-Projekten von Schweizer Finanzinstituten erforderlichen Fragen stellt und die Antwort **sogleich bewertet**.
- Wird typischerweise vom Business selbst ausgefüllt und eignet sich für weniger riskante Vorhaben. Für grössere Cloud-Projekte empfehlen wir unser Tool **CCRA-FI zur Prüfung und Dokumentation der Compliance und Risiken**; es bildete die Grundlage für die Entwicklung der "Light"-Version, mit welcher Vorhaben mit viel weniger Aufwand und einfacher beurteilt werden können.
- Zu Beginn werden Fragen gestellt, um die **Prüfbereiche** und das **Risiko** zu ermitteln (z.B. ob das Outsourcing-RS gilt oder das Berufsgeheimnis betroffen ist).
- Die **Lizenzierung** des Werkzeugs erfolgt über eine Jahrespauschale oder pro Projekt. Vergünstigungen gibt es für jene, die bereits das CCRA-FI lizenziert haben.
- Die **Vertragsteil** kann auch durch VISCHER ausgefüllt werden (teilautomatisiert KI-gestützt, kostengünstig).
- Basierend auf unserer Erfahrung aus Dutzenden von Projekten, entwickelt mit einer grossen **Kantonalbank**.

Abgedeckt ist:

- Projektbeschreibung
- Vertragsprüfung, inklusive ADV, Bankkundengeheimnis, OpRisk-RS und Outsourcing-RS der FINMA
- Dokumentation der Informationssicherheit
- Dokumentation der Geschäftsfortführung
- Fragen zum Datenschutz inklusive Datenschutz-Folgenabschätzung (DSFA)
- Risikobeurteilung
- Fragen zur Governance



Demo-Video: vischerlnk.com/ccra-fi-light-demo

(unter Verwendung der "Methode Rosenthal" - siehe separates Arbeitsblatt "FLARA")

teilt (1 Fall in der Periode = 100%)	4.38%
Lawful Access durch die ischen Nachrichtendienst ohne	6.48%
achtungperiode:	0.88%
	Sehr tief
tal zu einem Lawful Access kommt:	1300
tal zu einem Lawful Access kommt:	391

"Methode Rosenthal" in fünf Minuten (auch als separates Tool erhältlich)

Status Empfehlung	Begründung	Wer
Empfehlung/Bemerkung	Hierfür wird ein spezielles Amendement angeboten. Das sollte verlangt werden.	PR
Empfehlung/Bemerkung	Hierfür wird ein spezielles Amendement angeboten. Das sollte verlangt werden.	PR
Keine Bemerkungen		PR
Informationen fehlen	Welche Bankkundendaten werden von der Lösung in der Cloud gespeichert?	PR
Keine Bemerkungen		PR

2nd Line prüft Beurteilung der 1st Line

Regelungen zum Berufsgeheimnis im Vertrag (inkl. CID, Sachdaten, juristische Personen)	Regelung	Quelle und Details	Beurteilung	Unser Exposure	Restrisiko
3.30 Es besteht eine echte Verpflichtung, die dem Berufsgeheimnis unterliegenden Daten des Instituts geheim zu halten und diese Pflicht auf alle einbezogenen Mitarbeitenden und Dritte mit Datenzugang zu überbinden:	3 - Ja, der Vertrag sieht eine Pflicht zur Geheimhaltung der Daten vor, nicht nur Personendaten, aber sie wird nicht an Mitarbeitende und Dritte mit Datenzugang überbunden	Ziff. 4.2	Das genügt nicht; es braucht eine Pflicht zur Geheimhaltung für alle Personen.	Hoch	12
3.31 Die Geheimhaltungsverpflichtung gilt so lange über das Vertragsende hinaus, wie es das Berufsgeheimnis verlangt:	4 - Nein, sie gilt nur für eine nach Jahren definierte Zeit nach Vertragsende	Ziff. 4.2	Das genügt nicht, da die Geheimhaltungspflicht länger dauert.	Sehr hoch	16
3.32 Der Anbieter ist verpflichtet, gegen Zugriffe durch ausländische Behörden den Rechtsweg gegen diese auszuschöpfen, auch wenn er das Institut nicht informieren darf ("Defend-your-Data"-Klausel):	1 - Ja, das ist er	Ziff. 4.3	i.O.	N/A	
3.33 Die Bestimmungen des AVV gelten nicht nur für Personendaten, sondern für alle Daten, die unter das Berufsgeheimnis fallen:	3 - Der AVV gilt nur für Personendaten	Ziff. 5.1	Eine solche Regelung ist nicht zwingend, aber von Vorteil.	Mittel	4

Die 1st Line beantwortet die relevanten Fragen (i.d.R. Multiple Choice) und sieht sogleich das Resultat