HodeiShield · Bewertung von Plattformen für Drittparteirisiken

Checkliste zur Bewertung von TPRM-Plattformen nach Branche

Haken Sie jeden Punkt in der Demo mit Ihren eigenen Lieferanten ab und notieren Sie, was das Werkzeug nicht leistet.

Kriterien, die für jede Branche gelten

- [ ] Ein Inventar der Dritten mit internem Verantwortlichen, Kritikalität, Vertragsdaten und Subunternehmern.
- [ ] Nachweise mit Verantwortlichem, Gültigkeitsdatum und Status, wobei abgelaufene Nachweise nicht mehr zählen.
- [ ] Wie Lieferanteninformationen gewonnen werden: Fragebogen, Dokumente, externer Scan, SBOM. Jeder Weg misst etwas anderes.
- [ ] Wie Bewertung oder Risiko berechnet werden: sichtbare Eingaben, dokumentierte Methode und als Schätzung gekennzeichnete Werte.
- [ ] Änderungsprotokoll, Export Ihrer Daten und eine API, damit Sie das Werkzeug wieder verlassen können.
- [ ] Wo die Daten gehostet werden, welche Unterauftragsverarbeiter beteiligt sind und was die Plattform nicht leistet. Keine macht Sie allein konform.

DORA: Finanzunternehmen in der EU

- [ ] Ein Register mit LEI, Rechtsordnung, unterstützter Funktion und Kritikalität je Anbieter und je Vertrag.
- [ ] Export im Format der amtlichen Vorlagen (die Leitfäden der Aufsichtsbehörden nennen xBRL-CSV-Pakete), wobei die Einreichung über den offiziellen Kanal bei Ihnen bleibt.
- [ ] Verfolgung von Ausstiegsplan, Prüfrecht und Unterauftragskette je Vertrag.
- [ ] Eine Konzentrationsansicht: wie viele Funktionen vom selben Anbieter abhängen.

Quelle: Verordnung (EU) 2022/2554 (DORA), Artikel 28 bis 31, auf EUR-Lex `https://eur-lex.europa.eu/eli/reg/2022/2554/oj`
Durchführungsverordnung (EU) 2024/2956, Vorlagen für das Informationsregister, auf EUR-Lex `https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj`

NIS2: wesentliche und wichtige Einrichtungen in der EU

- [ ] Bewertung je Lieferant mit Schwachstellen und Sicherheitspraktiken, nicht nur ein allgemeiner Fragebogen.
- [ ] Klauseln zur Vorfallmeldung des Lieferanten an Sie, mit Fristenverfolgung.
- [ ] Berichte, die das Leitungsorgan billigen und prüfen kann.
- [ ] Vorfallbehandlung mit den Fristen von Artikel 23: 24 Stunden, 72 Stunden und ein Monat.

Quelle: Richtlinie (EU) 2022/2555 (NIS2), Artikel 20, 21 und 23, auf EUR-Lex https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Durchführungsverordnung (EU) 2024/2690, technische und methodische Anforderungen, auf EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS: spanischer öffentlicher Sektor und seine Lieferanten

- [ ] Dass sie die Systemkategorie (Basis, mittel, hoch) unterscheidet und zeigt, welche op.ext-Maßnahmen gelten.
- [ ] Dienstgütevereinbarungen je Lieferant und regelmäßige Messung ihrer Einhaltung.
- [ ] Auswirkungs- und Risikoanalyse für einen Vorfall in der Lieferkette, mit Eindämmungsmaßnahmen.
- [ ] Den ENS-Konformitätsstatus des Lieferanten selbst, wenn er eine öffentliche Stelle bedient.

Quelle: Real Decreto 311/2022 (ENS), Artikel 2 und Anhang II, Maßnahmen op.ext, im BOE (spanisch) https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA: US-Gesundheitswesen und Business Associates

- [ ] Eine Kennzeichnung, welche Dritten mit Gesundheitsinformationen in Berührung kommen, und der Stand des Business-Associate-Vertrags jedes Dritten, mit Daten.
- [ ] Ein Verzeichnis der Subunternehmer des Business Associate und ihrer Zusicherungen.
- [ ] Verfolgung der Klauseln zur Meldung von Verletzungen und der 60-Tage-Frist.
- [ ] Wenn die Plattform selbst Gesundheitsinformationen speichert, ist sie Business Associate: Fordern Sie den Vertrag an, bevor Sie Daten laden.

Quelle: 45 CFR 164.308(b), Verträge mit Business Associates, auf eCFR https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), Verträge mit Business Associates (Security Rule), auf eCFR https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), Weitergabe an Business Associates, auf eCFR https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), Inhalt der Verträge mit Business Associates, auf eCFR https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, Meldung durch einen Business Associate, auf eCFR https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0: die US-Lieferkette der Verteidigung

- [ ] Ein Feld je Lieferant für die Art der verarbeiteten Informationen (FCI oder CUI) und das geforderte CMMC-Level.
- [ ] Einen Nachweis, dass Sie die Anforderungen im Vertrag weitergegeben haben (Flow-down).
- [ ] Den Stand jedes Subunternehmers gegenüber dem geforderten Level, mit Datum des letzten Nachweises.
- [ ] Wenn Sie CUI in das Werkzeug laden, dass sein Hosting die Cloud-Anforderung von 170.16(c) erfüllt.

Quelle: 32 CFR 170.23, Anwendung auf Subunternehmer, auf eCFR `https://www.ecfr.gov/current/title-32/section-170.23`
32 CFR Part 170 (CMMC-Programm), auf eCFR `https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170`

SAMA und NCA ECC: Finanz- und Nationalsektor Saudi-Arabiens

- [ ] Dass die Rahmenwerkbibliothek SAMA und ECC enthält und die Ausgabe nennt (die von uns geprüfte ist ECC-2:2024).
- [ ] Ein Inventar der Dritten mit Zugang zu Systemen oder Daten und Vertragsklauseln je Lieferant.
- [ ] Eine Kennzeichnung für Auslagerungs- und Cloud-Anbieter, die bei SAMA eine eigene Unterdomäne haben.
- [ ] Nachweise je Kontrolle, mit Verantwortlichem und Datum, um der Aufsicht zu antworten.

Quelle: SAMA Cyber Security Framework, Domäne 3.4 «Third Party Cyber Security», im SAMA Rulebook `https://rulebook.sama.gov.sa/en/34-third-party-cyber-security-0`
NCA Essential Cybersecurity Controls (ECC-2:2024), Domäne 4 `https://cdn.nca.gov.sa/api/files/public/upload/da829b21-c4ef-4a6e-9f6e-82690d612ee9_ECC-2-2024-.pdf`

Notizen