HodeiShield · Valutazione delle piattaforme di rischio di terze parti

Checklist di valutazione delle piattaforme TPRM per settore

Spunta ogni punto durante la demo con i tuoi fornitori e annota ciò che lo strumento non fa.

Criteri validi per qualsiasi settore

- [ ] Un inventario delle terze parti con responsabile interno, criticità, dati del contratto e subfornitori.
- [ ] Evidenze con responsabile, data di validità e stato, e l'evidenza scaduta che smette di contare.
- [ ] Come si ottengono le informazioni del fornitore: questionario, documenti, scansione esterna, SBOM. Ogni via misura qualcosa di diverso.
- [ ] Come si calcola il punteggio o il rischio: input visibili, metodo documentato e stime segnalate come tali.
- [ ] Un registro delle modifiche, l'esportazione dei tuoi dati e un'API, per poter lasciare lo strumento.
- [ ] Dove sono ospitati i dati, quali subresponsabili intervengono e cosa la piattaforma non fa. Nessuna ti rende conforme da sola.

DORA: entità finanziarie dell'UE

- [ ] Un registro con LEI, giurisdizione, funzione supportata e criticità per fornitore e per contratto.
- [ ] Esportazione nel formato dei modelli ufficiali (le guide dei supervisori citano pacchetti xBRL-CSV), con l'invio tramite il canale ufficiale che resta a te.
- [ ] Monitoraggio per contratto di piano di uscita, diritto di audit e catena di subappalto.
- [ ] Una vista di concentrazione: quante funzioni dipendono dallo stesso fornitore.

Fonte: Regolamento (UE) 2022/2554 (DORA), articoli da 28 a 31, su EUR-Lex `https://eur-lex.europa.eu/eli/reg/2022/2554/oj`
Regolamento di esecuzione (UE) 2024/2956, modelli del registro delle informazioni, su EUR-Lex `https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj`

NIS2: soggetti essenziali e importanti dell'UE

- [ ] Valutazione per fornitore con vulnerabilità e pratiche di sicurezza, non solo un questionario generico.
- [ ] Clausole di notifica degli incidenti dal fornitore verso di te, con monitoraggio del termine.
- [ ] Report che l'organo di gestione possa approvare e rivedere.
- [ ] Gestione degli incidenti con i termini dell'articolo 23: 24 ore, 72 ore e un mese.

Fonte: Direttiva (UE) 2022/2555 (NIS2), articoli 20, 21 e 23, su EUR-Lex https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Regolamento di esecuzione (UE) 2024/2690, requisiti tecnici e metodologici, su EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS: settore pubblico spagnolo e suoi fornitori

- [ ] Che distingua la categoria del sistema (base, media, alta) e mostri quali misure op.ext si applicano.
- [ ] Accordi sul livello di servizio per fornitore e misurazione periodica del loro rispetto.
- [ ] Analisi di impatto e di rischio per un incidente nato nella catena di approvvigionamento, con misure di contenimento.
- [ ] Lo stato di conformità ENS del fornitore stesso quando serve un ente pubblico.

Fonte: Real Decreto 311/2022 (ENS), articolo 2 e allegato II, misure op.ext, nel BOE (in spagnolo) https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA: sanità negli Stati Uniti e business associate

- [ ] Un contrassegno delle terze parti che toccano informazioni sanitarie e lo stato del contratto di business associate di ciascuna, con le date.
- [ ] Un registro dei subappaltatori del business associate e delle loro garanzie.
- [ ] Monitoraggio delle clausole di notifica delle violazioni e del termine di 60 giorni.
- [ ] Se la piattaforma stessa conserverà informazioni sanitarie, è un business associate: chiedi il contratto prima di caricare dati.

Fonte: 45 CFR 164.308(b), contratti con i business associate, su eCFR https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), contratti con i business associate (Security Rule), su eCFR https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), comunicazioni ai business associate, su eCFR https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), contenuto dei contratti con i business associate, su eCFR https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, notifica da parte di un business associate, su eCFR https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0: catena di fornitura della difesa USA

- [ ] Un campo per fornitore con il tipo di informazioni trattate (FCI o CUI) e il livello CMMC richiesto.
- [ ] La prova di aver trasferito i requisiti nel contratto (flow-down).
- [ ] Lo stato di ogni subappaltatore rispetto al livello richiesto, con la data dell'ultima evidenza.
- [ ] Se caricherai CUI nello strumento, che il suo hosting rispetti il requisito cloud di 170.16(c).

Fonte: 32 CFR 170.23, applicazione ai subappaltatori, su eCFR `https://www.ecfr.gov/current/title-32/section-170.23`
32 CFR Part 170 (programma CMMC), su eCFR `https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170`

SAMA ed ECC della NCA: settori finanziario e nazionale saudita

- [ ] Che la libreria di framework includa SAMA ed ECC e indichi l'edizione (quella che abbiamo consultato è ECC-2:2024).
- [ ] Un inventario delle terze parti con accesso a sistemi o dati e le clausole contrattuali per fornitore.
- [ ] Un contrassegno per i fornitori di esternalizzazione e di cloud, che in SAMA hanno un sottodominio proprio.
- [ ] Evidenze per controllo, con responsabile e data, per rispondere all'ente di vigilanza.

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

Note