HodeiShield · Evaluating third-party risk platforms

TPRM platform evaluation checklist by sector

Tick each point during the demo with your own suppliers and note what the tool does not do.

Criteria that apply to any sector

- [ ] A third-party inventory with an internal owner, criticality, contract data and subcontractors.
- [ ] Evidence with an owner, a validity date and a status, and expired evidence that stops counting.
- [ ] How supplier information is obtained: questionnaire, documents, external scan, SBOM. Each route measures something different.
- [ ] How the score or risk is calculated: visible inputs, a documented method and estimates marked as estimates.
- [ ] A change log, export of your data and an API, so you can leave the tool.
- [ ] Where data is hosted, which subprocessors take part and what the platform does not do. None makes you compliant on its own.

DORA: EU financial entities

- [ ] A register with LEI, jurisdiction, the function supported and criticality per provider and per contract.
- [ ] Export in the format of the official templates (the supervisors' guidance names xBRL-CSV packages), with filing through the official channel still in your hands.
- [ ] Per-contract tracking of exit plan, audit right and the subcontracting chain.
- [ ] A concentration view: how many functions depend on the same provider.

Source: Regulation (EU) 2022/2554 (DORA), Articles 28 to 31, on EUR-Lex `https://eur-lex.europa.eu/eli/reg/2022/2554/oj`
Implementing Regulation (EU) 2024/2956, register of information templates, on EUR-Lex `https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj`

NIS2: essential and important entities in the EU

- [ ] Assessment per supplier covering vulnerabilities and security practices, not only a generic questionnaire.
- [ ] Incident notification clauses from the supplier towards you, with deadline tracking.
- [ ] Reports that the management body can approve and review.
- [ ] Incident handling with the Article 23 deadlines: 24 hours, 72 hours and one month.

Source: Directive (EU) 2022/2555 (NIS2), Articles 20, 21 and 23, on EUR-Lex https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Implementing Regulation (EU) 2024/2690, technical and methodological requirements, on EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS: the Spanish public sector and its suppliers

- [ ] That it distinguishes the system category (basic, medium, high) and shows which op.ext measures apply.
- [ ] Service level agreements per supplier and periodic measurement of compliance.
- [ ] Impact and risk analysis for an incident that starts in the supply chain, with containment measures.
- [ ] The supplier's own ENS conformity status when it serves a public body.

Source: Royal Decree 311/2022 (ENS), Article 2 and Annex II, op.ext measures, in the BOE (Spanish) https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA: US healthcare and business associates

- [ ] A flag for which third parties touch health information and the status of each business associate contract, with dates.
- [ ] A record of the business associate's subcontractors and their assurances.
- [ ] Tracking of breach notification clauses and the 60-day limit.
- [ ] If the platform itself will store health information, it is a business associate: ask for the contract before loading data.

Source: 45 CFR 164.308(b), business associate contracts, on eCFR https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), business associate contracts (Security Rule), on eCFR https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), disclosures to business associates, on eCFR https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), content of business associate contracts, on eCFR https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, notification by a business associate, on eCFR https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0: the US defence supply chain

- [ ] A field per supplier for the type of information it handles (FCI or CUI) and the CMMC level required.
- [ ] Evidence that you have flowed the requirements down in the contract.
- [ ] The status of each subcontractor against the required level, with the date of the last evidence.
- [ ] If you will load CUI into the tool, that its hosting meets the cloud requirement of 170.16(c).

Source: 32 CFR 170.23, application to subcontractors, on eCFR `https://www.ecfr.gov/current/title-32/section-170.23`
32 CFR Part 170 (CMMC program), on eCFR `https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170`

SAMA and NCA ECC: Saudi financial and national sectors

- [ ] That the framework library includes SAMA and ECC and states the edition (the one we consulted is ECC-2:2024).
- [ ] An inventory of third parties with access to systems or data, and contract clauses per supplier.
- [ ] A flag for outsourcing and cloud providers, which have their own subdomain in SAMA.
- [ ] Evidence per control, with an owner and a date, to answer the supervising body.

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

Notes