HodeiShield · Hirugarrenen arriskuko plataformen ebaluazioa

TPRM plataformen ebaluazio-zerrenda sektorearen arabera

Markatu puntu bakoitza demoan zure hornitzaileekin eta idatzi tresnak zer ez duen egiten.

Edozein sektoretan balio duten irizpideak

- [ ] Hirugarrenen inbentarioa: barne-arduraduna, kritikotasuna, kontratuaren datuak eta azpikontratistak.
- [ ] Ebidentzia arduradunarekin, baliozkotasun-datarekin eta egoerarekin, eta iraungitakoak zenbatzeari uztea.
- [ ] Hornitzailearen informazioa nola lortzen den: galdetegia, dokumentuak, kanpoko eskaneatzea, SBOM. Bide bakoitzak gauza desberdina neurtzen du.
- [ ] Puntuazioa edo arriskua nola kalkulatzen den: sarrera ikusgarriak, metodo dokumentatua eta zenbatespen gisa markatutako balioak.
- [ ] Aldaketen erregistroa, zure datuen esportazioa eta API bat, tresna uzteko aukera izateko.
- [ ] Datuak non ostatatzen diren, zer azpiduntzaile parte hartzen duten eta plataformak zer ez duen egiten. Bakar batek ere ez zaitu bere kabuz betetzera eramaten.

DORA: EBko finantza-erakundeak

- [ ] Erregistro bat LEI, jurisdikzio, onartzen duen funtzio eta kritikotasunarekin, hornitzaile eta kontratu bakoitzeko.
- [ ] Txantiloi ofizialen formatuko esportazioa (gainbegiratzaileen gidek xBRL-CSV paketeak aipatzen dituzte), kanal ofizialetik aurkeztea zure esku geratuz.
- [ ] Kontratu bakoitzeko irteera-planaren, auditoria-eskubidearen eta azpikontratazio-katearen jarraipena.
- [ ] Kontzentrazio-ikuspegi bat: zenbat funtziok dauden hornitzaile beraren menpe.

Iturria: 2022/2554 Erregelamendua (EB) (DORA), 28 eta 31 artikuluen artean, EUR-Lex-en https://eur-lex.europa.eu/eli/reg/2022/2554/oj
2024/2956 Betearazpen-erregelamendua (EB), informazio-erregistroaren txantiloiak, EUR-Lex-en https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

NIS2: EBko erakunde funtsezko eta garrantzitsuak

- [ ] Hornitzaile bakoitzeko ebaluazioa, ahulguneak eta segurtasun-jardunak barne, ez galdetegi generiko bat soilik.
- [ ] Hornitzaileak zuri egindako intzidentzien jakinarazpen-klausulak, epearen jarraipenarekin.
- [ ] Zuzendaritza-organoak onartu eta berrikus ditzakeen txostenak.
- [ ] Intzidentzien kudeaketa 23. artikuluko epeekin: 24 ordu, 72 ordu eta hilabete bat.

Iturria: 2022/2555 Zuzentaraua (EB) (NIS2), 20., 21. eta 23. artikuluak, EUR-Lex-en https://eur-lex.europa.eu/eli/dir/2022/2555/oj
2024/2690 Betearazpen-erregelamendua (EB), eskakizun tekniko eta metodologikoak, EUR-Lex-en https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS: Espainiako sektore publikoa eta bere hornitzaileak

- [ ] Sistemaren kategoria bereizten duela (oinarrizkoa, ertaina, altua) eta zer op.ext neurri aplikatzen diren erakusten duela.
- [ ] Hornitzaile bakoitzeko zerbitzu-mailaren akordioak eta haien betetzearen aldizkako neurketa.
- [ ] Hornidura-katean sortutako intzidentzia baterako inpaktu- eta arrisku-analisia, ukipen-neurriekin.
- [ ] Hornitzailearen beraren ENS konformitate-egoera, erakunde publiko bati zerbitzua ematen dionean.

Iturria: 311/2022 Errege Dekretua (ENS), 2. artikulua eta II. eranskina, op.ext neurriak, BOE-n (gaztelaniaz) https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA: AEBetako osasuna eta business associate-ak

- [ ] Zer hirugarrenek ukitzen duten osasun-informazioa markatzea eta bakoitzaren business associate kontratuaren egoera, datekin.
- [ ] Business associate-aren azpikontratisten eta haien bermeen erregistroa.
- [ ] Urraketak jakinarazteko klausulen eta 60 eguneko epearen jarraipena.
- [ ] Plataformak berak osasun-informazioa gordeko badu, business associate da: eskatu kontratua datuak kargatu aurretik.

Iturria: 45 CFR 164.308(b), business associate-ekiko kontratuak, eCFR-n https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), business associate-en kontratuak (Security Rule), eCFR-n https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), business associate-ei egindako jakinarazpenak, eCFR-n https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), business associate-en kontratuen edukia, eCFR-n https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, business associate-aren jakinarazpena, eCFR-n https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0: AEBetako defentsa-hornidura katea

- [ ] Hornitzaile bakoitzeko eremu bat maneiatzen duen informazio motarekin (FCI edo CUI) eta eskatzen zaion CMMC mailarekin.
- [ ] Eskakizunak kontratuan transmititu dituzula frogatzen duen ebidentzia (flow-down).
- [ ] Azpikontratista bakoitzaren egoera eskatutako mailaren aldean, azken ebidentziaren datarekin.
- [ ] CUI tresnan kargatuko baduzu, haren ostatatzeak 170.16(c)-ko hodei-eskakizuna betetzen duela.

Iturria: 32 CFR 170.23, azpikontratistei aplikatzea, eCFR-n https://www.ecfr.gov/current/title-32/section-170.23
32 CFR 170. zatia (CMMC programa), eCFR-n https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

SAMA eta NCAren ECC: Saudi Arabiako finantza- eta sektore nazionala

- [ ] Esparruen liburutegiak SAMA eta ECC barne hartzen dituela eta edizioa adierazten duela (guk kontsultatutakoa ECC-2:2024 da).
- [ ] Sistemetara edo datuetara sarbidea duten hirugarrenen inbentarioa eta hornitzaile bakoitzeko kontratu-klausulak.
- [ ] Azpikontratazio- eta hodei-hornitzaileen marka, SAMAn azpidomeinu propioa dutenak.
- [ ] Kontrol bakoitzeko ebidentzia, arduradunarekin eta datarekin, gainbegiratze-erakundeari erantzuteko.

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

---

Oharrak