

NIS2 kontrollnimekiri

Kümme NIS2 miinimumnõuet ühes vaates: mida auditeerija tõendina küsib, milline on kiire võit ja milline on tüüpiline puudujääk. Märki tehtud punktid ja vaata, kus seisad.

Koostanud Tehisabiline OÜ · Viimati sisuliselt uuendatud 24. oktoobril 2026

Lühidalt

NIS2 kontrollnimekiri katab direktiivi artikli 21 kümme miinimumnõuet. Iga meetme juures on kirjas, mida auditeerija tõendina küsib, milline on kiire võit ja milline on tüüpiline puudujääk. Nimekiri aitab seisu kaardistada ja tegevuskava järjestada, kuid ei asenda sõltumatut auditit ega hinda meetmete tegelikku toimimist.

Kasuta seda juhatuse või turvajuhi töövahendina: märki tehtud punktid, vaata edenemist ja vali järgmised sammud. Edenemine salvestub ainult sinu brauseris.

Laadi kontrollnimekiri PDF-ina · Intsidendist teatamise juhend

Kümme meedet

☐ 1. Riskianalüüs ja turvapoliitika

Nõue: dokumenteeritud riskianalüüs, kinnitatud turvapoliitika ja ülevaade kriitilistest infovaradest.

Auditeerija küsib: riskiregistrit omanikega, poliitika versiooni ja kinnitamise minutit, infovarade loetelu.

Kiire võit: kirjuta üles kümme kriitilisemat infovara ja viis suurimat riski koos vastutajaga.

Tüüpiline puudujääk: poliitika on olemas, kuid sellel puudub omanik ja regulaarne ülevaatus.

☐ 2. Intsidentide käsitlemine

Nõue: tuvastamise, käsitlemise, eskaleerimise ja teatamise kord koos rollidega.

Auditeerija küsib: intsidendiplaani, kontaktide nimekirja, viimase õppuse tulemusi ja teatamise malli.

Kiire võit: üheleheküljeline tegevusplaan koos ööpäevaringse kontaktiga.

Tüüpiline puudujääk: plaan on kirjutatud, kuid seda pole kordagi läbi harjutatud.

☐ 3. Toimepidevus ja varundus

Nõue: toimepidevusplaan, ajakohased varukoopiad ja taastamise harjutamine.

Auditeerija küsib: varunduse taastetesti logi, taastamisaega (RTO), andmekao piiri (RPO) ja kriisiside plaani.

Kiire võit: taasta selle nädala jooksul üks kriitiline süsteem varukoopiast ja mõõda kulunud aeg.

Tüüpiline puudujääk: varundus on olemas, kuid taastamist pole kunagi testitud.

☐ 4. Tarneahela turve

Nõue: teadlikkus tarnijatest, kriitiliste tarnijate turvanõuded ja nende hindamine.

Auditeerija küsib: tarnijate loetelu kriitilisusega, lepingute turvatingimusi ja ülevaatuse märkmeid.

Kiire võit: märgi kümme kriitilisemat tarnijat ja nende ligipääsud sinu süsteemidele.

Tüüpiline puudujääk: lepingutes puuduvad turvanõuded ja intsidendist teatamise kohustus.

☐ 5. Turvaline hankimine ja arendus

Nõue: turvanõuded hankimisel, turvaline arendus ja haavatavuste haldamise kord.

Auditeerija küsib: arendustöö kontrollnimekirja, sõltuvuste skaneerimise aruandeid ja parandamise tähtaegu.

Kiire võit: lülita sisse sõltuvuste turbeteated ja pane kriitiliste haavatavuste parandamise tähtjaks seitse päeva.

Tüüpiline puudujääk: haavatavusi skaneeritakse, kuid puudub tähtaeg ja vastutaja.

☐ 6. Meetmete tõhususe hindamine

Nõue: regulaarne testimine ja ülevaatus, mis näitab, kas meetmed päriselt toimivad.

Auditeerija küsib: testiraporteid, paranduste jälgimist ja juhtkonna ülevaatuse märkmeid.

Kiire võit: lepi kokku üks läbistustest või lauaõppus ja seo leiud parandusplaaniga.

Tüüpiline puudujääk: test on tehtud, kuid leiud jäävad jälgimata.

☐ 7. Krüptograafia ja krüpteerimine

Nõue: krüpteerimise kasutamise põhimõtted, võtmete haldus ja sertifikaatide jälgimine.

Auditeerija küsib: TLS-i seadistust, võtmete loetelu ja sertifikaatide aegumise jälgimist.

Kiire võit: koosta sertifikaatide ja saladuste loetelu koos aegumiskuupäevadega.

Tüüpiline puudujääk: võtmed ja paroolid on koodirepos või jagatud tabelis.

☐ 8. Ligipääsukontroll ja MFA

Nõue: vähimate õiguste põhimõte, ligipääsude ülevaatus ja mitmefaktoriline autentimine.

Auditeerija küsib: õiguste matriksit, töölt lahkumise protseduuri ja MFA kohaldamise tõendit.

Kiire võit: kehtesta MFA e-postile, halduskontodele ja pilveteenustele.

Tüüpiline puudujääk: jagatud admin-kontod ja endiste töötajate ligipääsud.

☐ 9. Koolitused ja küberhügieen

Nõue: regulaarne koolitus töötajatele ja juhtidele, sealhulgas praktilised õppused.

Auditeerija küsib: koolituste toimumise tõendeid, materjale ja õppuste tulemusi.

Kiire võit: viia läbi 30-minutiline sessioon ja üks andmepüügi test.

Tüüpiline puudujääk: koolitus on tehtud üks kord töölevõtmisel.

☐ 10. Juhtkonna vastutus

Nõue: juhtorgan kinnitab meetmed, jälgib nende täitmist ja vastutab nende eest.

Auditeerija küsib: juhatuse koosoleku protokolle, riskide kinnitamist ja turvanäitajaid.

Kiire võit: lisa küberturvalisus juhatuse päevakorda püsiva punktina.

Tüüpiline puudujääk: vastutus on delegeeritud ilma järelevalve ja aruandluseta.

Teavitamine: 24 tundi, 72 tundi ja üks kuu

Olulisest küberintsidendist tuleb teatada kolmes etapis: varajane hoiatus 24 tunni jooksul, täpsustav teade 72 tunni jooksul ja lõpparuanne ühe kuu jooksul ([direktiiv 2022/2555](#), [artikkel 23](#) (<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>)). Eestis esitatakse teated Riigi Infosüsteemi Ametile. Täpne sisu ja vorm on kirjas [intsidendist teatamise juhendis](#).

Isikuandmetega seotud rikkest tuleb lisaks teatada Andmekaitse Inspeksioonile 72 tunni jooksul ([AKI](https://www.aki.ee/) (<https://www.aki.ee/>)). Need kohustused võivad samal ajal kehtida.

Tõendid, mida auditeerija küsib

Riskianalüüs

Peamine tõend

Riskiregister, poliitika ja kinnitamise minut

Kes hoiab

Juhtkond / turvajuht

Intsidendid

Peamine tõend

Plaan, kontaktid, õppuse ja teatamise tõendid

Kes hoiab

IT / turvajuht

Toimepidevus

Peamine tõend

Taastetesti logi, RTO ja RPO

Kes hoiab

IT

Tarneahel

Peamine tõend

Tarnijate loetelu ja lepingutingimused

Kes hoiab

Hanked / juhtkond

Arendus

Peamine tööend

Sõltuvuste skaneeringud ja parandustähtjad

Kes hoiab

Arendus

Testimine

Peamine tööend

Testiraportid ja paranduste jälgimine

Kes hoiab

Turvajuht

Krüptograafia

Peamine tööend

Võtmete loetelu ja sertifikaatide jälgimine

Kes hoiab

IT

Ligipääs

Peamine tööend

Õiguste maatriks ja MFA tööend

Kes hoiab

IT

Koolitus

Peamine tõend

Osalejate nimekiri ja õppuse tulemused

Kes hoiab

Personal / turvajuht

Juhtkond

Peamine tõend

Juhatus protokoll ja riskide kinnitamine

Kes hoiab

Juhtkond

Küsimused kontrollnimekirja kohta

Mis on NIS2 kontrollnimekiri?

See on kümne NIS2 miinimumnõude praktiline läbivaatus: iga meetme juures on kirjas, mida auditeerija tõendina küsib, milline on kiire võit ja milline on tüüpiline puudujääk.

Kas kontrollnimekiri asendab auditit?

Ei. Kontrollnimekiri aitab seisu kaardistada ja tegevuskava järjestada, kuid ei hinda meetmete tegelikku toimimist ega asenda sõltumatut auditit.

Kellele kontrollnimekiri mõeldud on?

Eelkõige NIS2 kohustuslastele ja nende juhtidele, kes peavad meetmete seisu kinnitama, ning ettevõtetele, kes soovivad esmase turvahügieeni üle vaadata.

Kas märkeruutude edenemine salvestatakse kuskile?

Ei. Edenemine salvestub ainult sinu brauseri lokaalsesse mällu ja ei saadeta serverisse. Saad selle igal ajal nullida.

Kust alustada, kui aega on vähe?

Alusta varunduse taastetestist, mitmefaktorilisest autentimisest ja ligipääsude ülevaatamisest. Need kolm annavad suurima mõju väikseima töömahuga.
