TIS2 IR DORA: SENI-NAUJI SANTYKIAI SU TREČIOSIOMIS ŠALIMIS

Martynas Savickas,
vCISO vadovas

Kas reguliuoja?

DORA - Lietuvos bankas

TIS2 - Nacionalinis kibernetinio saugumo centras (NKSC) per Kibernetinio saugumo įstatymą

Kokia trečiųjų šalių (tiekėjų) valdymo prasmė?

- Pasitikėjimo valdymas (validavimas)
- Tiekimo grandinės monitoringas
- Atsparumo valdymas
- Įsipareigojimų formalizavimas

Kontrolės būdai

- Klausimynai (ilgi/trumpi, formalūs/detalūs)
- Auditas (vidinis, nepriklausomas išorinis)
- Sertifikatai
- Detalūs reikalavimai kontraktuose (pvz. SLA)
- Rizikos vertinimas

Valdymo būdai

- Vidiniai resursai - nauja funkcija
- Vidiniai resursai - priskyrimas (pirkimai, teisė, operacijos)
- Auditas (vidinis, nepriklausomas išorinis)
- Paslaugos teikėjas (išorinis)

Kontrolės siekis. Principai

Parodomasis

- Noras minimizuoti sąnaudas, turėti kažką jei reiks parodyti, siekiama apsidrausti, nematoma vertė.

Aktualusis

- Atsižvelgiama į įmonės brandą ir galimybes (resursus), įvertinama įtaka verslui ne tik atitikties požiūriu, bet ir keičiant sprendimų priėmimo principus.

Perfekcionistinis (teorinis)

- Vadovaujamasi pina apimtimi gerosiomis praktikomis, šablonais, principais. Neatsižvelgiama į ribotas galimybes išlaikyti užsibrėžtą detalumą, kuriamos labai komplikuotos kontrolės priemonės.

Aktualus principas

- Tinkamiausiais organizacijai, su žemo/vidutinio lygio Informacijos apsaugos branda
- Pirmus 12-24 mėnesius kuriamas Informacijos apsaugos valdymo ir trečiųjų šalių valdymo santykio pagrindas griežtai kontroliuojant sąnaudas
- Subalansuotas detalumo ir kontrolės mechanizmų tobulinimas
- Galimybė vadovams nutarti kai detalumo užtenka priimti kokybiškiems sprendimams
- Galimybė turėti numatomas ir pastovias kontrolių sąnaudas

Siekiai

- Itakos minimizavimas
- Atsparumo faktoriaus įvedimas renkantis IRT paslaugas
- Pakeičiamumo supaprastinimas ir užtikrinimas
- Numatomos paslaugų alternatyvos
- Incidentų sprendimai, veiksmų planai ir jų testavimas

O jei aš paslaugos teikėjas?

Anksčiau ar vėliau teks:

- Pasiruošti trumpiems ir ilgiems klausimynams
- Turėti veiksmingą informacijos apsaugos valdymo politiką
- Atlikti nepriklausomą informacijos apsaugos valdymo auditą
- Apsvarstyti kibernetinių incidentų žalos draudimo įsigijimą
- Į derybas ir sutartis įtraukti atitikties valdymo sąnaudas
- Testuoti savo atsparumą ir turėti tokio testavimo įrodymus

Dėkoju už Jūsų dėmesį!

Klausimai?

https://www.linkedin.com/in/martynassavickas/

martynas@smartciso.lt