Cyber Security – kokią audito įmonę pasirinkti reikalaujamų Kibernetinio saugumo auditų atlikimui?

Pirma, ką reiškia „reikalaujami“ kibernetinio saugumo auditai? „Reikalavimas“ – kyla iš Kibernetinio saugumo įstatymo, kuriuo buvo nustatyta pareiga įmonėms atlikti kibernetinio saugumo auditus ne rečiau kaip kartą per 3 metus (žr. Kibernetinio saugumo įstatymo 14 straipsnio 8 dalį, bei Aprašo 8 skirsnį, kuriame rasite detalizuotą informaciją – t.y. kad įmonės vadovas turi būti patvirtinęs auditų atlikimo tvarką bei, kad vadovas turi būti pasiruošęs pateikti atliktų kibernetinių saugumo audito ataskaitas į KSIS sistemą NKSC pareikalavus).

Antra, kas gali atlikti Kibernetinio saugumo auditus? Atsakymas – pagal Kibernetinio saugumo įstatymą, tai dviejų tipų įmonės (žr. Kibernetinio saugumo įstatymo 14 straipsnio 8 dalį):

- Arba nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugumo atitikties auditoriai, audito įmonės ar kitos institucijos.
- Nacionalinio kibernetinio saugumo centro (toliau – NKSC) mokymus išklausę ir kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą išlaikę asmenys, kurie atitinka Nacionalinio kibernetinio saugumo centro kibernetinio saugumo auditų atlikimo metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus, (toliau kartu – auditoriai).

Trečia, kaip žinoti kokie tarptautiniai sertifikatai tinkami? Atsakymas – gera žinia, kad NKSC 2025.06.27 dieną pateikė sąrašą - žr. Priedą Nr.1, kuriame nurodomi kokie pvz., ISACA, CompTIA sertifikatai yra tinkami.

Ketvirta, kaip žinoti kas yra išklausę NKSC nurodytus mokymus? Atsakymas – sąrašas asmenų kurie turi sertifikatus nėra paskelbtas, tačiau yra aišku kokius mokymus turi būti asmenys išklausę (žr. Priedą Nr2).

Bendra rekomendacija – prieš užsakant **Kibernetinio saugumo auditą** pasitikrinti ar auditas bus NKSC „formaliai užskaitytas“, t.y. ar bus atliktas įmonės, kuri atitinka keliamus reikalavimus. Atitinkamai rekomenduotina paprašyti, kad auditą atliekanti įmonė pateiktų reikiamus sertifikatus (pvz., ISO27001 sertifikatą ir konkretaus asmens, atliksiančio auditą sertifikatą).

OIXIO UAB | Savanorių pr. 321C, LT-50120 Kaunas | Liepyno g. 25A, LT-08108 Vilnius | www.oixio.eu/lt

Kibernetinio saugumo auditorių tarptautinių organizacijų sertifikatų sąrašas

Sąrašas pateiktas – Kibernetinio saugumo mokymų skirtų kibernetinio saugumo subjekto vadovui, kibernetinio saugumo vadovui ir saugos įgaliotiniui ir kibernetinio saugumo auditoriui tvarkos aprašo 1 priede.

Nr.	Pilnas sertifikato pavadinimas	Sutrumpintas sertifikato pavadinimas
1.	Computing Technology Industry Association Advanced Security Practitioner	CompTIA CASP+
2.	International Information System Security Certification Consortium, Inc. Certified in Governance, Risk and Compliance	ISC2 CGRC
3.	International Information System Security Certification Consortium, Inc. Information Systems Security Management Professional	ISC2 ISSMP
4.	International Information System Security Certification Consortium, Inc. Certified Information Systems Security Professional	ISC2 CISSP
5.	Global Information Assurance Certification Systems and Network Auditor	GIAC GSNA
6.	Global Information Assurance Certification Security Leadership Certification	GIAC GSLC
7.	Information Systems Audit and Control Association Certified Information Systems Auditor	ISACA CISA
8.	Information Systems Audit and Control Association Certified Information Security Manager	ISACA CISM
9.	Information Systems Audit and Control Association Certified in Risk and Information Systems Control	ISACA CRISC
10.	Information Systems Audit and Control Association Certified in Governance of Enterprise IT	ISACA CGEIT
11.	International Council of E-Commerce Consultants Certified Chief Information Security Officer	EC CCISO
12.	ISO/IEC 27001 Auditor	-
13.	ISO/IEC 27001 Lead Auditor	-
14.	ISO/IEC 27001 Senior Lead Auditor	-

NKSC reikalaujami mokymai ir atitinkamai išduodami sertifikatai

- Iš NKSC pateikiamų mokymų sąrašo, tinkamas Kibernetinio saugumo vadovo kursas ir atitinkamas sertifikatas.