

TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU



 **NKS** NACIONALNO
KOORDINACIJSKO
SREDIŠTE

CARNET

Revizije kibernetičke sigurnosti - put do provedbe

Domagoj Javorović
dr. sc. Natalija Parlov Una



Što je NIS2 *compliance*?



Zakon o kibernetičkoj sigurnosti (NN 14/2024)

Nacionalni regulatorni okvir za provedbu NIS2 u RH

čl. 30, st. 3 – mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe uredit će se uredbom iz članka 24. ovoga Zakona.

čl. 31, st. 2 – provjera usklađenosti ... obavlja se u postupku revizije kibernetičke sigurnosti ključnih i važnih subjekata te u postupku samoprocjene kibernetičke sigurnosti važnih subjekata

čl. 33, st. 2 – Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti propisuju ..., pravila, tehničke zahtjeve, norme i postupke koji se primjenjuju u provedbi revizije kibernetičke sigurnosti ...



Uredba o kibernetičkoj sigurnosti (NN 135/2024)

Prilog II – Mjere upravljanja kibernetičkim sigurnosnim rizicima – sastavni dio Uredbe



Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti

Prilog B – Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima
Prilog C – Katalog kontrola

„NIS2 *compliance*” u Hrvatskoj znači usklađenost sa Zakonom o kibernetičkoj sigurnosti

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti

Kroz postupak certifikacije provjerava se:

- sposobnost organizacije
- stručnost djelatnika
- i osigurava standardizirani pristup revizijama

Revizija doprinosi:

- dokazivanju usklađenosti sa ZKS-om
- pouzdanijem nadzoru nad provedbom
- pravodobnom prepoznavanju i otklanjanju nedostataka
- kontinuiranom poboljšanju sigurnosnih praksi
- jačanju kibernetičke otpornosti organizacija i RH



Revizija kibernetičke sigurnosti osigurava:

- ✓ neovisnost
- ✓ dosljednost
- ✓ stručnost
- ✓ provjerljivost
- ✓ povjerenje i
- ✓ identifikaciju stvarnih rizika

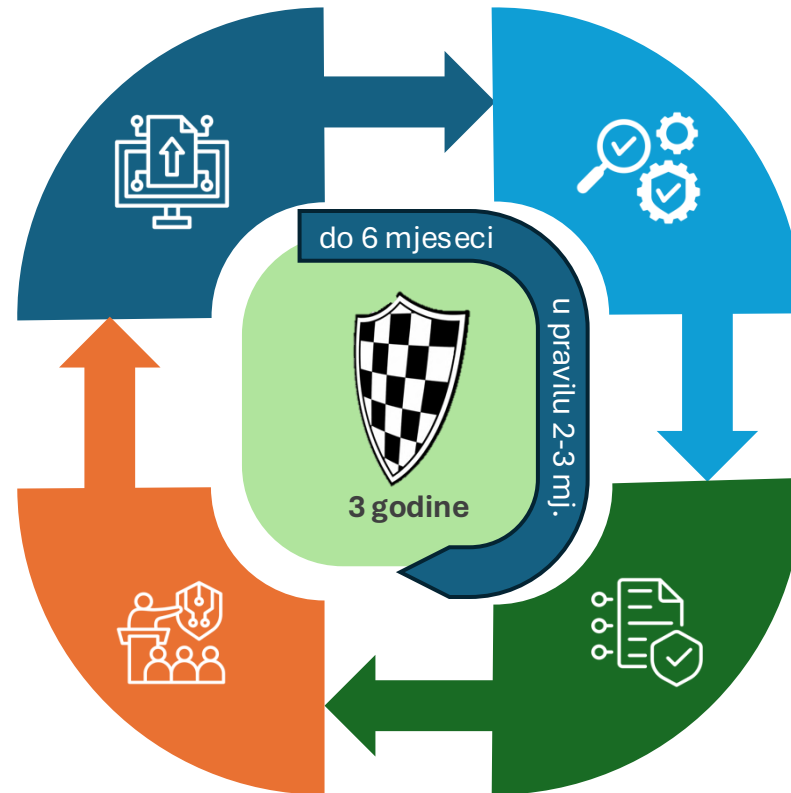
Revizije kibernetičke sigurnosti mogu provoditi samo certificirani pružatelji upravljanih sigurnosnih usluga (PRUS)

Certifikacijski ciklus

21. kolovoza 2025. godine donesena su
Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti

Prijava i preliminarna provjera

PRUS podnosi zahtjev i dokazuje osnovne organizacijske, tehničke i stručne preduvjete.



Analiza dokumentacije

ZSIS provjera politike, procedure, metodologiju revizije, neovisnost, nepristranost, način sprječavanja sukoba interesa,...

Izdavanje i nadzor

Certifikat se izdaje na tri godine, uz redovne nadzore i moguće nenajavljene nadzore

Revizorska posjeta i završna evaluacija

ZSIS provjerava stvarnu implementaciju procesa, resurse i kompetencije revizorskog tima te donosi odluku o certifikaciji.

Proces usklađen sa ISO/IEC 17065:2012

Registar certificiranih pružatelja upravljanih sigurnosnih usluga



<https://www.zsis.hr/default.aspx?id=660>

Kontakt:

certificiranje_rks@zsis.hr
zsis@zsis.hr



Hvala na pažnji.

