



REVIZIJE PREMA UREDBI O KIBERNETIČKOJ SIGURNOSTI

– ŠTO OČEKIVATI U PRAKSI?

Tomislav Boros – ZSIS
Marko Žalac – Deloitte

Direktiva NIS 2 (Direktiva (EU) 2022/2555)

Osiguravanje mrežnih i informacijskih sustava



Zakon o kibernetičkoj sigurnosti (NN, 14/24)

Postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti



Uredba o kibernetičkoj sigurnosti (NN, 135/2024)

Razrada operativnih i provedbenih elemenata Zakona



Nacionalni regulatorni okvir za provedbu Direktive NIS 2 (Direktiva (EU) 2022/2555)

Zakon o kibernetičkoj sigurnosti (NN, 14/24)

Postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti



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

2 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

3 čl. 32. st. 1 – Reviziju kibernetičke sigurnosti ključnih i važnih subjekata **provode revizori kibernetičke sigurnosti**.
st. 2 – ... su pružatelji upravljanih sigurnosnih usluga kojima je izdan:
– nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti ...

4 čl. 33. st. 1 – **Nacionalni sigurnosni certifikat** za reviziju kibernetičke sigurnosti izdaje središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti **na temelju pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti**.
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)

Razrada operativnih i provedbenih elemenata Zakona

Prilog II – Mjere upravljanja kibernetičkim sigurnosnim rizicima



Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti

21. kolovoza 2025. godine

Prilog B – Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima

Prilog C – Katalog kontrola



Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti



Što?

Kroz postupak certifikacije provjerava se:

- sposobnost organizacije
- stručnost djelatnika
- osigurava standardizirani pristup revizijama



Zašto?

Revizija kibernetičke sigurnosti predstavlja **službeni** mehanizam dokazivanja usklađenosti stanja kibernetičke sigurnosti, osigurava:

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



Zbog?

Revizija doprinosi:

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



Tko?

Reviziju provode **certificirani** revizori kibernetičke sigurnosti, odnosno – pružatelji upravljanih sigurnosnih usluga (PRUS*) koji posjeduju **nacionalni sigurnosni certifikat**, dok za tijela državne uprave i druga državna tijela reviziju provodi **središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti (ZSIS)**

*PRUS – poslovni subjekt odnosno pravna osoba



Postupak certifikacije i certifikacijski ciklus

usklađen s ISO/IEC 17065:2012 – Zahtjevi za tijela koja provode certifikaciju proizvoda procesa i usluga

1



Prijava za certifikaciju

Dostavljanje relevantne dokumentacije ZSIS-u

3



Preliminarna provjera

Provjera osnovnih svojstava dostavljene dokumentacije / uvjeta

5



Analiza dokumentacije

Analiza cjelokupne dokumentacije i procesa revizije

7



Završna neovisna evaluacija

Evaluacija i procjena rizika od neovisne osobe ili tima

2



Sastanak

Održavanje pripremnog sastanka radi pojašnjavanja osnovnih uvjeta

4



Dodatne radnje

Dopune ili ispravci dokumentacije u slučaju pronađenih nedostataka ili nesukladnosti

6



Revizorska posjeta

Pregled:

- Stručnog osoblja – revizora
- Stvarno stanje i usporedba s propisanom dokumentacijom
- Oprema
- ...

8



Izdavanje Nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti

Unos podataka u Registar

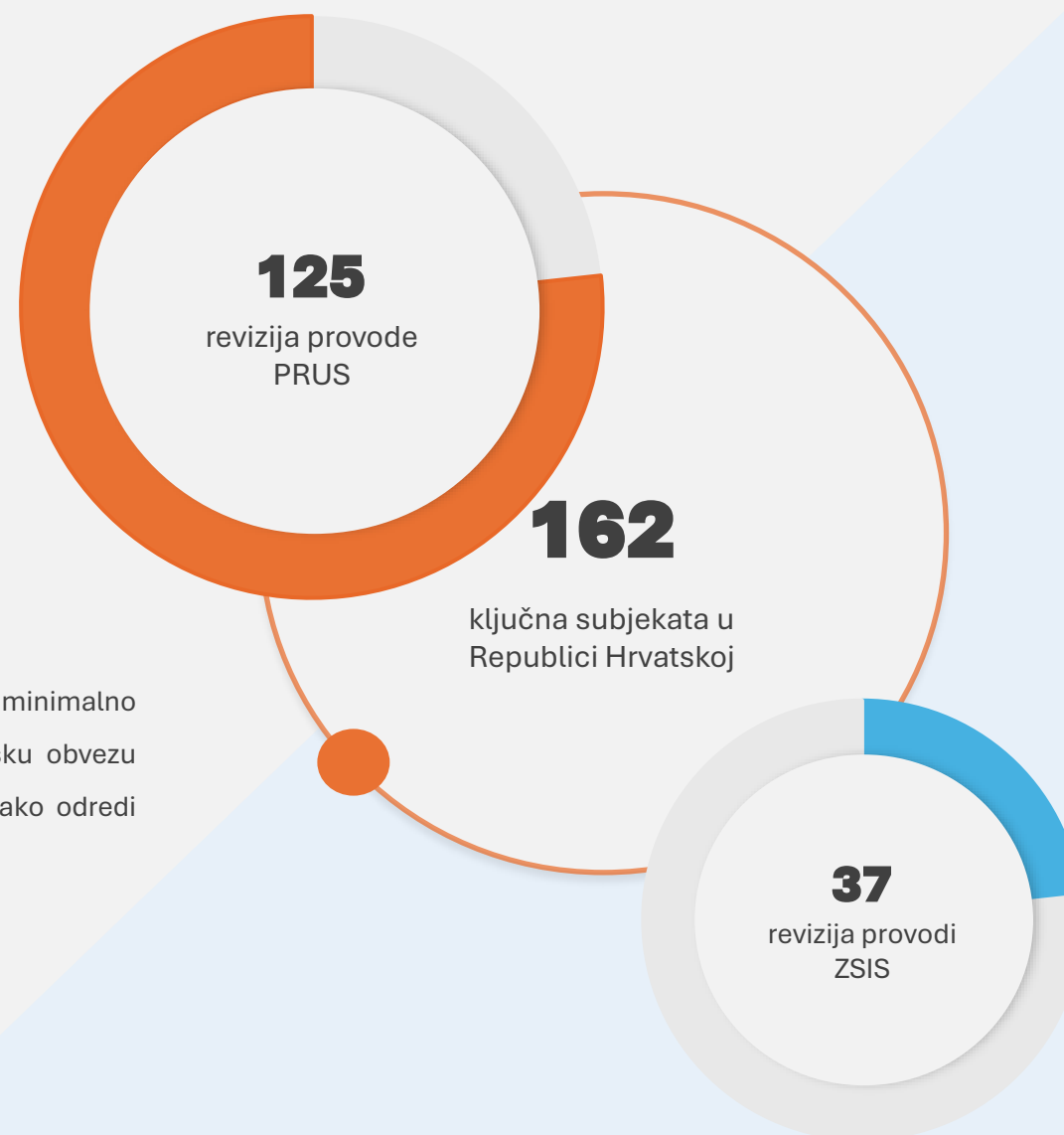


usklađen s ISO/IEC 17065:2012 – Zahtjevi za tijela koja provode certifikaciju proizvoda procesa i usluga

Poslovna vrijednost Nacionalnog sigurnosnog certifikata

Prema Izvješću Nacionalnog centra za kibernetičku sigurnost za 2. kvartal 2026. godine (*Pregled implementacije Zakona o kibernetičkoj sigurnosti (Q2 2026)*), u Republici Hrvatskoj trenutno je kategorizirano **162 ključna subjekata** koji imaju zakonsku **obvezu** provedbe revizije **najmanje jednom** svake dvije godine, a od kojih za čak **125 ključnih subjekata**, reviziju kibernetičke sigurnosti provode **certificirani** pružatelji upravljanih sigurnosnih usluga (PRUS). ZSIS je nadležan za provedbu revizije nad 37 tijela državne uprave.

Osim **ključnih subjekata** koji imaju zakonsku obvezu provoditi reviziju redovno, minimalno jednom u dvije godine, na tržištu postoji i **636 važan subjekt**, koji nemaju zakonsku obvezu redovite provedbe revizije, ali koji također mogu biti dužni provesti reviziju ukoliko tako odredi nadležno tijelo. Kod tih subjekata reviziju također provodi **certificirani** PRUS.





Dosadašnja iskustva

u certifikacijskim postupcima za reviziju kibernetičke sigurnosti

- Dugotrajni interni procesi odlučivanja
- Nepotpuno ispunjavanje organizacijskih zahtjeva
 - međunarodni certifikati u opseg ne uključuju uslugu revizije → potrebno kreirati relevantnu dokumentaciju (*npr. politike i procedure, pravila i sl.*)
- Neusklađenost sa svih 13 mjera za NAPREDNU razinu – kategorizacija i certifikacija → odvojeni procesi

Nepotpuno ispunjavanje stručnih zahtjeva:

- potreban broj provedenih revizija,
- minimalno 3 vođene revizije u tri godine,
- godine relevantnog radnog iskustva,
- odgovarajući stupanj obrazovanja te
- nedostatak stručnih osoba – gubitak sposobnosti



Registar certificiranih

pružatelja upravljanih sigurnosnih usluga



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

Kontakt

- certificiranje_rks@zsis.hr
- zsis@zsis.hr

