

Deloitte.

Revizija UKS-a u praksi

Od regulatornih zahtjeva do operativne implementacije

Zagreb, Rujan 2026.



Sadržaj



Regulatorni okvir



Hrvatski okvir

Zakon o kibernetičkoj sigurnosti (NN 14/2024)
Uredba o kibernetičkoj sigurnosti (NN 134/2024)



Europski okvir

Direktiva (EU)
2022/2555 (NIS2)



Institucionalni okvir

NCSC-HR / SOA
ZSIS
CERT / CSIRT
HNB / HANFA
HAKOM

! NIS2 definira načela, a hrvatski Zakon i Uredba definiraju konkretne obveze, razine mjera i način provjere usklađenosti.

Tko mora biti usklađen?

NIS2 se primjenjuje na javne i privatne subjekte iz obuhvaćenih sektora ovisno o njihovoj veličini ili posebnim kriterijima

Ključni subjekti



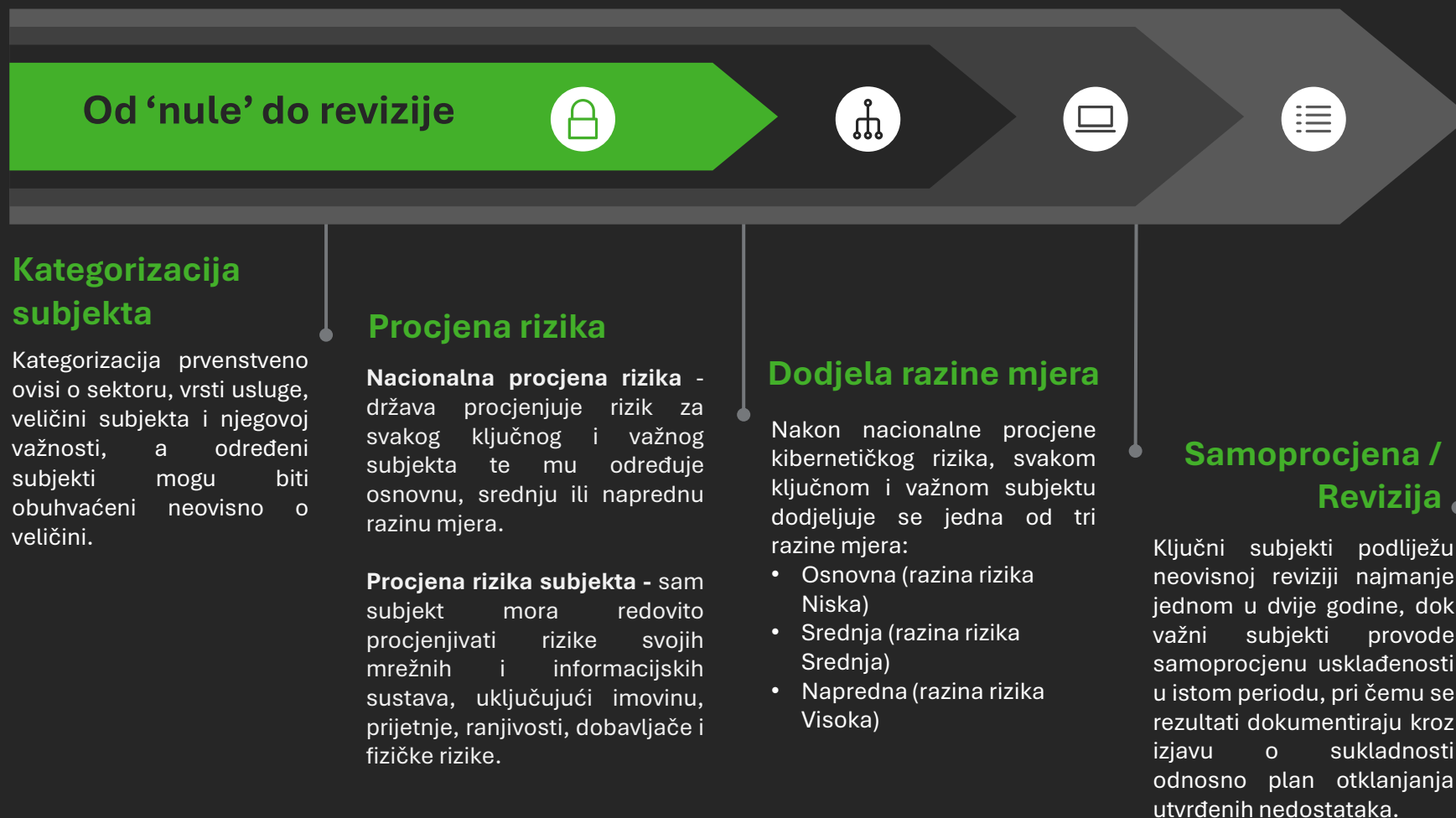
Važni subjekti



	Broj zaposlenih 	Godišnji prihod / imovina 
Veliki*	>250	>50/43 mil €
Srednji*	>50	>10 mil €
Mali*	>10	>2 mil €

*Potrebno je zadovoljiti oba kriterija

Kako Uredba povezuje subjekte i obveze?



Nisu svi subjekti obvezni provoditi isti broj i istu složenost kontrola. Opseg zahtjeva ovisi o:

- *Kritičnosti subjekta*
- *Rezultatima procjene rizika*
- *Dodijeljenoj razini mjera*

Model procjene rizika

NIS2 – Model nacionalne procjene kibernetičkog rizika

Nacionalna procjena rizika provodi se za svaki ključni i važni subjekt u okviru kategorizacije, a njezin je cilj odrediti obvezujuću razinu mjera kibernetičke sigurnosti.

Nacionalna procjena rizika

Provodi je nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, na temelju metodologije i procjena koje razvija središnje državno tijelo za kibernetičku sigurnost.

Ulazni podaci

- Veličina subjekta
- Sektor u kojem subjekt posluje
- Relevantne vrste kibernetičkih napada
- Vrste i sposobnosti napadača
- Vjerojatnost napada
- Potencijalna ozbiljnost poremećaja usluga/djelatnosti
- Stanje kibernetičke sigurnosti na globalnoj i nacionalnoj razini

Rezultat procjene

Niska razina rizika	Srednja razina rizika	Visoka razina rizika
Osnovne mjere	Srednje mjere	Napredne mjere



Nacionalna procjena rizika → razina rizika subjekta → obvezujuća razina mjera kibernetičke sigurnosti

Razine mjera kibernetičke sigurnosti

Osnovna razina	Niska razina rizika	Temeljne mjere zaštite	Zaštita od uobičajenih prijetnji	Osnovna razina organizacijskih i tehničkih kontrola
Srednja razina	Srednja razina rizika	Naprednije mjere zaštite	Dodatne mjere za povećane rizike	Proširene kontrole i zahtjevi
Napredna razina	Visoka razina rizika	Najviša razina zaštite	Mjere za sofisticirane i ciljane prijetnje	Najstroži zahtjevi i rokovi

Viša razina mjera uključuje mjere prethodne razine i dodaje zahtjevnije mjere proporcionalne većoj razini kibernetičkog rizika.

Mjere upravljanja kibernetičkim sigurnosnim rizicima

13 kategorija mjera za ključne i važne subjekte

**Predanost i odgovornost osoba odgovornih za provedbu
mjera upravljanja kibernetičkim sigurnosnim rizicima**



Revizija kibernetičke sigurnosti



Od regulatornog zahtjeva do dokaza usklađenosti – revizija potvrđuje da su zahtjevi Uredbe o kibernetičkoj sigurnosti ne samo formalno ispunjeni, već i učinkovito implementirani.

Revizijski proces



Testiranje kontrola kibernetičke sigurnosti



Ocjenjivanje kontrola kibernetičke sigurnosti

Ocjena	Dokumentacija	Implementacija
1 – Nedostatno	Dokumentacija ne postoji ili nije poznata provoditeljima	Proces se provodi ad hoc i bez praćenja
2 – Osnovno	Osnovna, nepotpuna ili neažurna dokumentacija	Proces je neformalan i provodi se sporadično
3 – Uspostavljeno	Formalno odobrena i ažurirana dokumentacija	Proces je strukturiran i redovito se provodi
4 – Napredno	Potpuna i ažurna dokumentacija, uz manje iznimke	Kontrola je potpuno implementirana, uz praćenje i izvještavanje
5 – Optimizirano	Kontinuirano poboljšavanje i minimalne iznimke	Napredno praćenje, kontinuirano poboljšavanje i minimalne iznimke

Ocjena kontrole određuje se kao aritmetička sredina ocjene dokumentacije kontrole i ocjene implementacije kontrole.



Svaka kontrola ima postavljen minimalni bodovni prag ocjene koji mora biti ispunjen kako bi se smatrala zadovoljenom.



Za prolazak podmjere nije dovoljno ispuniti samo pojedinačne bodovne pragove ocjena kontrola, već prosječna ocjena svih kontrola također mora zadovoljiti unaprijed definirani ukupni bodovni prag.

Primjer – Revizija i ocjenjivanje kontrola te podmjera

Prilog B – Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima

Mjera 1 – Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima

Cilj: Cilj mjere je osigurati da osobe odgovorne za upravljanje mjerama iz članka 29. Zakona (u daljnjem tekstu: osobe odgovorne za upravljanje mjerama) prepoznaju kibernetičku sigurnost kao ključni aspekt poslovanja subjekta i aktivno sudjeluju u upravljanju kibernetičkom sigurnošću i poboljšanju razine kibernetičke sigurnosti u subjektu kroz integraciju kibernetičke sigurnosti u strateške planove i odluke o poslovanju subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

1.1. definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.

tbl 1.	RAZINE MJERE		
KONTROLA	OSNOVNA	SREDNJA	NAPREDNA
POL-001	≥3	≥4	≥4
ORG-001	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	> 3.5	≥ 4.0

Prilog C – Katalog kontrola

POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike

Ova kontrola osigurava da subjekt ima formalno usvojen strateški akt kibernetičke sigurnosne politike, odobren od strane upravljačkog tijela. Strateški akt predstavlja temelj za organizacijske aktivnosti subjekta u kibernetičkoj sigurnosti i daje okvir za definiranje ključnih ciljeva, mjera upravljanja rizicima, organizacijskih struktura te raspodjele uloga, odgovornosti, ovlasti i obveza, pri čemu jasno definirani ciljevi kibernetičke sigurnosti i otpornosti imaju ključnu ulogu u osiguravanju učinkovitosti mjera zaštite, omogućujući usklađivanje sigurnosnih aktivnosti s poslovnim potrebama i okruženju subjekta te usmjeravanje napora prema prioritetnim rizicima. Subjekt je obavezan najmanje jednom godišnje procjenjivati djelotvornost mjera te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.

U procesu provjere provjerava se postoji li dokument koji je formalno usvojen od strane upravljačkog tijela kao i jesu li svi ključni dionici informirani o njegovom sadržaju. Provjerava se pokriva li dokument ključne aspekte kao što su ciljevi, mjere i raspodjela odgovornosti i ovlasti te je li ažuriran prema potrebi nakon što je najmanje jednom tijekom tekuće godine prethodno provedena procjena djelotvornosti mjera. Na taj način se osigurava da strateški akt ostaje relevantan i prilagođen promjenjivim sigurnosnim izazovima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Strateški akt ne postoji.
2	Strateški akt je u pripremi i sadrži sve osnovne elemente, ali nije formalno usvojen od strane upravljačkog tijela.
3	Strateški akt je dokumentiran, sadrži sve osnovne elemente i formalno je usvojen od strane upravljačkog tijela.
4	Strateški akt je dokumentiran, sadrži sve osnovne elemente, formalno usvojen od strane upravljačkog tijela i implementiran u poslovne procese subjekta, uzimajući u obzir poslovne prioritete subjekta.
5	Strateški akt je dokumentiran, sadrži sve osnovne elemente, formalno je usvojen od strane upravljačkog tijela i implementiran u poslovne procese subjekta te ažuriran po potrebi kao i po provedbi procjene djelotvornosti mjera koja se provodi najmanje jednom tijekom tekuće godine.

Ako je prosjek i prolazi čak i kad forma

Izvor: <https://www.zsis.hr/>

Izvještavanje

Struktura Izvješća

U svrhu standardizacije i unaprjeđenja procesa izvještavanja o provedenim revizijama kibernetičke sigurnosti, propisuje se obvezni sadržaj i struktura izvješća o provedenoj reviziji kibernetičke sigurnosti. Cilj je osigurati konzistentnost, jasnoću i sveobuhvatnost informacija koje su ključne za procjenu stanja kibernetičke sigurnosti unutar subjekta.

Izvor: <https://www.zsis.hr/>

Uvod s opisom ciljeva i opsega revizije

Detaljan prikaz nalaza po mjerama

Potpis revizora



Naslovnica s osnovnim informacijama

Sažetak ključnih pronalazaka i preporuka

Zaključak

Prilozi s relevantnim dokazima

Primjer izgleda detaljnog prikaza kontrole:

Naziv kontrole: POL-001 - Postojanje strateškog akta kibernetičke sigurnosne politike

Opis kontrole: Ova kontrola osigurava da subjekt ima formalno usvojen strateški akt kibernetičke sigurnosne politike, odobren od strane upravljačkog tijela. Ovaj dokument definira ključne principe, ciljeve i smjernice za upravljanje kibernetičkom sigurnošću, čime postavlja temelj za učinkovitu zaštitu resursa i podataka.

Ocjena kontrole: 3.

Nalazi: Subjekt ima formalno izrađen strateški akt kibernetičke sigurnosne politike, koji je odobren od strane upravljačkog tijela. Dokument pokriva većinu ključnih područja kibernetičke sigurnosti, uključujući upravljanje rizicima, zaštitu podataka i odgovor na incidente. Međutim, tijekom revizije uočeno je sljedeće:



Dokument nije ažuriran posljednje dvije godine, iako je politika formalno definirala da se revizija treba provoditi godišnje.

Politika ne uključuje specifične smjernice za sigurnost udaljenog rada, što je postalo ključno u trenutnim operativnim uvjetima.

Nisu dostupni zapisi o formalnoj distribuciji i obuci zaposlenika u vezi s ovim dokumentom.

Uzrok/ci nesukladnosti:

Nedostatak resursa ili neadekvatan nadzor nad provođenjem redovitih revizija dokumenta.

Politika nije ažurirana kako bi se prilagodila novim radnim uvjetima, poput sve većeg udjela udaljenog rada.

Nedostatak formalne distribucije: Procedura za obavješćavanje zaposlenika o sadržaju i važnosti dokumenta nije dovoljno jasno definirana.

Posljedice nesukladnosti:

Zastarjeli strateški akt ne odražava trenutne prijetnje i operativne izazove, što može rezultirati slabijim odgovorom na sigurnosne incidente.

Neinformirani zaposlenici povećavaju rizik od nesvjesnih sigurnosnih propusta.

Usvojiti proceduru za redovitu reviziju dokumenta i definirati odgovornu osobu ili tim koji će pratiti provedbu te obavješćavati upravljačko tijelo o statusu.



Uvesti formalni proces distribucije dokumenta i obuke zaposlenika kako bi se osiguralo da svi zaposleni razumiju ključne smjernice i postupke definirane u politici.

Izraditi zapisnike o distribuciji i obukama kako bi se mogla dokumentirati usklađenost sa zahtjevima politike.

Dokazi i reference:

Pregled kibernetičke sigurnosne politike (verzija iz 2021.).

Izvještaji upravljačkog tijela o odobravanju politike.

Interni zapisnici o distribuciji politika i obukama zaposlenika (nisu pronađeni za predmetni dokument).

Za svaki nalaz revizor mora opisati:

- kontrolu
- ocjenu
- nalaz
- uzrok
- posljedicu
- dokaz
- preporuku

Nalaz mora biti jasan, logično strukturiran i usmjeren na pružanje korisnih informacija koje subjekt može odmah primijeniti za unapređenje svog sigurnosnog sustava.

Izvor: <https://www.zsis.hr/>



O predavaču



Marko Žalac



Deloitte



091 2370 091



mzalac@deloittece.com

