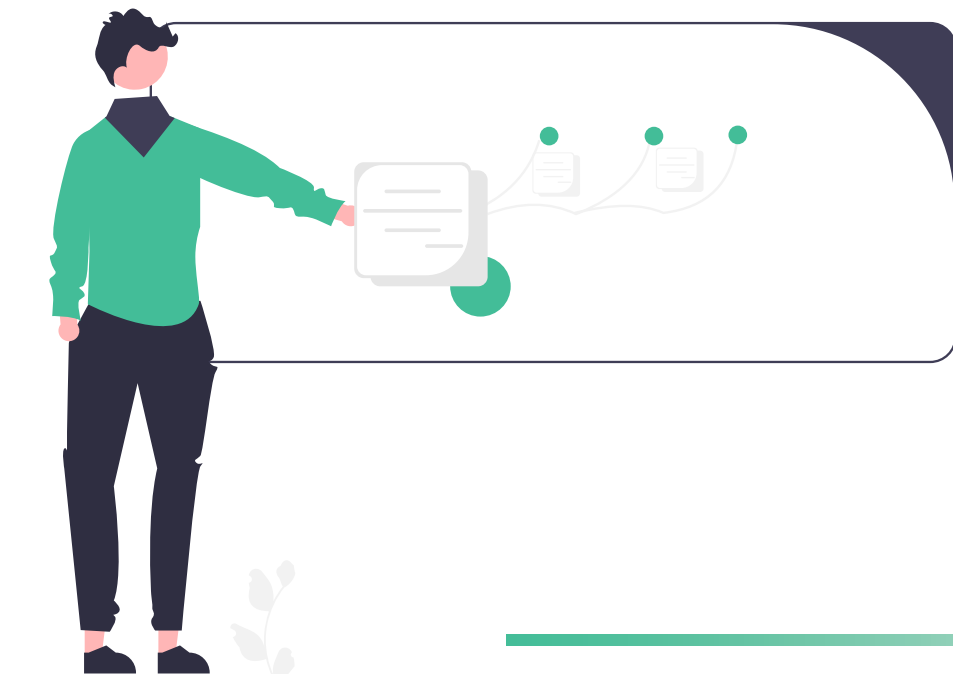


Zakon o informacijski varnosti

**Pot do novega zakona, ključne spremembe
in določbe v povezavi z revidiranjem**

dr. Uroš Svete, direktor urada
Matjaž Mravljak, direktor inšpekcije

Gradivo je last Slovenskega inštituta za revizijo in je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.



Sprejet: 23. 5. 2025
Objavljen: 4. 6. 2025
Začetek veljave: 19. 6. 2025

Direktiva NIS 2: rok za prenos 17. 10. 2025

Zakon o informacijski varnosti (ZInfV-1)

Uradni list RS, št. 40/25

Proces sprejema ZInfV-1 (pot do zakona)

- 14. december 2022 – **sprejem NIS 2 direktive**
- 20. februar 2023 – **delovna skupina URSIV za pripravo zakona**
- **predstavitev delovnega osnutka zakona** ministrstvu in vladnim službam ter Koordinacijski skupini za kibernetско varnost
- 16. februar 2024 – **prvi krog javne obravnave zakona**
- 15. maj 2024 – **drugi krog javne obravnave zakona**
- 15. maj 2024 – **prvi krog medresorskega usklajevanja**
- 4. september 2024 – **drugi krog medresorskega usklajevanja**
- 21. november 2024 – **delovna skupina za pripravo platforme za prigrasitev incidentov**
- 23. december 2024 – **tretji krog medresorskega usklajevanja**
- 28. marec 2025 – **zakon URSIV vložil v obravnavo na Vlado RS**

ZInfV-1 (novosti in nacionalne posebnosti)

- zakon je nadomestil ZInfV in **posegel v ZEKom-2**
- vzpostavil je dve kategoriji zavezancev: bistveni in pomembni subjekti
- razširil je obseg zavezancev (področje uporabe) – **Priloga 1**: visoko kritični sektorji, **Priloga 2**: kritični sektorji in **Priloga 3**: drugi subjekti javne uprave na državni ravni
- URSIV ostaja pristojni nacionalni organ
- vlada določi skupine CSIRT
- določil je enotno kontaktno točko in organ za obvladovanje kriz
- določil je naloge Nacionalnega koordinacijskega centra za kibernetisko varnost in Nacionalnega kibernetiskega vozlišča

ZInfV-1 (novosti in nacionalne posebnosti)

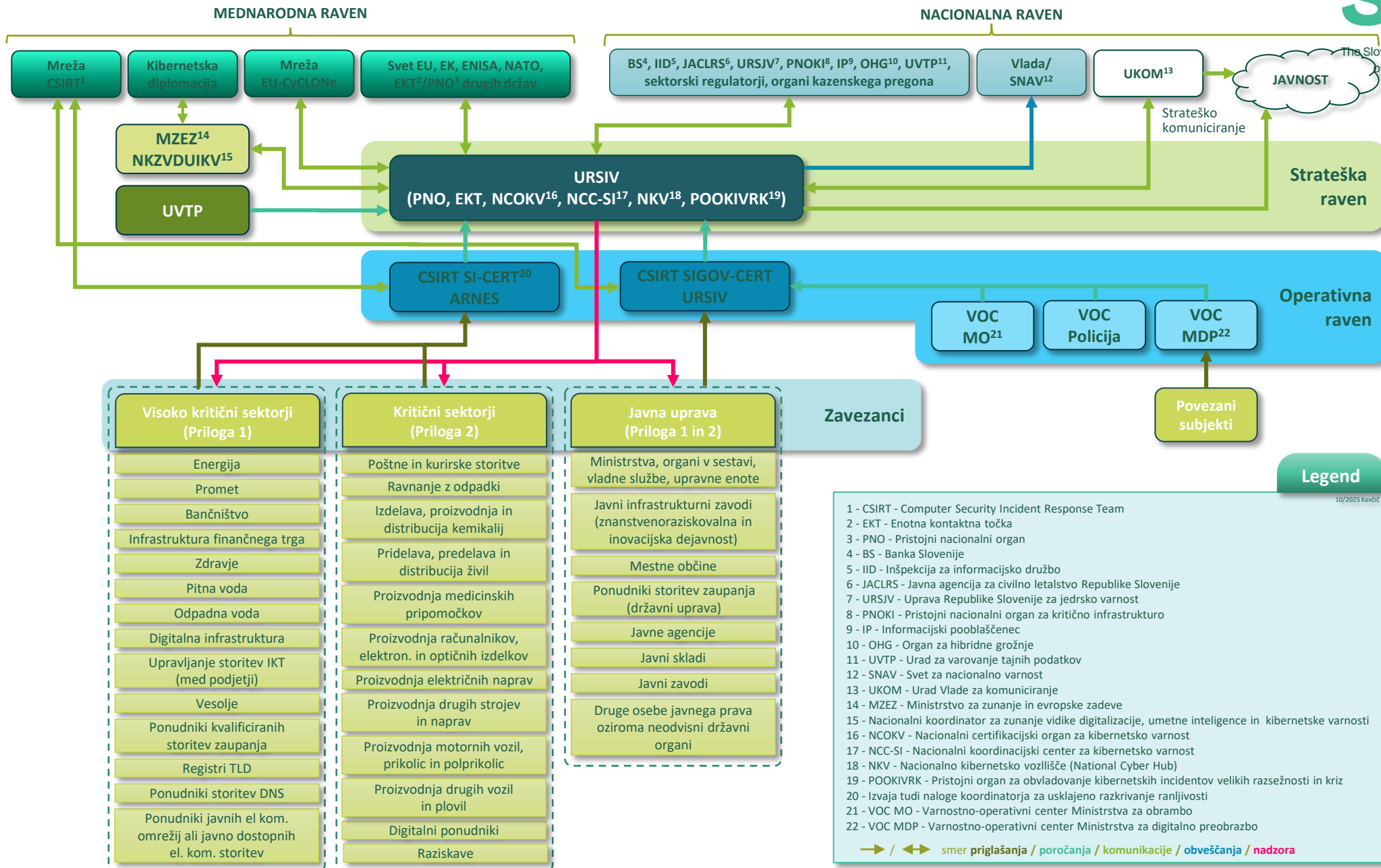
- vzpostavil je koordinatorja za usklajeno razkrivanje ranljivosti
- povečal je obveznosti – strožje zahteve za prijave incidentov in zahteve za izvajanje varnostnih ukrepov
- predpisal je izvedbo samo-registracije bistvenih in pomembnih subjektov
- ohranil je možnost dodatne določitve zavezancev (vlada z odločbo)
- usklajen je s sistemskim zakonom za področje kritične infrastrukture
- razširil je strategijo kibernetске varnosti
- ohranil je nadzorni organ – Inšpekcija za informacijsko varnost v URSIV

ZInfV-1 (novosti in nacionalne posebnosti)

- predpisal je višje globe za zavezance, ki ne izpolnjujejo predpisanih varnostnih zahtev in ne prijavljajo pomembnih incidentov
- omogočil je več sodelovanja med državami članicami EU ob resnih incidentih in izmenjavo informacij ter najboljših praks
- vzpostavil je nacionalni okvir za obvladovanje kibernetских kriz (nacionalni načrt, EU-CyCLONe)
- določil je odgovornost odgovornih oseb zavezancev (poslovodstva) in predpisal obvezno izobraževanje odgovornih oseb zavezancev
- omogočil je izvedbo preverjanja preteklosti zaposlenih pri zavezancih in pogodbenih partnerjih (delovna mesta, ključna za izvajanje storitev)

ZInfV-1 (novosti in nacionalne posebnosti)

- ohranil je nacionalno pristojnost vrednotenja incidentov, določitev ocene ogroženosti in ukrepanje
- razširil je nacionalne določbe o kibernetiski obrambi
- določil je večjo odgovornost ponudnikov digitalnih storitev za zagotavljanje varnosti svojih sistemov ter uvedel mehanizme za ocenjevanje skladnosti
- določil je obvezno izvedbo ocene skladnosti za **bistvene subjekte** (najmanj na 2 leti)
- določil je obvezno izvedbo samoocene skladnosti za **pomembne subjekte** (najmanj na 2 leti)

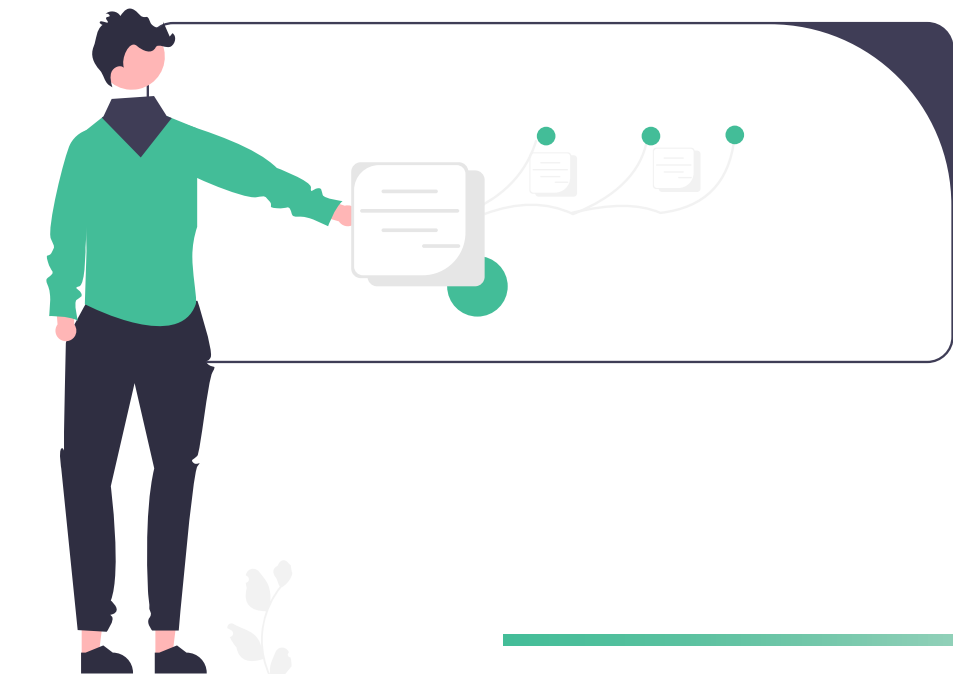


Pomembni mejniki ZInfV-1

Zinfv-1 določa prehodno obdobje za uskladitev z zakonom :

DOKUMENTACIJA IN VARNOSTNI UKREPI

- **zavezanci iz ZInfV** (IBS, ODU in PDS) imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 6. 2026**
- **bistveni in pomembni subjekti** (novi) imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 12. 2026**
- **operaterji po ZEKom-2** (ki so zavezanci) imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 6. 2026**



Določbe ZInfV-1 v povezavi z revizijo in revidiranjem

- **opredelitev pojmov** (revizor, notranji revizor, veččak)
- **izvajanje ocene in samoocene skladnosti** zavezancev
- **ukrepi inšpektorja pri nadzoru** bistvenih in pomembnih subjektov
- **izbira revizorja in stroški revizij**

- **Revizor informacijskih sistemov** je oseba z ustreznim revizijskim znanjem, ki je preizkušeni revizor informacijskih sistemov, ki je pridobil strokovni naziv pri Slovenskem inštitutu za revizijo ter je **vpisan v njegov register aktivnih preizkušenih revizorjev informacijskih sistemov**.
- **Notranji revizor** je preizkušeni notranji revizor, ki je pridobil strokovni naziv pri Slovenskem inštitutu za revizijo in je **vpisan v njegov register aktivnih preizkušenih notranjih revizorjev**.
- **Veščak za informacijsko varnost** je posameznik ali organizacija, ki ima **izkazano poglobljeno strokovno znanje na področju informacijsko komunikacijskih tehnologij**, katerega ali katere delo revizor uporabi kot strokovno pomoč revizorju pri pridobivanju zadostnih in ustreznih revizijskih dokazov.

Izvajanje ocene skladnosti bistvenih subjektov

Bistveni subjekti morajo izvajati oceno skladnosti **najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta.**

- izvaja **revizor informacijskih sistemov kot revizijo skladnosti** s predpisi s področja informacijske varnosti
- izvaja **notranji revizor v okviru notranje revizije**, ki se izvaja na podlagi drugih predpisov in vključuje tudi področje informacijske varnosti iz ZInfV-1 **v sodelovanju z veščakom za informacijsko tehnologijo**

Izvajanje samoocene skladnosti pomembnih subjektov

Pomembni subjekti morajo izvajati samooceno skladnosti **najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta.**

Dokumentirano se preveri skladnost z varnostno dokumentacijo in izvajanje ukrepov za obvladovanje tveganj za kibernetско varnost.

- izvaja jo lahko **ustrezno usposobljena oseba** pri pomembnem subjektu
- izvaja jo lahko **revizor informacijskih sistemov**
- izvaja jo lahko **notranji revizor v okviru notranje revizije**

Ukrepi inšpektorja pri nadzoru bistvenih subjektov

Revizije skladnosti po odredbi inšpektorja lahko izvajajo le revizorji informacijskih sistemov.

Zavezanec za izvedbo revizije skladnosti, ki jo odredi inšpektor, **izbere revizorja informacijskih sistemov**. O svoji izbiri in o začetku postopka revizije skladnosti obvesti inšpektorja v roku 30 dni od podane zahteve inšpektorja.

- inšpektor lahko odredi izvedbo **redne in ciljno usmerjene revizije skladnosti** s predpisi s področja informacijske in kibernetske varnosti.
- Inšpektor lahko odredi izvedbo **izredne revizije skladnosti**, ko je to utemeljeno zaradi pomembnega incidenta ali očitne kršitve ZInfV-1.
- Inšpektor lahko **odredi, da zavezanec v razumnem roku izvede priporočila**, dana na podlagi izvedene revizije skladnosti.

Ukrepi inšpektorja pri nadzoru pomembnih subjektov

Revizije skladnosti po odredbi inšpektorja lahko izvajajo le revizorji informacijskih sistemov.

Zavezanec za izvedbo ciljno usmerjene revizije skladnosti, ki jo odredi inšpektor, **izbere revizorja informacijskih sistemov**. O svoji izbiri in o začetku postopka revizije skladnosti obvesti inšpektorja v roku 30 dni od podane zahteve inšpektorja.

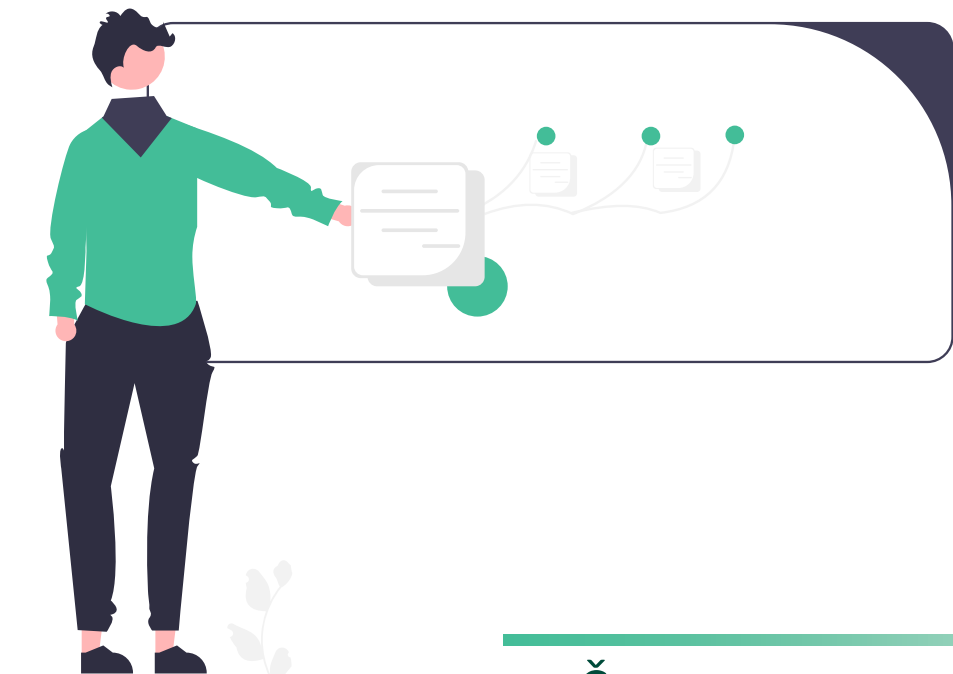
- inšpektor lahko **odredi izvedbo ciljno usmerjene revizije skladnosti** s predpisi s področja informacijske in kibernetske varnosti.
- Inšpektor lahko **odredi, da zavezanec v razumnem roku izvede priporočila**, dana na podlagi izvedene ciljno usmerjene revizije skladnosti.

Ukrepi inšpektorja pri nadzoru po Uredbi 2019/881/EU

Revizije skladnosti po odredbi inšpektorja lahko izvajajo le revizorji informacijskih sistemov.

Zavezanec za izvedbo ciljno usmerjene revizije skladnosti, ki jo odredi inšpektor, **izbere revizorja informacijskih sistemov**. O svoji izbiri in o začetku postopka revizije skladnosti obvesti inšpektorja v roku 30 dni od podane zahteve inšpektorja.

- Inšpektor lahko odredi izvedbo **ciljno usmerjene revizije skladnosti** z Uredbo 2019/881/EU.
- Inšpektor lahko odredi, da zavezanec v razumnem roku **izvede priporočila, dana na podlagi ciljno usmerjene revizije skladnosti**.



Izbira revizorja informacijskih sistemov in stroški revizije

- Če **zavezanec ne izbere** revizorja IS v skladu z določbami 49. člena ZInfV-1, **revizorja IS s sklepom določi inšpektor.**
- Revizor IS zaposlen pri zavezancu - v kolikor **lahko zagotovi nepristranskost in neodvisnost revizorja IS.**
- **Stroške redne, izredne in ciljno usmerjene revizije skladnosti, ki jo opravi revizor IS, krije zavezanec,** razen v ustrezno utemeljenih primerih, ko inšpektor (s sklepom) odloči drugače.



REPUBLIKA SLOVENIJA
**URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST**



dr. Uroš Svete, direktor URSIV

Matjaž Mravljak, direktor Inšpekcije za informacijsko varnost

gp.uiv@gov.si

www.uiv.gov.si

X: [@URSIV_Slovenia](#)