

# Sodelovanje med preizkušnim notranjim revizorjem in preizkušnim revizorjem informacijskih sistemov

---

Matic Štern

## 33. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov

---

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.

# Kdo sem in kaj počnem?

- Preteklih 8 let **notranji revizor** v Telekomu Slovenije (TS); v timu notranjih revizorjev pretežno izvajam notranje revizije in svetovalne posle, ki so bolj povezani s področjem strategije, upravljanja in varnosti informacijsko-komunikacijskih tehnologij. Kmalu po pridružitvi timu notranjih revizorjev sem pridobil licenco CISA, letos pa tudi **PRIS**.
- Pred tem sem več kot 10 let delal v IT – od systemske in omrežne administracije, upravljanja baz podatkov, razvoja informacijskih rešitev (še pred prihodom v TS) ter sodeloval pri vodenju večjih IT projektov, predvsem na področju IT analize, testiranja, po-projektne podpore produkciji, vzpostavitvi in izboljšavah nekaterih IT procesov ...
- Rad pridobivam ter delim izkušnje in znanje.

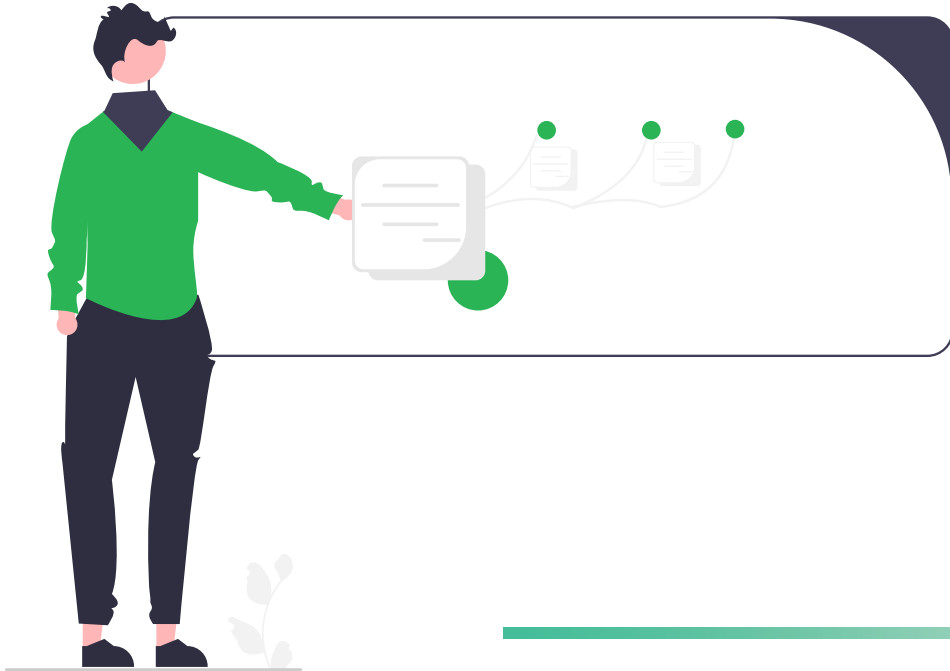


Slika ustvarjena z UI.

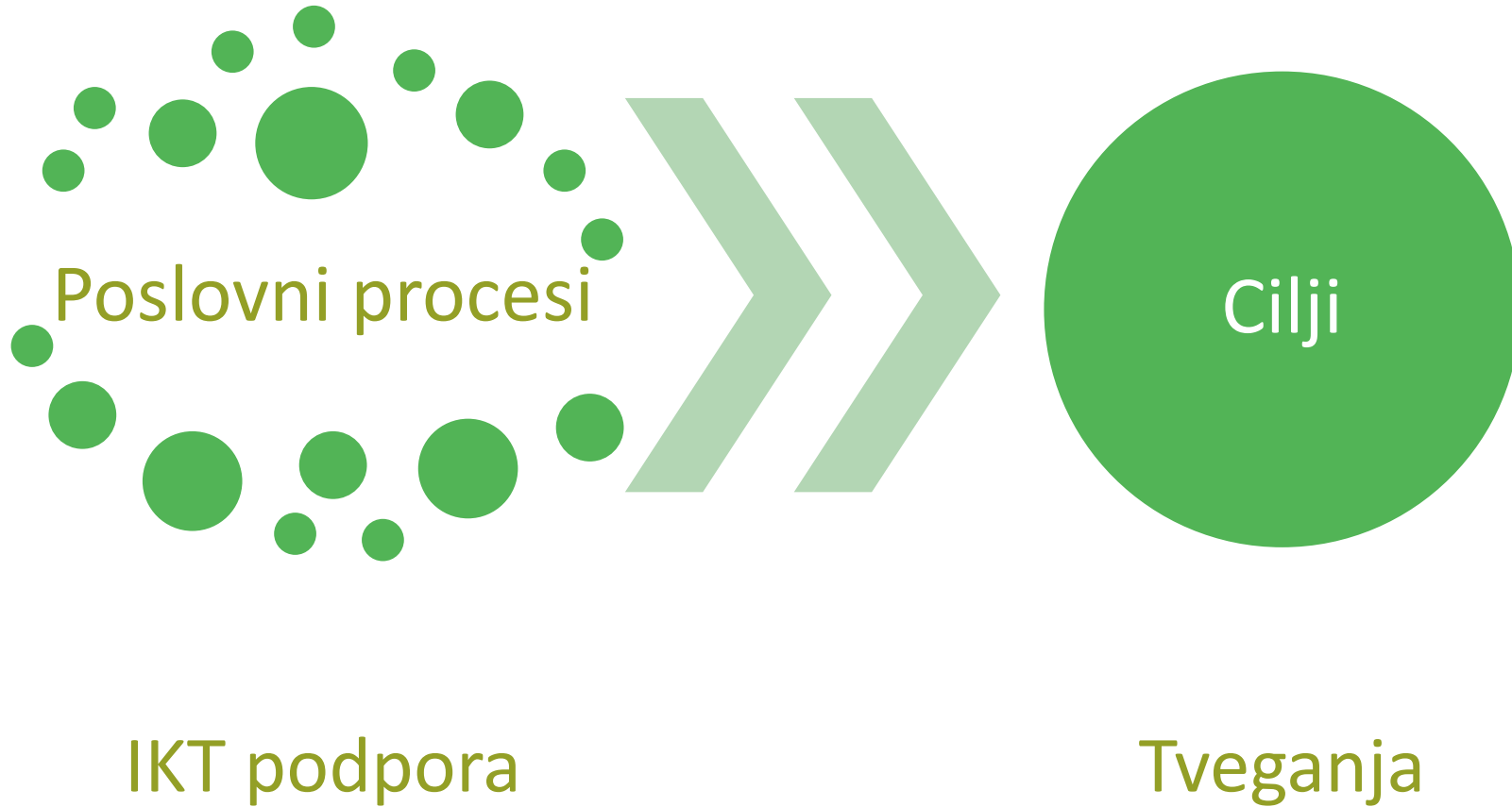


## Aktivni PRIS

**Preizkušeni revizorji informacijskih sistemov**  
(Qualified Information Systems Auditors)



Zakaj je sodelovanje med  
PNR in PRIS pomembno?



## USPEŠNOST

Doseganje cilja.

## UČINKOVITOST

Izvedba aktivnosti za doseganje cilja na optimalen način (vidik porabe virov).

*Informacijski sistemi: **varnost** (zaupanje) in **uporabna/poslovna vrednost** (korist).*

## KOMPLEKSNOŠT POSLOVNEGA OKOLJA

- Poslovni model
- Panoga
- Konkurenca
- Predpisi/regulacija



- Poslovni procesi

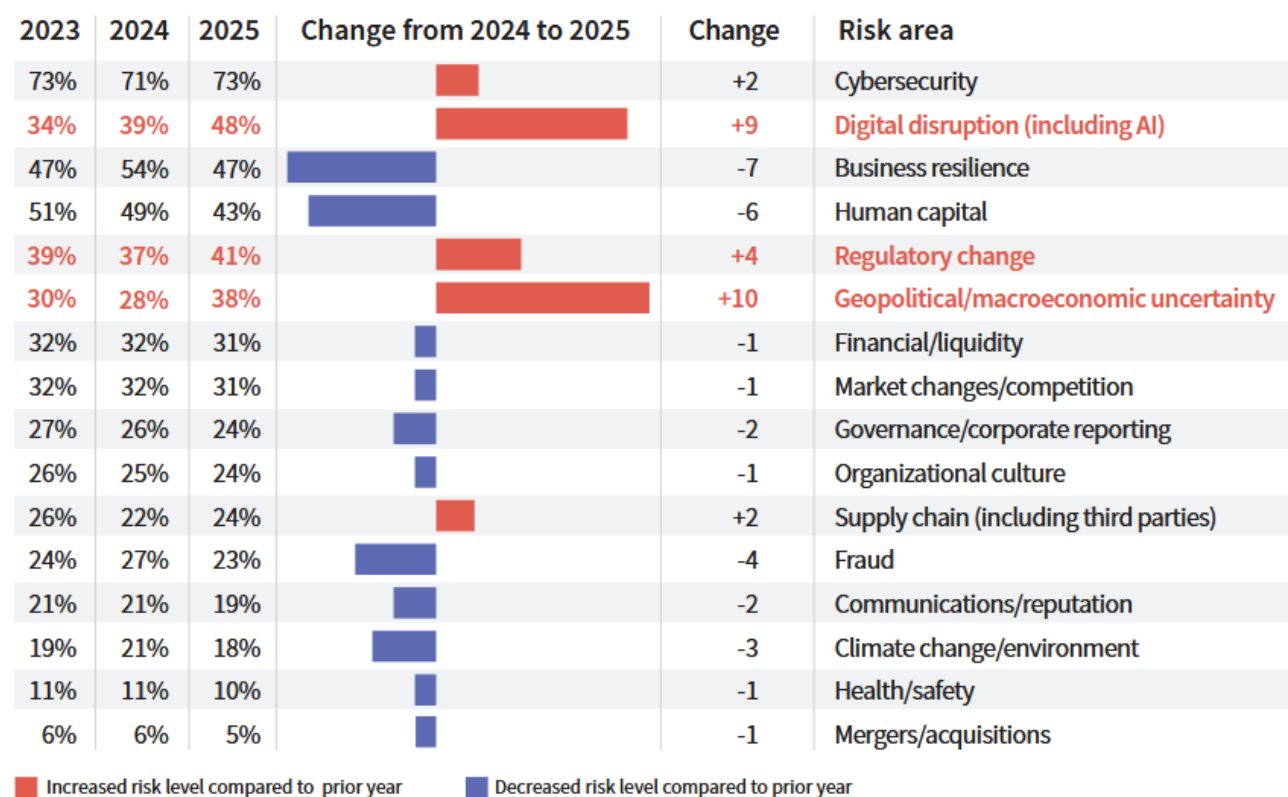
## KOMPLEKSNOŠT IKT

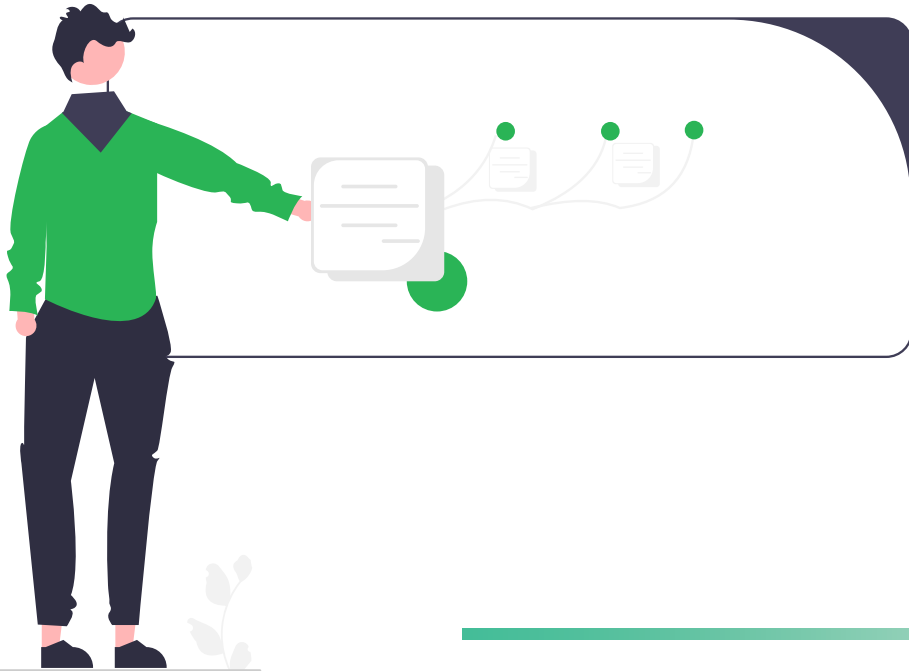
- Hibridna IKT okolja („on-prem“ in „cloud“)
- Hiter razvoj tehnologije (UI, „shadow IT“, ...)
- Odvisnost od dobaviteljev
- Kibernetiska tveganja
- Izvedba zahtev predpisov v praksi

## GLOBAL – RISK LEVELS

### Exhibit 1.2. Global – Risk Level Trend

Survey question: What are the Top 5 risks your organization currently faces? (Choose 5.)





# PNR in PRIS



Strokovnost smo razvili in pridobili v izobraževalnem programu, ki ga izvaja SIR za pridobitev strokovnega naziva, ter z izkušnjami pri izvajanju notranjih revizij. *Aktivni preizkušeni notranji revizorji* smo tisti, ki smo se pisno zavezali, da bomo pri svojem delu spoštovali **Kodeks poklicne etike notranjih revizorjev**, delovali v skladu s pravili stroke, razvrščenimi v **Hierarhiji pravil notranjega revidiranja**, ter se **nenehno strokovno izobraževali**, da bomo širili svoje znanje, veščine in druge sposobnosti.

<https://www.si-revizija.si/notranji-revizorji/aktivni-pnr>

Osredotoča se na širši poslovno-organizacijski kontekst, razumevanje ciljev organizacije in obvladovanje tveganj pri doseganju teh ciljev ter (skladnost), uspešnost in učinkovitost poslovnih procesov.

**Revizor informacijskih sistemov** z veljavno licenco Slovenskega inštituta za revizijo (SIR) je *strokovno usposobljen za izvajanje revizijskega pregleda ter izpolnjuje najvišje strokovne in etične standarde*. Pri izvajanju revizijskega pregleda informacijskega sistema upošteva veljavno zakonodajo in standarde revidiranja, sledi uveljavljenim mednarodnim postopkom organizacije ISACA, upošteva razširjene in mednarodno sprejete standarde organizacije ISO in dobre prakse ter na podlagi teh poda priporočila za izboljšanje na področjih, za katera je opravil revizijski pregled.

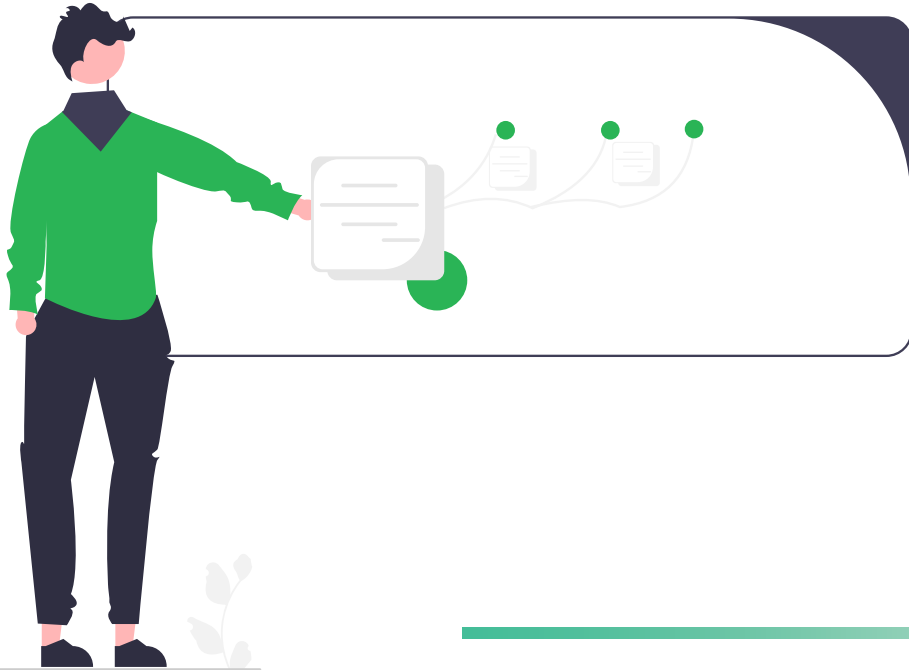
<https://www.si-revizija.si/revizorji-is/predstavitev>

Pozornost daje pristopom za obvladovanje tveganj ustreznosti in varnosti informacijskih sistemov, pri čemer so pomembni tehnična globina in specifična znanja o delovanju informacijskih sistemov.

## Zakaj (aktivna) PNR in PRIS?

---

- Usposobljenost preko strukturiranega izobraževanja.
- Poznavanje značilnosti poslovnega in regulatornega okolja na področju Republike Slovenije.
- Izpolnjevanje etičnih standardov in pravil stroke.
- Vzdrževanje strokovnih kompetenc.
- Izmenjava izkušenj, znanj in veščin med nosilci različnih strokovnih nazivov na SiR.



# Sodelovanje PNR in PRIS

- **Soizvajanje**
- **Sodelovanje** PRIS-a kot specializiranega strokovnjaka
- Izvedba **ločenih revizij** istega področja
- **Samostojna notranja revizija**, ki jo izvede **PRIS**

Če se posel vodi kot notranja revizija, mora biti vzpostavljen osnovni okvir GIAS.

- **SOIZVAJANJE** notranje revizije – skupna revizija

Vsi koraki se izvedejo v skupnem sodelovanju.

- **SODELOVANJE** PRIS-a kot specializiranega strokovnjaka

PNR vodi notranjo revizijo, dogovorjene sklope, kjer je potreben podrobnejši tehnični pristop, izvede PRIS.

- **IZVEDBA LOČENIH REVIZIJ istega področja**

Vzajemna izmenjava ugotovitev.

Običajno eno poročilo (notranja revizija), lahko tudi ločeni.

- **Samostojna NOTRANJA REVIZIJA, ki jo izvede PRIS**

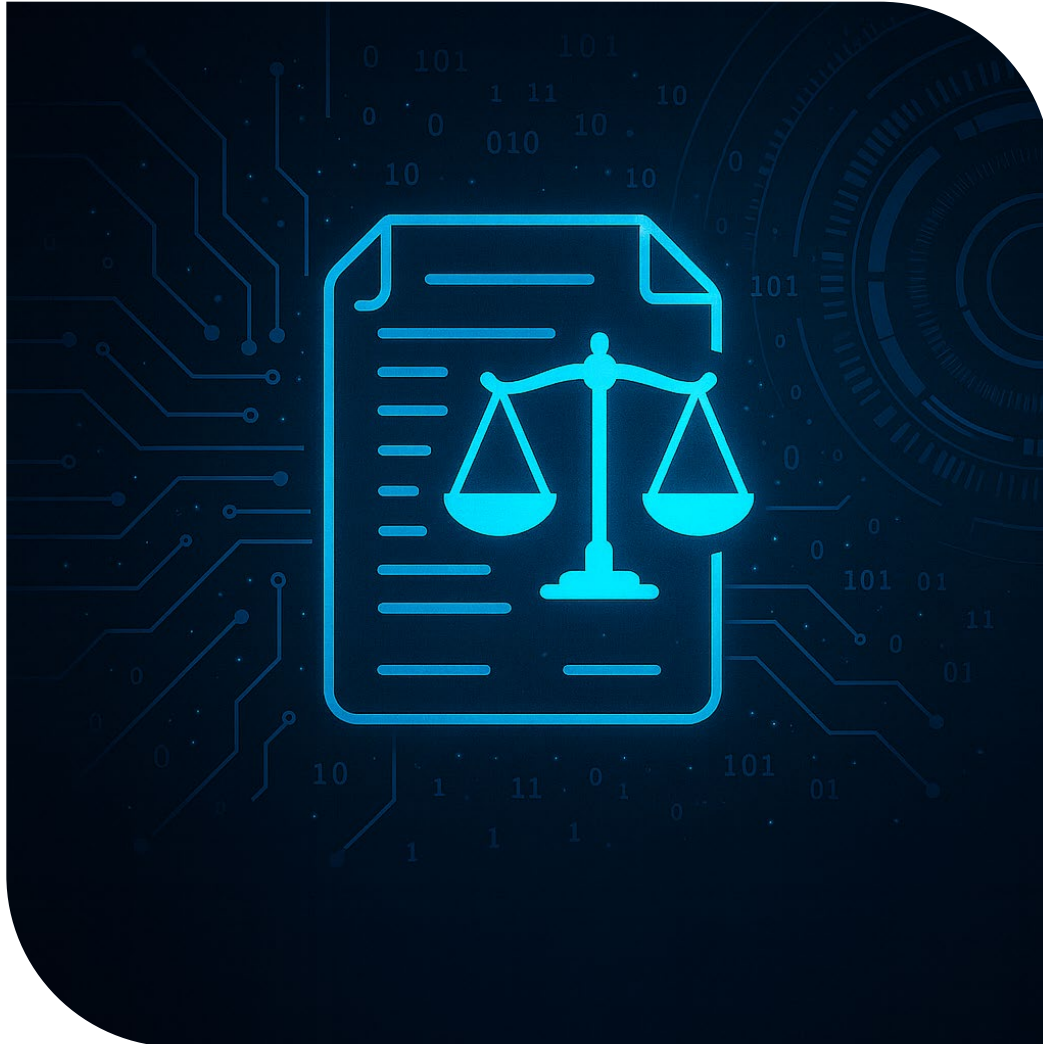
Celoten posel izvede PRIS, PNR usmerja z metodološkega vidika in vidika skladnosti s pravili stroke notranjega revidiranja.

- PNR: usklajenost politik, postopkov in obvladovanja tveganj kibernetске varnosti glede na strateške cilje organizacije.
- PRIS: preverjanje vzpostavljenosti in delovanja kontrol informacijskih sistemov za obvladovanje kibernetских tveganj.



Slika ustvarjena z UI.

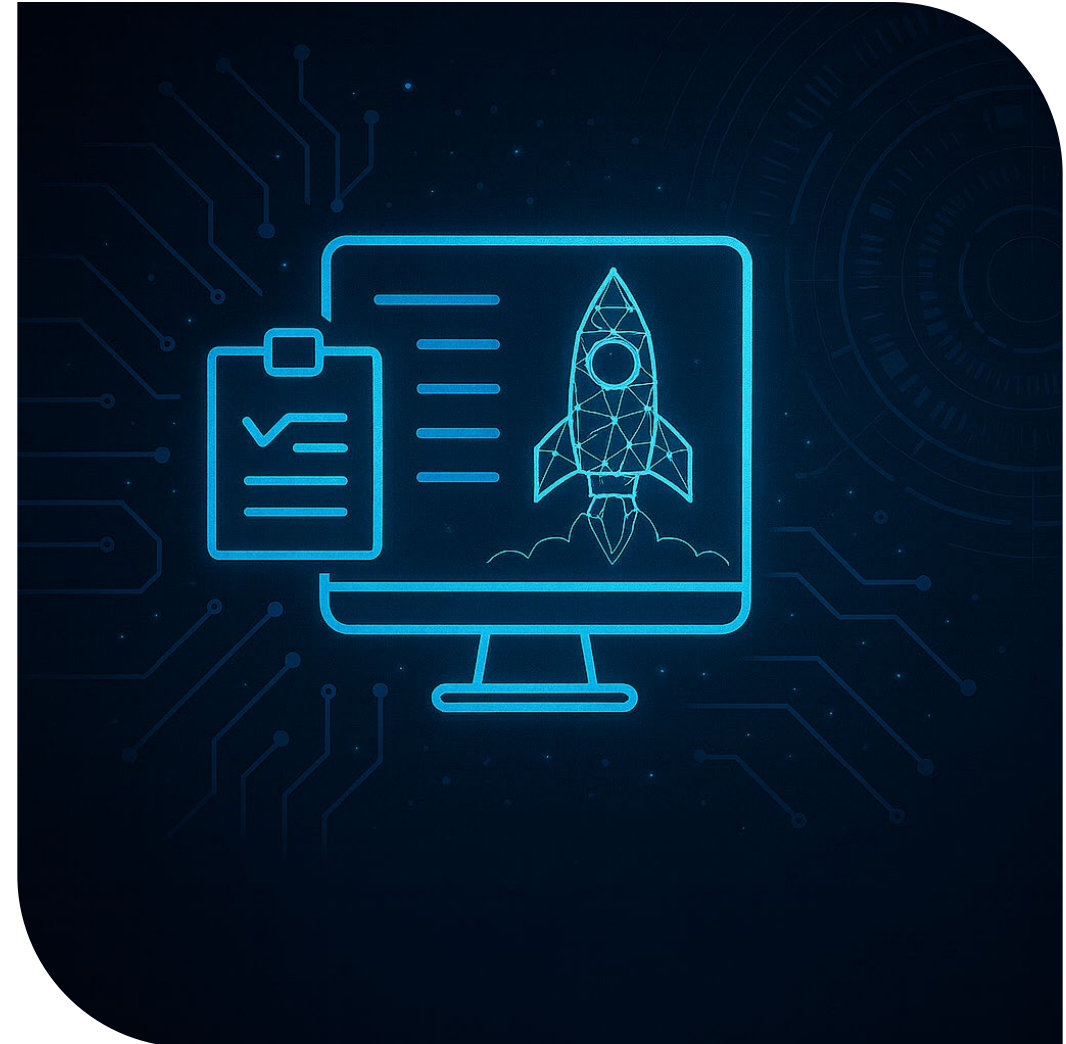




Slika ustvarjena z UI.

- PNR: primernost umeščenosti IT kontrol v procese, skladnost s predpisi in njihovo zasnovo.
- PRIS: testiranje delovanja IT kontrol, preverjanje uspešnosti, učinkovitosti, ustreznosti razvojnega pristopa in umeščenosti v arhitekturo IT okolja.

- PNR: projektni načrt, projektno vodenje, ekonomika projekta.
- PRIS: preverjanje ustreznosti pristopa tehnične izvedbe, ciljne arhitekture IKT okolja, primernosti izbranih IT rešitev, integriteta podatkov, implementacija kontrol zagotavljanja kibernetске varnosti.

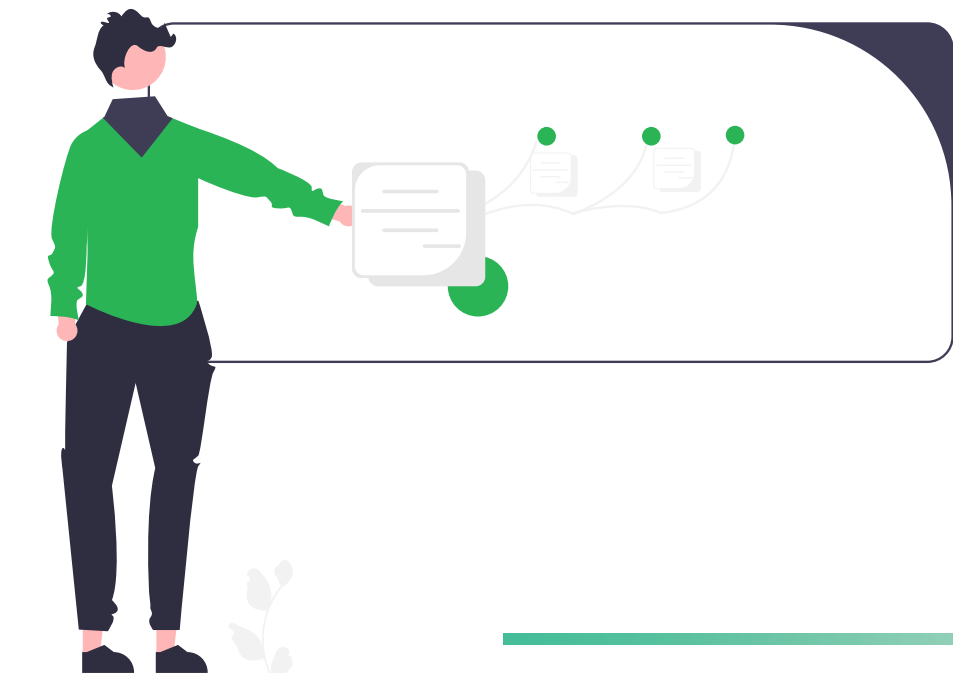


Slika ustvarjena z UI.



Slika ustvarjena z UI.

- PNR: pregled ustreznosti nabavnih postopkov in sklenjenih pogodb, spremljanje izvajanja storitev (SLA) in skladnost s predpisi.
- PRIS: preverjanje ustreznosti konfiguracije z vidika primernosti glede na potrebe, varnosti in zanesljivosti delovanja, primernost umestitve v arhitekturo.



# Značilnosti standardov obeh strok



## Globalni standardi notranjega revidiranja (Global Internal Audit Standards™)



<https://www.theiia.org/globalassets/site/standards/editable-versions/2023-7726-gui-global-ia-standards-esloveno-02-07-24.pdf>



[https://si-revizija.si/datoteke/revizorji-is/1584/itaf\\_v3\\_slovenscina.pdf](https://si-revizija.si/datoteke/revizorji-is/1584/itaf_v3_slovenscina.pdf)

- Izdajatelj: IIA.
- Izdani januarja 2024, v uporabi od januarja 2025 naprej.
- Vključeni v Hierarhijo pravil notranjega revidiranja.
- Spremembe v primerjavi z ISPPIA (iz 2017) neposredno ne vplivajo na sodelovanje med PNR in PRIS.
- PRIS, ki izvaja notranjo/-e revizijo/-e, naj se z njimi seznani.
- Podrobneje:
  - Področje II – Etika in strokovnost;
  - Področje V – Izvajanje storitev notranjega revidiranja.

- Integriteta
- Nepristranskost/objektivnost
- Zaupnost
- Strokovnost in usposobljenost
- Transparentnost poročanja



# Izvajanje notranjega revidiranja - podobnosti

GIAS	ITAF
13.2 Ocena tveganj posla	1202 Ocenjevanje tveganja pri načrtovanju
13.3 Cilji in obseg posla	1201 Načrtovanje posla
13.4 Sodila za ocenjevanje	1008 Merila
13.5 Viri posla	1201 Načrtovanje posla
13.6 Delovni program	1201 Načrtovanje posla 1203 Izvedba in nadzor
14.1 Zbiranje informacij za analize in ocene	1205 Dokazi
14.2 Analize in morebitne ugotovitve posla	1203 Izvedba in nadzor 1204 Pomembnost
14.6 Dokumentacija o poslu	1205 Dokazi 1203 Izvedba in nadzor
15.1 Končno sporočilo o poslu	1401 Poročanje
15.2 Potrjevanje uresničevanja priporočil ali načrtov ukrepanja	1402 Nadaljnja obravnava



# Izvajanje notranjega revidiranja – delno ujemanje

GIAS	ITAF	
13.1 Sporočilo o poslu	1201 Načrtovanje posla 1401 Poročanje	GIAS zahteva sprotno komuniciranje v okviru posla; ITAF komuniciranje formalizira v načrtu in končnem poročilu.
14.3 Vrednotenje ugotovitev	1203 Izvedba in nadzor 1204 Pomembnost 1205 Dokazi	ITAF eksplicitno ne zahteva ugotavljanja temeljnega vzroka.
14.4 Priporočila in načrti ukrepanja	1401 Poročanje	GIAS daje možnost med priporočili ali načrti ukrepanja vodstva.
14.5 Zaključki posla	1203 Izvedba in nadzor 1204 Pomembnost	GIAS zahteva pripravo zaključkov posla v smislu povzetka strokovne presoje o splošni bistvenosti zbirnih ugotovitev posla.

<https://www.theiia.org/globalassets/site/standards/editable-versions/2023-7726-gui-global-ia-standards-esloveno-02-07-24.pdf>

[https://si-revizija.si/datoteke/revizorji-is/1584/itaf\\_v3\\_slovenscina.pdf](https://si-revizija.si/datoteke/revizorji-is/1584/itaf_v3_slovenscina.pdf)

- Je obvezni del IPPF (poleg GIAS), uporaba je obvezna za storitve dajanja zagotovil. Presoja uporabe navedena v dokumentu, podrobnejše opredelitve v Uporabniškem priročniku Tematske zahteve za kibernetско varnost.
  - Tematska zahteva: [Cybersecurity Topical Requirement Slovenian](#)
  - Uporabniški priročnik: [Cybersecurity TR User Guide Slovenian](#)
- Objavljena 5. 2. 2025, obvezna uporaba v 12 mesecih od objave za notranje revizije, ki bodo vključevale to področje.

## UPRAVLJANJE (4 zahteve)

## OBVLADOVANJE TVEGANJ (6 zahtev)

## KONTROLE (7 zahtev)

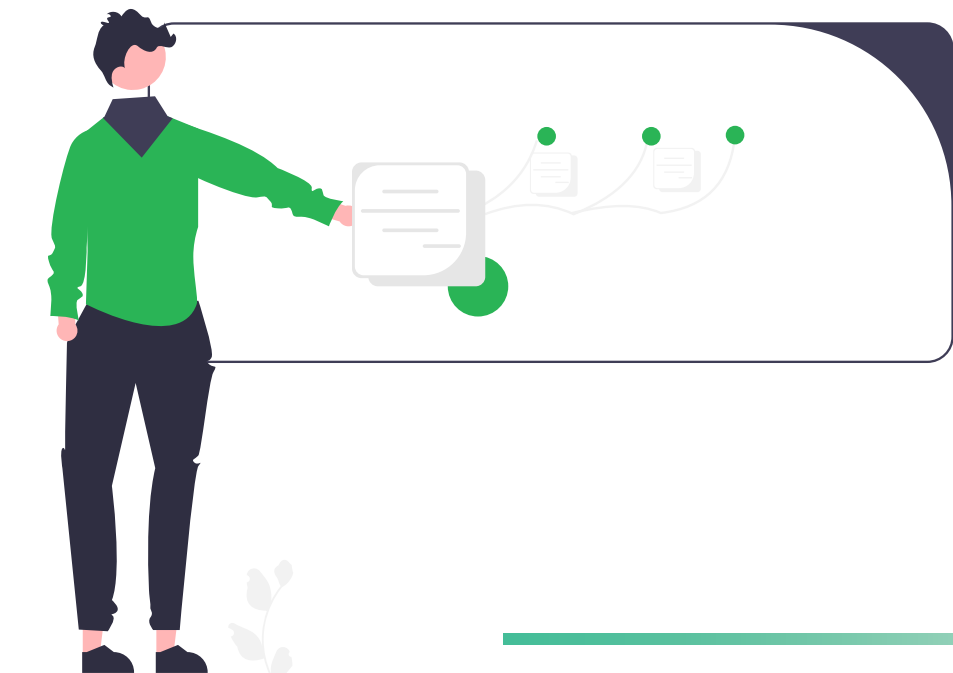
Zahteve kontrolnih procesov	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Vzpostavljen je proces, ki zagotavlja, da so vzpostavljene notranje kontrole in kontrole s strani dobaviteljev za zaščito zaupnosti, celovitosti in razpoložljivosti sistemov in podatkov organizacije. Kontrole se obdobjno ocenjujejo, da se ugotovi, ali delujejo na način, ki spodbuja doseganje organizacijskih ciljev kibernetške varnosti in pravočasno reševanje vprašanj.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

[https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity\\_tr\\_user\\_guide\\_slovenian.pdf](https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_tr_user_guide_slovenian.pdf)

## Pristopi sodelovanja

---

- Jasno opredeljene vloge in odgovornosti.
- Usklajena metodologija in terminologija.
- Skupna komunikacija z vodstvom.
- Stalno strokovno izpopolnjevanje.
- Vzajemno upoštevanje pravil stroke.



Uspešno in učinkovito  
doseganje ciljev organizacije,  
boljše obvladovanje tveganj in  
izboljšana kibernetika  
odpornost.

Komplementarnost pri obvladovanju tveganj v poslovnem okolju:  
PNR prispeva širino razumevanja poslovnega modela, strateških  
ciljev in procesov, PRIS pa tehnično poglobljeno presojo  
primernosti in varnosti informacijskih sistemov.

# Hvala za pozornost!

