Notranja revizija v javnem sektorju – 20 let pozneje
Konferenca Urada za nadzor proračuna

REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

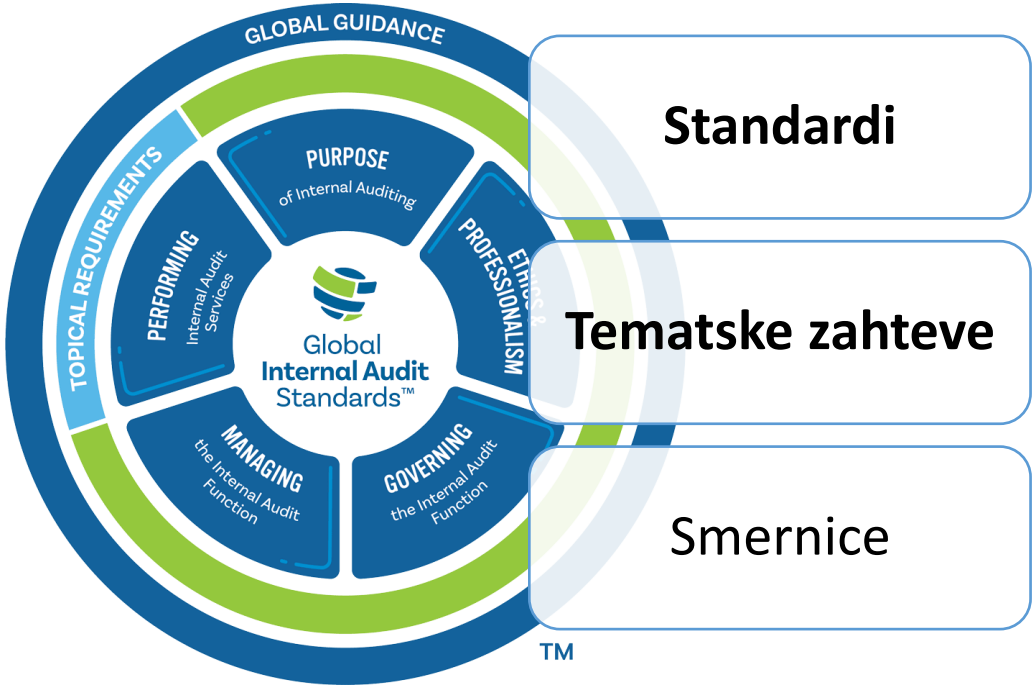
NIS2 in tematska Zahteva za kibernetsko varnost

Kaj čaka notranje revizorje 2025

Jaka Kosmač, univ. dipl. prav., državni revizor, CISA
Mag. Maja Hmelak, CIA, PNR, PRIS, CISA

30 1994 2024 RS RS

Kaj so tematske zahteve in kako predstavljajo del IPPF



Standardi

Tematske zahteve

Smernice

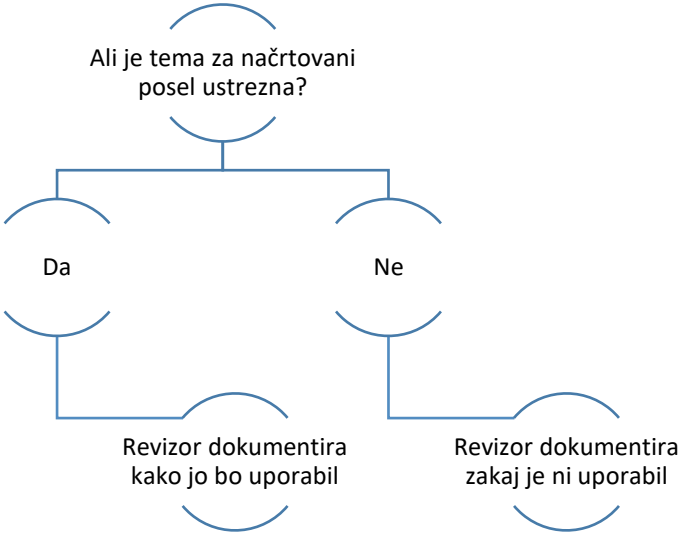
- Doslednost
- Strokovnost — Osnovna **merila** za presojo določene teme
- Kakovost

Uporaba je obvezna najkasneje 12 mesecev po izdaji!

Slika je povzeta po opisu IPPF na spletni strani inštituta za notranjo revizijo https://www.theiia.org/en/standards/2024-standards/topical-requirements/

Kaj so tematske zahteve in kako predstavljajo del IPPF

Uporaba je obvezna najkasneje 12 mesecev po izdaji!



Kaj so tematske zahteve in kako predstavljajo del IPPF

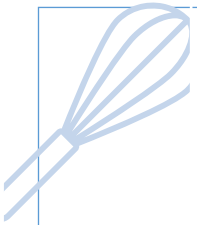
Elementi tematske zahteve

- Tematska zahteva
- Uporabniški priročnik

Osnovna **merila** vsake tematske zahteve

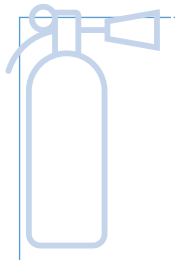
- Kako se področje **upravlja**?
- Kako na področju **obvladujemo tveganja**?
- Kako so na področju vzpostavljene **kontrole?**

Tematska zahteva za kibernetsko varnost



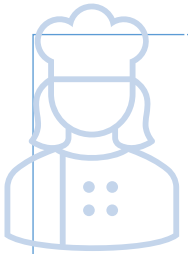
UPRAVLJANJE

- formalna strategija kibernetske varnosti in merljivi cilji
- kibernetska varnost v vseh fazah življenjskega cikla IT sredstev
- vključeni vsi ključni deležniki (poslovodstvo, IT, HR, pravna služba, skladnost)



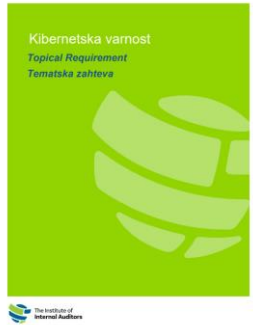
OBVLADOVANJE TVEGANJ

- celovit proces obvladovanja tveganj
- obvladovanje tveganj zajema celotno organizacijo (IT, HR, pravna služba, skladnost, ipd.)
- jasno določene odgovornosti in redno poročanje
- postopek za pravočasno eskalacijo
- ozaveščanje vodstva in zaposlenih o tveganjih
- proces odzivanja na incidente in okrevanja

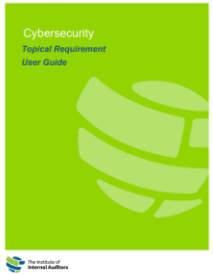


KONTROLE

- vzpostavljene kontrole za zaščito sistemov in podatkov
- obvladovanje talentov
- spremljanje kibernetskih groženj
- tehnične kontrole: konfiguracija naprav, šifriranje, popravki, upravljanje dostopov, DevSecOps
- omrežne kontrole: segmentacija, požarne pregrade, ZTNA/VPN, IoT, IDS/IPS
- zaščita končnih komunikacijskih točk (e-pošta, splet, videokonference, družbeni mediji, oblak)



Uporabniški priročnik k zahtevi



Podpora NR:

- Izvedba
- Dokumentiranje in poročanje
- QA

Poglobljeno razumevanje področja kibernetske varnosti

Podrobne usmeritve:

- Upravljanje
- Obvladovanje tveganj
- Kontrole

Priloge:

- **A** - praktični primere uporabe tematske zahteve
- **B** - povezave z drugimi okviri (npr. NIST, COBIT).
- C - orodje za dokumentacijo presoje zahtev in izjem

Direktiva NIS 2

Razširitev področja uporabe

Ukrepi za zagotavljanje kibernetske varnosti

Odgovornost upravljalnih organov

Obveznost poročanja

Uvedba upravnih glob

Izboljšanje sodelovanja na ravni EU in skupne sposobnosti za pripravo in odzivanje ter vzpostavitev mreže EU-CYCLONE

Zakon o informacijski varnosti (ZInfV-1)

- 17. 10. 2024
- Uveljavitev v letu 2025

Podrobneje določa:

- zavezance,
- nacionalni sistem informacijske varnosti,
- ukrepe za obvladovanje tveganj in priglasitev incidentov,
- nadzor…

Kdo so zavezanci po ZInfV-1?

Subjekti, ki spadajo med vrste subjektov iz Prilog 1 ali Priloge 2, če imajo:

– vsaj 50 zaposlenih in

– letni promet ali letno bilančno vsoto vsaj 10 milijonov evrov.

Priloga 1: Visoko kritični sektorji

- Energija;
- Transport;
- Bančništvo;
- Infrastruktura finančnega trga;
- Zdravstveni sektor;
- Oskrba s pitno vodo in njena distribucija;
- Odpadna voda;
- Digitalna infrastruktura.
- Upravljanje storitev IKT (med podjetji);
- Javna uprava;
- Vesolje.

Priloga 2: Drugi kritični sektorji

- Poštne in kurirske storitve;
- Ravnanje z odpadki;
- Izdelava, proizvodnja in distribucija kemikalij;
- Pridelava, predelava in distribucija živil;
- Proizvodnja;
- Digitalni ponudniki;
- Raziskave.

Zavezanci ne glede na število zaposlenih, letni promet ali bilančno vsoto

- če storitev opravljajo: a) ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, b) ponudniki storitev zaupanja, c) registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen;
- je subjekt edini ponudnik storitve ali dejavnosti v Republiki Sloveniji, katere izvajanje ga uvršča med vrste subjektov iz Priloge 1 ali 2;
- bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na **javni red, javno varnost ali javno zdravje**;

Zavezanci ne glede na število zaposlenih, letni promet ali bilančno vsoto

- bi motnja pri opravljanju storitve subjekta lahko povzročila sistemsko tveganje, zlasti za sektorje iz Priloge 1 ali 2, v katerih bi lahko taka motnja imela čezmejni vpliv;
- ima subjekt poseben pomen na državni ali lokalni ravni za posamezni sektor iz Priloge 1 ali 2 ali za izvajanje posamezne storitve, ki ga uvršča med vrste subjektov iz Priloge 1 ali 2 ali zaradi medsebojne odvisnosti z drugimi sektorji iz Prilog 1 ali 2 v Republiki Sloveniji;
- gre za **subjekt javne uprave na državni ravni.**

Drugi zavezanci

- subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja področje kritične infrastrukture;
- subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost;
- subjekti, ki so v državnih načrtih zaščite in reševanja opredeljeni kot službe državnega pomena, če bi nedelovanje njihovih omrežnih in informacijskih sistemov ogrozilo izvajanje nalog zaščite in reševanja iz prej navedenih načrtov in
- **mestne občine kot subjekti javne uprave na lokalni ravni.**

Obveznosti zavezancev

Zavezanci (bistveni in pomembni subjekti) sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz:

- 21. člena ZInfV-1 – **varnostna dokumentacija** in
- 22. člena ZInfV-1 – **ukrepi za obvladovanje tveganj**
- v **osemnajstih mesecih** od uveljavitve tega zakona (62. člen ZInfV-1).

Varnostna dokumentacija (21. člen ZInfV-1)

Bistveni in pomembni subjekti vzpostavijo in vzdržujejo:

- dokumentirani sistem upravljanja varovanja informacij in
- sistem upravljanja neprekinjenega poslovanja,

ki temeljita na pristopu upoštevanja vseh nevarnosti.

Ukrepi za obvladovanje tveganj (22. člen ZInfV-1)

Bistveni in pomembni subjekti morajo sprejeti:

- tehnične,
- operativne in
- organizacijske ukrepe

za **zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti** omrežnih in informacijskih sistemov oziroma

za **obvladovanje tveganj** za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev

ter **za preprečevanje ali zmanjšanje** vpliva incidentov na prejemnike svojih storitev in druge storitve.

Ocena skladnosti (25. člen ZInfV-1)

- **Bistveni subjekti** morajo **oceno skladnosti** izvajati najmanj **enkrat** na **dve leti** ali v primeru pojava pomembnega incidenta.
- Ocena skladnosti se izvaja kot **revizija skladnosti** s predpisi s področja informacijske varnosti ali v **okviru notranje revizije**, ki se izvaja na podlagi drugih predpisov in vključuje področje informacijske varnosti.
- Oceno skladnosti lahko v okviru notranje revizije poleg revizorjev informacijskih sistemov izvajajo tudi **notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo**, katerega delo revizor uporabi kot strokovno pomoč pri pridobivanju zadostnih in ustreznih revizijskih dokazov.
- Revizor informacijskih sistemov ali notranji revizor pripravi poročilo o izvedeni oceni skladnosti.

Samoocena skladnosti (25. člen ZInfV-1)

- **Pomembni subjekti** izvedejo **samooceno skladnosti** najmanj **enkrat** na **dve leti** ali v primeru **pojava pomembnega incidenta**.
- Samoocena skladnosti se izvede na način, da se dokumentirano preverita skladnost pomembnega subjekta z njegovo varnostno dokumentacijo in izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost.
- Samoocena skladnosti se lahko izvede tudi **v okviru notranje revizije**.

Povezani subjekti – Minimalne varnostne zahteve (10. odstavek 22. člena ZInfV-1)

- Upravljavec centralnega državnega informacijsko-komunikacijskega sistema mora povezanim subjektom določiti **minimalne varnostne zahteve informacijske in kibernetske varnosti.**
- Upravljavec centralnega državnega informacijsko-komunikacijskega sistema pooblaščen, da izvede **ustrezne, nujne in sorazmerne ukrepe** za zaščito centralnega državnega informacijsko- komunikacijskega sistema.
- Ukrepi vključujejo tudi **začasni odklop posameznega povezanega subjekta** iz centralnega državnega informacijsko-komunikacijskega sistema, dokler ugotovljena tveganja niso odpravljena.

Sankcije za odgovorne osebe javnega sektorja

Prekrški bistvenih subjektov – globa za odgovorno osebo v državnem organu ali samoupravni lokalni skupnosti od **1.000 do 10.000** EUR oziroma od **500 do 3.000** EUR.

Prekrški pomembnih subjektov – globa za odgovorno osebo v državnem organu ali samoupravni lokalni skupnosti od **1.000 do 7.000** EUR oziroma od **200 do 2.000** EUR.

Praktični razmisleki za javni sektor

Centralizacija informacijskih storitev za javni sektor na MJU

2011 · 2012 · 2013 · 2014 · 2015 · 2016 · 2017 · 2018 · 2019 · 2020 · 2021 · 2022 · 2023

Stanje pred 2015

Skupno omrežje državnih organov

Nekatere skupne informacijske rešitve

2015–2020

REORGANIZACIJA DRŽAVNE INFORMATIKE

s ciljem centralizacije
- finančnih
- človeških in
- tehničnih virov

Stanje konec 2021 (po razpoložljivih podatki MJU)

115 strank domenskih, datotečnih, poštnih in drugih centralno vzpostavljenih storitev

334 strank uporablja več kot 25.000 kvalificiranih digitalnih potrdil

62 strank, katerih sektorski informacijski sistemi gostujejo na infrastrukturi MJU

14 strank gostuje v varnih strežniških prostorih MJU

686 strank uporablja oddaljeni dostop do omrežja državnih organov HKOM

86 storitev v Katalogu informacijskih storitev MJU

Nejasnosti glede informacijskih storitev MJU

KAJ NATANČNO so informacijske storitve MJU?

- MJU je **šele ob koncu obdobja,** na katero se nanaša revizija, **objavilo katalog** vseh svojih **informacijskih storitev.**
- MJU v javno objavljenih dokumentih **večine storitev ni podrobneje predstavilo.**
- Organizacije javnega sektorja **niso vedele, katere storitve imajo na voljo** in katere morajo same poiskati na trgu.

KOMU TOČNO so namenjene?

- Katere vrste organizacij jih **po zakonu morajo uporabljati?**
- Katere vrste organizacij **smejo prostovoljno pristopiti** k informacijskim storitvam MJU?
- **Za katere vrste organizacij** so informacijske storitve MJU **plačljive** in v katerih okoliščinah?

POD KAKŠNIMI POGOJI jih lahko stranke uporabljajo?

MJU za večino informacijskih storitev **ni javno objavilo:**

- načina pristopa k storitvi
- splošnih pogojev uporabe
- delitve odgovornosti za upravljanje storitve

MJU v okviru svojih pristojnosti ni zagotovilo, da bi se v področnih predpisih ustrezno normativno uredile zakonske podlage, ki povzročajo nejasnosti.

Pogodbeni dogovori o informacijskih storitvah s strankami MJU

KAKO je MJU upravljalo pogodbene dogovore?

- **ni imelo točne in ažurne evidence** pogodbenih dogovorov
- **ni razpolagalo z nekaterimi veljavnimi verzijami** posameznih pogodbenih dogovorov
- v nekaterih primerih je izvajalo informacijske storitve **brez pisnega pogodbenega dogovora**

ČESA pogodbeni dogovori **niso opredeljevali?**

- nekateri pogodbeni dogovori **niso jasno opredeljevali predmeta pogodbe** (na primer informacijskih storitev, ki jih MJU za stranko izvaja)
- nekateri pogodbeni dogovori **niso nedvoumno opredeljevali pravic in obveznosti pogodbenih strani** (na primer za informacijsko varnost in varstvo osebnih podatkov)
- praviloma pogodbeni dogovori **niso opredeljevali kazalcev kakovosti storitev** ali postopkov njihovega spremljanja

Poimenovanja informacijskih storitev v zakonskih podlagah, v javno objavljenih dokumentih MJU in v pogodbenih dogovorih **so se razlikovala, zato ni bilo vselej jasno, na kaj se določen dogovor pravzaprav nanaša.**

Za zaključek – kaj lahko naredimo DNR?