# Breme predpisov in standardizacije v sezoni 2024/2025

Boštjan Kežmah

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko,
Maribor, Slovenija
bostjan.kezmah@um.si

Prispevek obravnava vpliv novih predpisov in sprememb standardov na področju informacijske varnosti, s poudarkom na standardu ISO/IEC 27001:2023 in prihajajočem slovenskem Zakonu o informacijski varnosti (ZInfV-1). Zakon bo bistveno razširil število zavezancev, kar bo zanje predstavljalo dodatne obremenitve pri zagotavljanju skladnosti s predpisi. Poudarek prispevka je na ključnih spremembah standarda ISO 27001, zlasti v prilogi A, kjer je število kontrol zmanjšano na 93, vendar so te postale zahtevnejše in bolj celovite. Med novimi kontrolami v praksi predstavljajo izziv obveščevalne informacije o grožnjah, informacijska varnost pri uporabi oblačnih storitev in pripravljenost IKT za neprekinjeno poslovanje zaradi nepopolnega razumevanja in izvajanja teh kontrol. Prihajajoče spremembe bodo od organizacij zahtevale večjo pozornost in prilagoditve v operativnih in strateških postopkih.

**Ključne besede:**
standardizacija
dobre prakse
normativni okvir
spremembe predpisov
ISO 27001

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-894-9
DOI https://doi.org/10.18690/um.feri.4.2024.12

# 1 Uvod

V zadnjih letih je bilo objavljenih veliko sprememb tako v predpisih kot standardih na področju informacijskih sistemov, še posebej na področju kibernetske varnosti.

V Sloveniji trenutno pričakujemo sprejem novega Zakona o informacijski varnosti (ZInfV-1), ki v času nastajanja tega prispevka še ni bil sprejet, je pa že bil v javni obravnavi do 31. 5. 2024. [1]

Javnost sicer nima vpogleda v nadaljnje medresorsko in drugo podrobno usklajevanje končnega predpisa, zato do predložitve zakona v sprejem Državnemu zboru in seveda samega sprejema zakona ne bomo zanesljivo poznali njegove dokončne vsebine, lahko pa na podlagi podanih pripomb na zakon sklepamo, da zavezanci pričakujejo, da bo zanje predstavljal pomembno dodatno obremenitev.

Če je bilo doslej ponudnikov bistvenih storitev približno sto, predlagatelj zakona pričakuje, da bo število zavezancev desetkrat večje, torej da bo zavezancev več kot tisoč. Predlagatelj zakona je Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) in s predlagano spremembo zakona prenaša v slovenski pravni red Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembo Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitev Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z dne 27. 12. 2022, str.80.), nazadnje popravljene s Popravkom Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 239 z dne 28. 9. 2023, str. 48) (v nadaljnjem besedilu: Direktiva (EU) 2022/2555).

Razen nepregledno dolgega citata pravne podlage URSIV izpostavlja, da je namen osnutka predloga ZInfV-1 bo tudi sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah. [2]

24. člen predloga ZInfV-1 določa, da bistveni in pomembni subjekti zaradi zagotovitve skladnega izvajanja ukrepov iz 20. in 21. člena tega zakona v čim večji meri uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. [3]

Iz pojasnil k spremembam zakona pa je mogoče v pojasnilu k 24. členu razbrati, da predlagatelj zakona med drugim prepoznava standard ISO/IEC 27001, mednarodni standard za upravljanje informacijske varnosti, ki določa zahteve za vzpostavitev, izvajanje, vzdrževanje in izboljšanje sistema upravljanja informacijske varnosti v organizacijah kot enega od standardov, ki bi izpolnjevali pogoje iz predlaganega 24. člena.

# 2 ISO/IEC 27001

Čeprav ima standard ISO/IEC 27001 že dolgo zgodovino, bo uporabnike standarda zanimala predvsem zadnja sprememba.

V Sloveniji so prevzeti standardi označeni s predpono SIST in je tako v primeru informacijske varnosti zadnja različica »SIST EN ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)« (v nadaljevanju: ISO 27001).

Da je vse skupaj še bolj nepregledno, je bil zaradi klimatskih sprememb naknadno izdan še dodatek »ISO/IEC 27001:2022/Amd 1:2024 Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes«, ki se nanaša na upoštevanje tveganja klimatskih sprememb na informacijsko varnost. Seveda ga je treba kupiti posebej.

Uporabnika, ki bo nameraval vpeljevati ISO 27001, bo presenetila skopa vsebina standarda, ki ne vsebuje podrobnih informacij o zahtevanih notranjih kontrolah.

Te so razdeljene v dva večja dela, uvodni del in prilogo A. Uvodni del predstavlja osnovni okvir za vzpostavitev, implementacijo, vzdrževanje in stalno izboljševanje sistema za upravljanje informacijske varnosti (ISMS). Vključuje: splošne zahteve, vodstvo in odgovornost, obvladovanje tveganj in neprestane izboljšave.

Uvodni del je po vsebini enak kot uvodni del standarda ISO 9001. Vendar bi tudi v standardu ISO 9001 zaman iskali pojasnila o podrobnih zahtevah oziroma priporočilih glede vpeljave notranjih kontrol iz uvodnega poglavja, saj je podrobna razlaga v standardu ISO/TS 9002, ki predstavlja dobro prakso za uvajanje standarda ISO 9001.

Priloga A, ki je za tehnike bistveno bolj zanimiva, saj vsebuje tudi sklop tehničnih kontrol, je razdeljena v poglavja organizacijskih ukrepov, ukrepov za zaščito ljudi, fizične ukrepe in tehnične ukrepe. Dobro prakso za kontrole iz priloge A pa najdemo v standardu ISO 27002.

V praksi to pomeni, da za uvajanje standarda potrebujemo predvsem naslednje podlage:

- »SIST EN ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)«, iz katerega na enem mestu razberemo vse krovne zahteve za skladnost s standardom.
- »SIST-TS ISO/TS 9002:2016 Quality management systems - Guidelines for the application of ISO 9001:2015«, ki vsebuje smernice za izpolnjevanje kontrolnih zahtev iz uvodnega dela standarda. Priporočena literatura tudi za tiste, ki bi hkrati vpeljevali standard ISO 9001.
- »SIST EN ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)«, ki vsebuje podroben opis dobrih praks za izpolnitev zahtev po kontrolah iz ISO 27001.
- »ISO/IEC 27001:2022/Amd 1:2024 Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes«, obvezni dodatek, ki standardu 27001 dodaja zahteve v zvezi z obravnavanjem tveganj, ki so povezani s klimatskimi spremembami (velja tudi za ISO 9001).

Pozoren bralec bo morda opazil, da je letnica ISO 27002 starejša od letnice ISO 27001. Ker 27002 obravnava samo prilogo A iz standarda ISO 27001, ni nujno nenavadno, da je bil celotni standard sprejet kasneje, kot je bila sprejeta dokončna odločitev o vsebini kontrol iz priloge A in je bil lahko zato standard ISO 27002, ki se nanaša samo na prilogo A, sprejet pred sprejemom standarda ISO 27001.

ISO 27002 bo bolj zanimiv dokument tudi za tiste, ki že imajo vpeljane kontrole po prejšnji različici standarda ISO 27001, saj v tem dokumentu v prilogi najdejo navzkrižni šifrant starih in novih oznak kontrol, zato bodo lažje prilagodili svoj dokument SOA (t.i. »Statement of Applicability«) novi različici standarda.

## 3 Nove kontrole v prilogi A po ISO 27002

V primerjavi s prejšnjo različico standarda je kontrol sicer navidezno manj, saj jih je v prilogi A le še 93 (prej 114) [4], vendar je številka zavajajoča. Dejansko obstoječe kontrole iz priloge A prejšnjega standarda niso bile ukinjene, bile so le združene, hkrati pa so bile dodane tudi nove. Posledica tega je, da je ISO 27001 v novejši različici zahtevnejši od prejšnje.

Do nastanka tega članka je bilo le za vzorec certifikacij po novem standardu, saj obstoječi standard velja še do jeseni 2025, zato so se za novega pretežno odločale organizacije, ki so se certificirale prvič.

Ne glede na to lahko že izpostavimo nekaj kontrol, ki so predstavljale težave novim certificirancem. Domnevamo lahko, da je to tudi posledica svetovalcev, ki se pri vpeljavi prav tako srečujejo z novimi zahtevami in enako kot presojevalci še z njimi nimajo veliko izkušenj.

### 3.1. Obveščevalne informacije o grožnjah (5.7)

Obveščevalne informacije o grožnjah so zbiranje, analiziranje in interpretiranje podatkov o obstoječih in potencialnih varnostnih grožnjah, ki lahko vplivajo na organizacijo. Gre za proaktiven pristop k informacijski varnosti, kjer organizacije spremljajo varnostne grožnje, kot so kibernetski napadi, zlonamerna programska oprema, ranljivosti v sistemih ali omrežjih in drugi varnostni incidenti.

Cilj te kontrole je zagotoviti vpogled v grožnje, da se organizacije lahko bolje pripravijo in zaščitijo svoje sisteme, podatke in omrežja. [4] Ponuja relevantne informacije, ki omogočajo odzivanje na trenutne in prihodnje grožnje.

Standard izrecno določa, da naj bi zbirali podatke o grožnjah informacijske varnosti in jih analizirali, da bi s tem ustvarili obveščevalne podatke.

Namen kontrole je vzpostaviti zavedanje organizacije o grožnjah v okolju, zato, da je mogoče izvajati ustrezne aktivnosti za njihovo obvladovanje.

Zbiranje podatkov vključuje tako podatke o obstoječih kot o porajajočih se grožnjah.

Dobra praksa določa tri sloje obveščevalnih informacij: [4]

- Strateške informacije obsegajo izmenjavo informacij na visoki ravni v zvezi s spreminjajočim se okoljem groženj, kot na primer vrste napadalcev in vrste napadov.
- Taktične informacije vsebujejo podatke o metodologijah napadalcev, orodjih in uporabljenih tehnologijah.
- Operativne informacije predstavljajo podrobnosti o specifičnih napadih, vključno s tehničnimi značilnostmi teh napadov.

Ob tem morajo biti obveščevalne informacije relevantne, podajati zavedanje o situaciji ter takšne, da je v zvezi z njimi mogoče ukrepati.

Dobra praksa vzpodbuja izmenjavo informacij z drugimi organizacijami kot skupno osnovo za izboljšanje obveščevalnih informacij o grožnjah.

V praksi so organizacije k temu pristopile neodločno in z zelo omejenimi viri. Večinoma se pri tem opirajo na informacije, ki jih prejemajo npr. od ponudnika protivirusne zaščite, ponudnika storitev v oblaku in ponudnika operacijskega sistema. Tako ozko razumevanje obveščevalnih podatkov ne dosega v celoti namena standarda, zato bo glede izvajanja te kontrole potrebnega še veliko osveščanja.

Dejansko je z dobro analizo razpoložljivih informacij mogoče tudi brez bistvenega finančnega vložka pridobiti prosto dostopne informacije, ki ob ustrezni obdelavi lahko zadoščajo za izpolnjevanje te kontrole.

Hkrati je treba izpostaviti, da bo v sklopu analize obsega certifikacije zelo težko utemeljeno trditi, da ta kontrola v neki organizaciji ni potrebna in da jo je zato mogoče izločiti iz SOA.

### 3.2. Informacijska varnost za uporabo oblačnih storitev (5.23)

Ob vse večjem razmahu oblačnih storitev je bil že čas, da dobijo oblačne storitve svojo kontrolo znotraj standarda ISO 27001.

Ta kontrola se nanaša na uporabo oblačnih storitev in ne njihovo zagotavljanje. Izrecno opis kontrole navaja, da predstavlja proces nabave, uporabe, vodenja in izhoda iz oblačnih storitev in da bi naj bil ta proces vzpostavljen skladno z zahtevami informacijske varnosti organizacije. [4]

Dobra praksa usmerja v vzpostavitev specifične politike za uporabo oblačnih storitev, ki bi morala biti dostopna zainteresiranim strankam. Ob tem izpostavlja, da je lahko pristop razširitev obstoječega pristopa k obvladovanju storitev, ki jih organizaciji zagotavljajo tretji ponudniki.

Bistveno je, da so odgovornosti jasno razmejene in jasno določene med organizacijo in ponudnikom oblačnih storitev.

Med drugim je treba med pomembnejšimi odgovornostmi določiti tudi postopek zamenjave ponudnika oblačnih storitev in prenehanje uporabe oblačnih storitev vključno z izhodno strategijo.

V praksi se izkaže, da organizacije premalo pozornosti posvetijo predvsem izhodni strategiji, ki je praviloma določena s pogodbo, to pa potem vodi do različnih sodnih sporov, predvsem pa realizirani množici tveganj, povezanih z izhodno strategijo, v najslabšem primeru tudi z resno, daljšo prekinitvijo storitve ali celo z nedostopnostjo podatkov, ki so bili shranjeni v oblaku.

Dobra praksa izrecno priznava, da so pri ponudnikih oblačnih storitev lahko pogodbe določene vnaprej in niso predmet pogajanj. Organizacija bi zato morala proučiti pogodbo ter opraviti analizo tveganja, da bi lahko identificirala preostala tveganja in sprejela ustrezne ukrepe za zmanjšanje tveganja glede na apetit tveganja, ki ga je določilo vodstvo.

V dobri praksi je podrobno določen seznam določb, ki bi morale biti sestavni del pogodbe s ponudnikom storitve v oblaku.

### 3.3. Pripravljenost informacijsko-komunikacijske tehnologije za neprekinjeno poslovanje (5.30)

Kljub temu, da je z nami že dolgo standard ISO 22301, ki se uporablja za neprekinjenost poslovanja in da imamo v tudi Sloveniji že nekaj organizacij, ki so certificirane po tem standardu, tudi standard ISO 27001 po novem vključuje kontrolo, ki se nanaša na neprekinjeno poslovanje.

ISO 22301 sicer bolj celovito naslavlja neprekinjenost poslovanja, na primer vključno z razpoložljivostjo nadomestnih prostorov, če običajnih poslovnih prostorov iz kakršnegakoli razloga ni mogoče uporabljati, zato se ISO 27001 bolj osredotoča na razpoložljivost informacij.

Nekateri so že v prejšnji različici standarda razumeli, da vključuje tudi neprekinjeno poslovanje, vendar to ne drži. Prejšnji ISO 27001 je imel le določbe v zvezi z zagotavljanjem neprekinjene informacijske varnosti. To pomeni neprekinjenost zagotavljanja informacijske varnosti na primer takrat, kadar ni električnega napajanja in se zato izključi video nadzorni sistem ali pa celo avtomatska kontrola dostopa z dostopnimi karticami. Neprekinjenost zagotavljanja informacijske varnosti ostaja tudi v novem ISO 27001.

Kontrola 5.30 pa je izrecno namenjena pripravljenosti informacijsko-komunikacijske tehnologije na neprekinjenost poslovanja. [4] Lahko bi rekli tudi, da predstavlja podmnožico neprekinjenega poslovanja, ki se nanaša le na neprekinjenost delovanja informacijskega sistema.

Dobra praksa glede izpolnitve te kontrole je jasna in zahteva vse od izdelave analize učinka na poslovanje, določitve točke okrevanja, časa okrevanja, načrtov okrevanja, kot tudi izvajanja testiranja načrtov okrevanja.

Ta kontrola je v primerjavi z ostalimi kontrolami zelo zahtevna, celo izrazito nesorazmerno zahtevna glede na to koliko truda je treba vložiti v vzpostavitev te kontrole.

V zvezi z zahtevnostjo vpeljave lahko svetujemo le, da posamezne odpustke glede doslednosti izvedbe te kontrole najdemo v analizi tveganja, ki je najboljše orodje za ugotavljanje in kasneje v certifikaciji tudi za dokazovanje skladnosti z zahtevami standarda. Vsekakor pa ta kontrola zahteva nesorazmeren napor pri prehodu na novo različico standarda, zato se ji splača posvetiti nekoliko več pozornosti čim prej v začetku priprav na prehod na novi standard.

# 4 Sklep

Predlagane spremembe slovenskega Zakona o informacijski varnosti (ZInfV-1) bodo pomembno vplivale na širitev kroga zavezancev, kar bo posledično povečalo potrebo po učinkoviti integraciji standardov kot je ISO 27001. Nova različica standarda ob tem prinaša zahtevnejše kontrole in združevanje obstoječih, kar bo predstavljalo izziv tudi za obstoječe uporabnike standarda in certificirane organizacije.

Ali bodo sprejete spremembe dejansko tudi vplivale na povečanje odpornosti in s tem zmanjšanje tveganj na področju kibernetske varnosti, bo pokazal čas.

# Literatura

[1] Javna obravnava osnutka predloga Zakona o informacijski varnosti (EVA 2023-1544-0005) – drugi krog, https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/674581?disposition=attachment, obiskano 20. 8. 2024.

[2] Informacija o predpisu, https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/660046?disposition=inline, obiskano 20. 8. 2024.

[3] Osnutek predloga: Zakon o informacijski varnosti, https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/674583?disposition=attachment, obiskano 20. 8. 2024.

[4] SIST EN ISO/IEC 27002:2022 Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Kontrole informacijske varnosti (ISO/IEC 27002:2022)