SPREMEMBE, KI JIH PRINAŠAJO NOVE RAZLIČICE V DRUŽINI STANDARDOV ZA INFORMACIJSKO VARNOST ISO/IEC 27000

ALENKA BREZAVŠČEK, DOROTEJA VIDMAR
Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija
alenka.brezavscek@um.si, doroteja.vidmar@um.si

Povzetek Družina standardov ISO/IEC 27000 predstavlja najbolj celovito zbirko standardov na področju informacijske varnosti. Njihova prednost je v splošni uporabnosti, saj je jih mogoče hitro in učinkovito implementirati v organizacije ne glede na njihovo dejavnost ali velikost. Družina standardov ISO/IEC 27000 predstavlja za organizacije uporabno in uveljavljeno ogrodje za presojo skladnosti in posledično certificiranje na področju informacijske varnosti. Zaradi navedenega je uporaba teh standardov v praksi globalno razširjena. V letu 2022 so se zgodile pomembne spremembe, saj sta dva od ključnih standardov v družini ISO/IEC 27000 dobila novi različici. V februarju 2022 je izšla nova različica standarda ISO/IEC 27002, v oktobru 2022 pa še nova različica standarda ISO/IEC 27001. Prenova obeh standardov je ključna za organizacije, ki se pri upravljanju informacijske varnosti opirajo na njihova določila. Namen prispevka je celovito prikazati, katere spremembe prinašata nova standarda ISO/IEC 27001:2022 in ISO/IEC 27002:2022 v primerjavi s preteklima različicama iz leta 2013. Ugotovili smo, da je bilo največ sprememb narejenih v dodatku standarda ISO/IEC 27001, kar pogojuje povsem prenovljeno strukturo standarda ISO/IEC 27002. Na kratko smo povzeli, kakšen je vpliv nastalih sprememb za organizacije, ki obravnavana standarda uporabljajo pri svojem poslovanju.

Ključne besede:
informacijska varnost, standardi, ISO/IEC 27001:2022, ISO/IEC 27002:2022, spremembe

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/um.fov.3.2023.15
ISBN 978-961-286-722-5

Changes Brought by New Versions in the ISO/IEC 27000 Family of Information Security Standards

Alenka Brezavšček, Doroteja Vidmar
University of Maribor, Faculty of organizational sciences, Kranj, Slovenia
alenka.brezavscek@um.si, doroteja.vidmar@um.si

Abstract The family of standards ISO /IEC 27000 represents the most comprehensive series of standards in the field of information security. Their advantage is their general applicability, as they can be implemented quickly and efficiently in any organisation, regardless of its sector or size. The ISO /IEC 27000 family provides organisations with a practical and established framework for information security assessment and certification. As a result, the use of these standards in practise is widespread globally. In 2022, the ISO /IEC 27000 family underwent significant changes, with two of the most important standards receiving new versions. A new version of ISO /IEC 27002 was published in February 2022, and ISO /IEC 27001 in October 2022. The revisions are very important for organisations implementing the requirements of the standards as part of information security management. The aim of this paper is to provide a comprehensive overview of the changes introduced by the new versions ISO /IEC 27001:2022 and ISO /IEC 27002:2022 compared to the 2013 versions. We found that most of the changes were made to Annex A of the ISO /IEC 27001, which required a completely new structure for the ISO /IEC 27002. We have briefly summarized the impact of these changes on organizations applying these standards in their business operations.

Keywords: information security, standards, ISO/IEC 27001:2022, ISO/IEC 27002:2022, changes

DOI https://doi.org/10.18690/um.fov.3.2023.15
ISBN 978-961-286-722-5
University of Maribor Press

1 Uvod

Družina standardov ISO/IEC 27000 predstavlja najbolj celovito zbirko standardov na področju informacijske varnosti (OGCIO, 2022). Njihova prednost je predvsem v splošni uporabnosti, saj je standarde možno hitro in učinkovito implementirati v različne organizacije ne glede na njihovo dejavnost ali velikost. Poleg tega predstavlja družina standardov ISO/IEC 27000 za organizacije uporabno in uveljavljeno ogrodje za presojo skladnosti in posledično certificiranje na področju informacijske varnosti. Zaradi vsega navedenega je uporaba teh standardov v praksi zelo razširjena tako v svetu kakor tudi v Sloveniji.

V letu 2022 so se v družini standardov ISO/IEC 27000 zgodile pomembne spremembe, saj sta dva od ključnih standardov v tej družini dobila novi različici. V mesecu februarju je izšla nova različica standarda ISO/IEC 27002, imenovana »*ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security control*s« (ISO, 2022b) v mesecu oktobru pa še nova različica standarda ISO/IEC 27001, imenovana »*ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements*« (ISO, 2022a). Prenova obeh standardov je ključnega pomena za vse organizacije, ki se pri upravljanju informacijske varnosti kakor koli opirajo na določila teh standardov. Spremembe bodo morale v svojem poslovanju upoštevati tako organizacije, ki že imajo certifikat skladnosti s prejšnjo različico standarda, kakor tudi organizacije, ki standarde uvajajo na bolj neformalen način in o certificiranju morda šele razmišljajo.

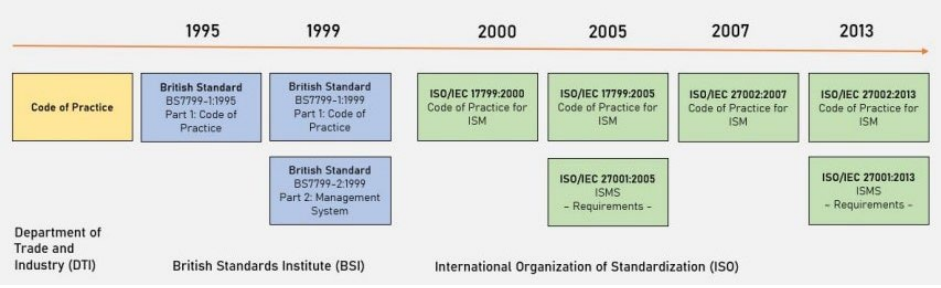
Ključni namen prispevka je celovito prikazati, katere spremembe prinašata novi različici standardov ISO/IEC 27001 (ISO, 2022a) in 27002 (ISO, 2022b) v primerjavi s preteklima različicama iz leta 2013 (ISO, 2013a, 2013b). Na sistematičen način bomo predstavili tako večje kot manjše spremembe kontrol v obeh standardih. Pod večje spremembe uvrščamo kontrole, ki so v zadnjih različicah standardov dodane na novo, kakor tudi kontrole, ki predstavljajo združitev že obstoječih kontrol. Med manjše spremembe pa uvrščamo bolj »kozmetične« popravke, kot so preimenovanje in/ali preštevilčenje že obstoječih kontrol. V diskusiji bomo zavzeli stališče, kaj konkretno spremembe obeh standardov pomenijo za organizacije, ki standarde v svoje poslovanje uvajajo.

Glede na to, da se tudi v slovenskem prostoru uporabljata angleški različici obravnavanih standardov, ki ju zasledimo pod imeni SIST EN ISO/IEC 27001:2022 in SIST EN ISO/IEC 27002:2022[1], smo navedbe, ki so neposredno citirane iz samih standardov, ohranili v izvorni obliki (t.j. v angleškem jeziku) slovenske prevode pa smo dodali le na mestih, kjer je bilo to smiselno in/ali potrebno.

2 Teoretično ozadje

2.1 Kronološki razvoj standardov ISO/IEC 27001 in 27002

Potek razvoja standardov ISO/IEC 27001 in 27002 do leta 2013 je ponazorjen na sliki 1.



Slika 1: Razvoj standardov ISO/IEC 27001 in ISO/IEC 27002
Vir: Volyntseva (2021)

Razvidno je, da je predhodnik današnjih standardov ISO/IEC 27001 in 27002 britanski standard BS 7799, ki ga je leta 1995 izdal British Standards Institute – BSI[2]. Od leta 2000 dalje pa razvoj teh standardov poteka pod okriljem mednarodne organizacije za standardizacijo International Organization for Standardization – ISO[3]. Ena od ključnih prelomnic se je zgodila v letu 2005, ko se je standard razdelil na dva dela oziroma na dva ločena standarda, pri čemer je prvi standard (takratni ISO/IEC 17799:2005) predstavljal kodeks dobre prakse za upravljanje informacijske varnosti v organizaciji »*Code of Practice for Infromation Security Management*«, drugi

[1] Oznaka SIST pomeni, da gre standard, ki smo ga privzeli v Republiki Sloveniji, oznaka EN pa pomeni, da je bi standard sprejet tudi s strani Evropske unije.
[2] https://www.bsigroup.com/
[3] https://www.iso.org/home.html

standard (takratni ISO/IEC 27001:2005) pa je definiral zahteve za sistem za upravljanje informacijske varnosti (v nadaljevanju SUIV) »*Information Security Management System (ISMS) Requirements*«. Podobna »logika« je privzeta tudi obstoječih verzijah obeh standardov. ISO/IEC 27001:2005 namreč predstavlja neposrednega predhodnika današnjega standarda ISO/IEC 27001:2022, medtem ko se je kodeks dobre prakse ISO/IEC 17799:2005 v letu 2007 preimenoval v ISO/IEC 27002:2007 in je tako neposredni predhodnik današnjega standarda ISO/IEC 27002:2022.

2.2 Razumevanje razlik med standardoma ISO/IEC 27001 in 27002

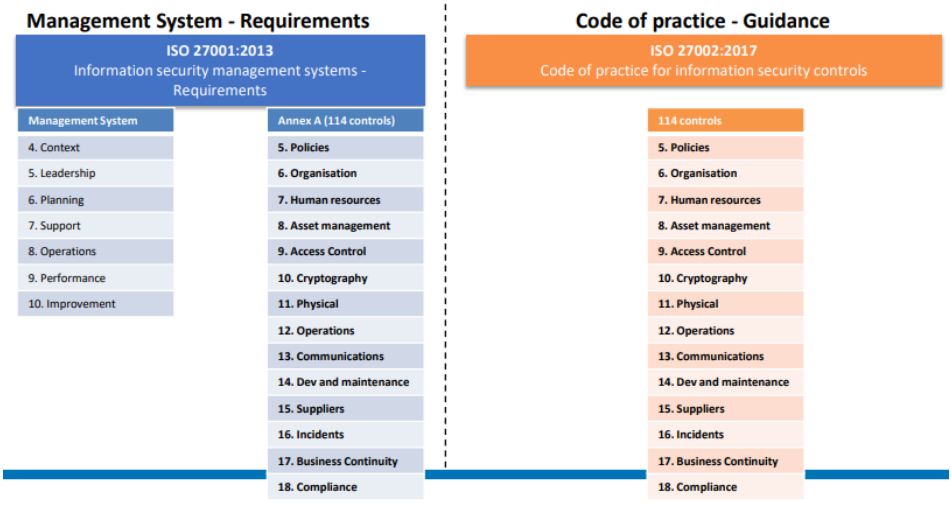
Oba standarda, ISO/IEC 27001 in ISO/IEC 27002, sta v tesni medsebojni povezavi, tako iz vidika vsebine kot same strukture, pa vendar med njima obstajajo pomembne razlike. Razumevanje le-teh je s stališča vpeljave standardov v prakso ključnega pomena.

ISO/IEC 27001 uvaja koncept SUIV (ang. ISMS – Information security management system), ki predstavlja kompleksen upravljavski sistem za obvladovanje in upravljanje informacijsko varnostnih tveganj v organizaciji. SUIV zajema set politik, postopkov in procedur, vezanih na zagotavljanje tako fizične in logične varnosti kakor tudi zagotavljanje skladnosti z obstoječo regulativo. Ključni namen ISO/IEC 27001 je torej zagotoviti ogrodje, ki je v pomoč pri načrtovanju, implementaciji, nadziranju, vzdrževanju in izboljševanju SUIV organizacije. ISO/IEC 27001 ne »vsiljuje« točno določenih informacijsko varnostnih kontrol, pač pa ponuja nabor zahtev, katerim naj bi SUIV v organizaciji zadoščal. Kot tak predstavlja ISO/IEC 27001 tudi specifikacije za certificiranje organizacije oziroma njenega SUIV (Adams, 2021). Pridobitev certifikata skladnosti s ISO/IEC 27001 je opcijska in ne obligatorna aktivnost, ki pa organizaciji, ki se za certificiranje odloči, prinese številne prednosti (glej npr. Shojaie et al., 2016).

Kot je razvidno iz slike 2 (leva stran), je standard ISO/IEC 27001 razdeljen na 2 dela: vsebinski del »*Managment system – Requirements*« in dodatek »Annex A«. Vsebinski del podaja zahteve za SUIV na sedmih različnih področjih (poglavja 4 - 10): »*Context*«, »*Ledership*«, »*Planning*, »*Support*, »*Operation*«, »*Performance*« in »*Improvement*«. Dodatek »*Annex A*« pa vsebuje seznam različnih varnostnih kontrol, ki so organizaciji lahko v pomoč pri doseganju zahtev iz vsebinskega dela standarda. Iz

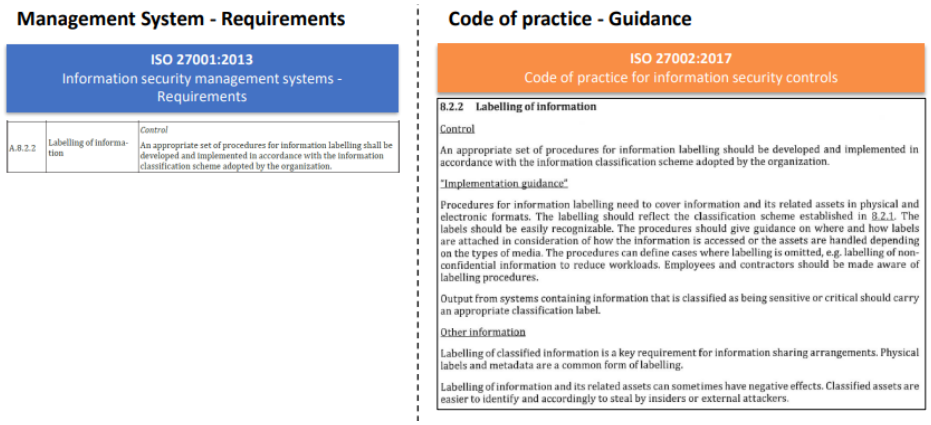
slike 2 je razvidno, da sta pretekli različici standardov vsebovali 114 kontrol, razdeljenih na 14 skupin.

Potrebno je poudariti, da so v dodatku ISO/IEC 27001 varnostne kontrole le skopo opredeljene (praktično le naštete), z vidikom implementacije posamezne kontrole pa se ta standard ne ukvarja. Na ta vidik je osredotočen drugi standard, ISO/IEC 27002, imenovan tudi kodeks dobre prakse (glej desno stran slike 2). ISO/IEC 27002 lahko torej razumemo kot podporni standard, ki za posamezno varnostno kontrolo, navedeno v dodatku standarda ISO/IEC 27001, podaja dokaj natančne usmeritve in navodila, kako to kontrolo v prakso tudi implementirati. Primer navedbe varnostne kontrole v dodatku ISO/IEC 27001 z usmeritvami za njeno implementacijo prikazuje slika 3.



Slika 2: Struktura standardov ISO/IEC 27001 (levo) in ISO/IEC 27002[4] (desno)
Vir: Volyntseva (2021)

[4] ISO/IEC 27001:2017 predstavlja vmesno različico, ki temelji na različici iz leta 2013 in vključuje popravke iz let 2014 in 2015.



Slika 3: Primer varnostne kontrole »*Labelling of information*« iz dodatka standarda ISO/IEC 27001:2013 z usmeritvami za njeno implementacijo v ISO/IEC 27002:2017
Vir: Volyntseva (2021)

3 Novosti v zadnjih različicah obeh standardov

3.1 Metodologija

Skladno z ustaljeno prakso rednega posodabljanja standardov, vezanih na informacijsko varnost, na vsakih pet let, sta oba standarda, ISO/IEC 27001 in ISO/IEC 27002, v letu 2022 dobila novi različici. ISO/IEC 27002:2022 je bil objavljen 15. februarja 2022, ISO/IEC 27001:2022 pa mu je sledil 25. oktobra 2022.

V nadaljevanju bomo na podlagi natančnega pregleda in primerjave obeh različic (2013 in 2022) obeh standardov (ISO/IEC 27001 in ISO/IEC 27002) proučili tako manjše, tehnične kot večje, vsebinske spremembe. Ključne spremembe bomo sistematično opisali in predstavili. Zavzeli bomo tudi stališče, kaj izvedene spremembe pomenijo za organizacije in ostalo zainteresirano strokovno javnost, ki obravnavana standarda pri svojem delu uporabljajo.

3.2 Razširitev fokusa iz informacijske varnosti na kibernetsko varnost in varovanje zasebnosti

Globalne spremembe na področju regulative, kot na primer uvedba predpisov za urejanje varnosti osebnih podatkov v mnogih državah (npr. Splošna uredba o varstvu podatkov (ang. General Data Protection Regulation - GDPR) v Evropski uniji, Zakon o varstvu osebnih podatkov (ang. Protection of Personal Information Act - POPIA) v Južni Afriki, Avstralska načela zasebnosti (ang. Australian Privacy Principles - APP)), porast kibernetsko-varnostnih tveganj, vse ostrejše zahteve in potrebe po zagotavljanju neprekinjenega poslovanja in varovanja zasebnosti uporabnikov so izzivi, s katerimi se soočajo organizacije po vsem svetu. Vse navedeno je le del razlogov, ki so pogojevali potrebo po razširitvi fokusa družine standardov ISO/IEC 27000, ki se doslej osredotočala predvsem na segment zagotavljanja informacijske varnosti. Kot je razvidno iz tabele 1, se novi različici standardov nanašata na širši koncept, kar se odraža tudi na spremembah imen obeh standardov. Segmentu informacijske varnosti sta tako dodana tudi segment kibernetske varnosti in varovanja zasebnosti uporabnikov.

Tabela 1: Staro in novo poimenovanje standardov ISO/IEC 27001 in 27002

	staro ime (2013)	novo ime (2022)
ISO/IEC 27001	ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements[5]	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements[6]
ISO/IEC 27002	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls[7]	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls[8]

[5] Slovenski standard: SIST ISO/IEC 27001:2013 Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti – Zahteve (poslovenjen le naslov, vsebina v angleškem jeziku).
[6] Še ni sprejet kot slovenski standard.
[7] Slovenski standard: SIST ISO/IEC 27002:2013 - Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti - Zahteve (poslovenjen le naslov, vsebina v angleškem jeziku).
[8] Slovenski standard: SIST EN ISO/IEC 27002:2022 Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Kontrole informacijske varnosti (poslovenjen le naslov, vsebina v angleškem jeziku).

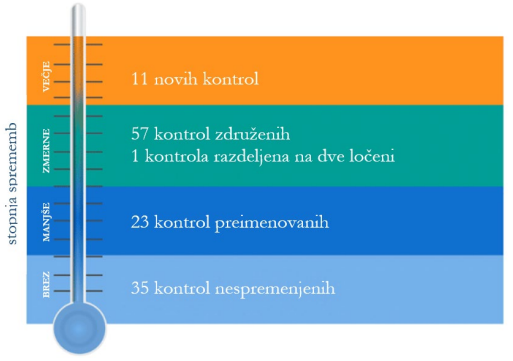
3.3 Kaj prinaša nova različica standarda ISO/IEC 27001:2022

Povzetek glavnih sprememb v novi različici standarda ISO/IEC 27001:2022 ponazarja slika 4. Razvidno je, da so se spremembe standarda ISO/IEC 27001 zgodile v naslednjih segmentih:

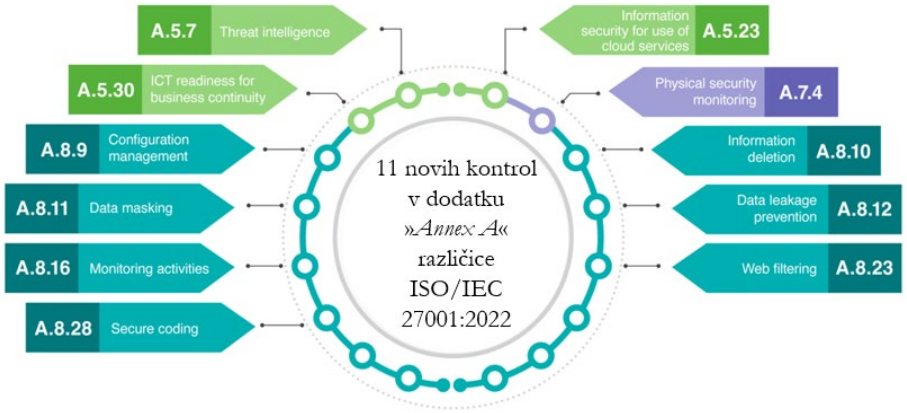
- **Vsebinski del (zahteve za SUIV):**
  - Naslovi poglavij 4 -10 (7 področij zahtev za SUIV) so ostali praktično nespremenjeni:
    - 4 – »*Context of the organization*« (slo. kontekst organizacije),
    - 5 – »*Ledership*« (slo. voditeljstvo),
    - 6 – »*Planning*« (slo. načrtovanje),
    - 7 – »*Support*« (slo. podpora),
    - 8 – »*Operations*« (slo. operacije),
    - 9 – »*Performance*« (slo. izvedba),
    - 10 – »*Improvement*« (slo. izboljšave).
  - Izvedeno je bilo nekaj manjših sprememb.
  - Dodane so bile nove zahteve za SUIV (Kosutic, 2022):
    - 4.2 c) – »*Requirements of interested parties to be addressed through ISMS*« (slo. potrebe in pričakovanja zainteresiranih strank naj bodo naslovljene prek SUIV),
    - 6.3 – »*Planning of Changes*« (slo. načrtovanje sprememb),
    - 8.1 – »*Establishing criteria for processes and implementing control for them in accordance with the criteria*« (slo. vzpostavitev kriterijev za procese in skladno s kriteriji vpeljava kontrol za procese),
    - 9.3.2 c) – »*Management review inputs - changes in needs and expectations of interested parties*« (slo. upravljanje »inputov« za presoje – spremembe v potrebah in pričakovanjih zainteresiranih deležnikov).
  - Nobena od ključnih zahtev za SUIV ni bila odstranjena.
- **Dodatek »*Annex A*«:**
  - Število kontrol se je zmanjšalo iz 114 na 93.
  - 93 kontrol je razvrščenih v 4 skupine (poglavja 5-8):
    - 5 – »*Organizational controls*« (slo. organizacijske kontrole),
    - 6 – »*People controls*« (slo. kontrole, vezane na ljudi),
    - 7 – »*Physical controls*« (slo. fizične kontrole),
    - 8 – »*Technolological controls*« (slo. tehnološke kontrole).
  - 11 kontrol je bilo dodanih na novo.

Slika 4: Povzetek glavnih sprememb v novi različici standarda ISO/IEC 27001:2022
Vir: prirejeno po Hyseni (2022)

Slika 5 podaja povzetek vseh sprememb v dodatku »*Annex A*« standarda ISO 27001:2022, na novo dodane kontrole pa so izpostavljene na sliki 6 ter podrobneje opisane v članku Kosutic (n.d.). Razvidno je, da je največ (7 od 11) na novo dodanih kontrol v poglavju 8 – »*Technolological controls*« (slo. tehnološke kontrole).



Slika 5: Povzetek sprememb v dodatku »*Annex A*« standarda ISO/IEC:2022
Vir: prirejeno po Kosutic (2022)



Slika 6: Nove varnostne kontrole v dodatku »*Annex A*« standarda ISO/IEC 27001:2022
Vir: prirejeno po Kosutic (n.d.)

3.4 Kaj prinaša nova različica standarda ISO/IEC 27002:2022

Posodobljena različica standarda ISO/IEC 27002:2022 ni več poimenovana kot kodeksa dobre prakse. Namesto tega predstavlja ISO/IEC 27002:2022 referenčni dokument, ki ponuja generičen nabor informacijsko varnostnih kontrol pri vzpostavitvi SUIV v organizacijo. Organizacije lahko uporabijo ISO/IEC 27002:2022 kot referenčni dokument v vsakem primeru, če je njihov SUIV zasnovan na podlagi ISO 27001, ali pa na kaki drugi metodologiji, ki jo izberejo (Flores, 2022). Ključne spremembe v standardu ISO/IEC 27002:2022 bi lahko strnili na naslednji način:

- povsem nova struktura dokumenta kot celote, ki je usklajena z dodatkom »*Annex A*« standarda ISO/IEC 27001:2022;
- prenovljen je izgled in struktura posamezne varnostne kontrole (opisano v nadaljevanju);
- posamezni varnostni kontroli je dodana t.i. tabela atributov (opisano v nadaljevanju).

Struktura zapisa varnostnih kontrol je prenovljena tako, da zapis pri posamezni varnostni kontroli vsebuje naslednje informacije:

- Razdelek »*Control title*« vsebuje poimenovanje varnostne kontrole;
- Dodana je tabela atributov »*Attribue table*«. Informacije, ki jih tabela atributov podaja, so zbrane v tabeli 2;
- Razdelek »*Control*« podaja podrobnejšo opredelitev varnostne kontrole z usmeritvijo, na katero zahtevo SUIV se nanaša;
- Razdelek »*Purpose*« pojasnjuje namen varnostne kontrole, podaja razlago glede smiselnosti in potrebe po implementaciji te kontrole (novost v različici 2022);
- Razdelek »*Guidance*« vsebuje usmeritve za implementacijo te varnostne kontrole;
- Razdelek »*Other information*« zagotavlja dodatno razlago ali usmeritve na morebitne druge dokumente v povezavi z dotično varnostno kontrolo.

Tabela 2: Informacije, zbrane v tabeli atributov za posamezno varnostno kontrolo standarda ISO/IEC 27002:2022

Vir: prirejeno po Flores (2022)

Atribut	**Razlaga**	**Možne vrednosti**[9]
»*Control type*« (slo. tip kontrole)	Kdaj in na kakšen način varnostna kontrola vpliva na možnost realizacije varnostnega incidenta in posledično na stopnjo tveganja.	#Preventive #Detective #Corrective
»*Information security properties*« (slo. načela informacijske varnosti)	H kateremu načelu triade CIA varnostna kontrola doprinese.	#Confidentiality #Integrity #Availability
»*Cybersecurity concepts*« (slo. koncepti kibernetske varnosti)	H kateremu konceptu kibernetske varnosti, definiranim v ISO/IEC TS 27110 (ISO, 2021), varnostna kontrola doprinese.	#Identify #Protect #Detect #Respond #Recover
»*Operational capabilities*« (slo. operativne zmogljivosti)	H kateremu področju zagotavljanja informacijske varnosti v praksi varnostna kontrola doprinese.	#Governance #Asset management #Information protection #Human resource security #Physical security #System and network security #Application security #Secure configuration #Identity and access management #Threat and vulnerability management #Continuity #Supplier relationships security #Legal and compliance #Information security event management #Information security assurance
»*Security domains*« (slo. domene varnosti)	H kateri domeni zagotavljanja varnosti v praksi varnostna kontrola doprinese.	#Governance and Ecosystem #Protection #Defense #Resilience

[9] Glede na to, da se v Sloveniji uporablja angleška različica standarda, so možne vrednosti namenoma zapisane v izvorni obliki in niso prevedene v slovenščino.

4 Diskusija: vpliv sprememb na organizacije

Spremembam standardov v družini ISO/IEC 27000 bodo morale slediti vse organizacije, tako tiste, ki že imajo certifikat skladnosti s standardom ISO/IEC 27001:2013, kot tiste, ki standard v svoje poslovanje šele uvajajo in/ali se pridobitev certifikata skladnosti še niso odločile. Predviden časovni potek uvajanja novih različic standardov v prakso ponazarja slika 7.

Slika 7: Predvideni časovni potek uvajanja novih različic standardov ISO/IEC 27001:2022 in ISO/IEC 27002:2022 v prakso
Vir: prirejeno po Kosutic (2022)

Razvidno je, da je prehodno obdobje za uvedbo 3 leta od izdaje standarda ISO/IEC 27001:2022 in bo tako trajalo do konca oktobra 2025 (NQA, 2022). Certificiranje po prejšnji različici ISO/IEC 27001:2013 je možno opraviti še do konca oktobra 2023. V prvi polovici leta 2023 se začenjajo izobraževanja za presojevalce po novi različici, zato bo pridobitev certifikata skladnosti z novo različico ISO 27001:2022 mogoča od sredine leta 2023 dalje.

Tako kot doslej, certifikat skladnosti z določili ISO/IEC 27001:2022 velja tri leta, pri čemer mora organizacija v drugem in tretjem letu izvajati nadzorne presoje svojega SUIV. Nadzorne presoje so za razliko od celovitih presoj SUIV manj

obsežne, saj se predvideva, da je SUIV certificirane stranke še zadošča zahtevam standarda ISO/IEC 27001.

Organizacije, ki se za certificiranje odločijo v vmesnem obdobju (do vzpostavitve procesa certificiranja po novi različici standarda), se lahko prostovoljno odločijo, katero različico standarda bodo izbrale (ISO/IEC 27001:2013 ali ISO/IEC 27001:2022), vendar se priporoča, da se organizacije, ki se podajajo v certifikacijo prvič, certificirajo po zadnji različici standarda ISO/IEC 27001:2022.

Prehodno obdobje omogoča vsem organizacijam, ki že imajo veljaven certifikat skladnosti z ISO/IEC 27001:2013, nadgradnjo in uskladitev certifikata z novo različico ISO/IEC 27001:2022 (ControlCase, 2022). Organizacije, ki se odločijo za tak korak, morajo svoj SUIV posodobiti skladno z zahtevami standarda ISO/IEC 27001:2022, preden se opravi presoja za prehod. Posodobitve se morajo ustrezno odražati v dokumentaciji, ki mora zagotavljati tudi dokaze, da vsi procesi organizacije, vključeni v SUIV, zadoščajo novim in/ali spremenjenih zahtevam v novi različici ISO/IEC 27001:2022 (NQA, 2022).

Vse presoje skladnosti z ISO/IEC 27001, ki bodo izvedene po oktobru 2025, bodo morale upoštevati določila nove različice ISO/IEC 27001:2022. Za organizacije je pomembno tudi zavedanje, da po izteku prehodnega obdobja preneha veljavnost vseh certifikatov skladnosti s staro različico ISO/IEC 27001:2013.

5 Zaključek

V prispevku smo proučili in sistematično analizirali, katere spremembe prinašata nova standarda ISO/IEC 27001:2022 in ISO/IEC 27002:2022 v primerjavi s preteklima različicama iz leta 2013. Ugotovili smo, da je bilo največ sprememb narejenih v dodatku standarda ISO/IEC 27001, kar pogojuje povsem prenovljeno strukturo standarda ISO/IEC 27002.

Nastale spremembe tangirajo vse organizacije, ki se pri upravljanju informacijske varnosti opirajo na določila standardov ISO/IEC 27001 in 27002. Zaradi splošne uporabnosti in razširjenosti standardov v praksi, je nabor teh organizacij obsežen in vključuje tako javni kot zasebni sektor. Analizirali smo, kaj nastale spremembe

potegnejo za sabo ter v kakšnih časovnih okvirih morajo organizacije ukrepati in nastale spremembe implementirati.

Po našem vedenju predstavlja pričujoči prispevek prvi tovrstni prispevek v slovenskem jeziku. Glede na aktualnost obravnavane problematike menimo, da bodo podane vsebine v veliko pomoč skrbnikom za informacijsko varnost v sleherni organizaciji.

Literatura

Adams, M. (2021, April 7). ISO 27001 Certification: Understanding the Process and Costs. Businesstechweekly. https://www.businesstechweekly.com/legal-and-compliance/iso27001-certification/iso-27001-certification-process-costs/

ControlCase. (2022). Updates and Changes to ISO 27001:2022. https://www.controlcase.com/updates-and-changes-to-iso-270012022/

Flores, M. (2022, March 8). What's New in ISO/IEC 27002: 2022 Updates. Advantio. https://www.advantio.com/blog/whats-new-in-iso/iec-27002-2022-updates

Hyseni, V. (2022, October 25). ISO/IEC 27001 - What are the main changes in 2022? Professional Evaluation and Certification Board [PECB]. https://pecb.com/article/isoiec-27001---what-are-the-main-changes-in-2022

ISO. (2013a). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization [ISO].

ISO. (2013b). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization [ISO].

ISO. (2021). ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines. International Organization for Standardization [ISO].

ISO. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization [ISO].

ISO. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization [ISO].

Kosutic, D. (n.d.). What are the 11 new security controls in ISO 27001:2022? Advisera. Retrieved February 22, 2023, from https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

Kosutic, D. (2022, October 25). ISO 27001:2022 Revision: What has changed? 2013 vs. 2022 version. Advisera. https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/

NQA. (2022). ISO 27001:2022 Transition Guidance. https://www.nqa.com/en-us/transitions/iso-27001-2022

OGCIO. (2022). An Overview of ISO/IEC 27000 family of Information Security Management System Standards. Office of the Government Chief Information Officer. https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/doc/overview_of_iso_27000_family.pdf

Shojaie, B., Federrath, H., & Saberi, I. (2016). Getting the Full Benefits of the ISO 27001 to Develop an ISMS based on Organisations' InfoSec Culture. In N. Clarke & S. Steven Furnell (Eds.), Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). Plymouth University.

Volyntseva, Y. (2021, April 7). ISO 27001 & 27002: Understanding the difference between ISO27001 and ISO27002. Businesstechweekly. https://www.businesstechweekly.com/legal-and-compliance/iso27001-certification/iso-27001-and-iso-27002/