vabilo na seminar

Od zahtev do prakse: Kaj prinaša novi standard SIST EN ISO/IEC 27001:2023

DATUM: 1 12 .2026
URA: 10.00–13.15

KRAJ: LJUBLJANA, SIST, Ulica gledališča BTC 2, predavalnica 2 v 2. nadstropju

www.sist.si

Uvod

Standard ISO/IEC 27001:2022, v Sloveniji privzet kot SIST EN ISO/IEC 27001:2023, Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Sistemi vodenja informacijske varnosti – Zahteve – Dopolnilo A1: Upoštevanje podnebnih sprememb (ISO/IEC 27001:2022/Amd 1:2024) predstavlja mednarodno uveljavljen okvir za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema vodenja informacijske varnosti. Organizacijam omogoča sistematično obvladovanje informacijskih varnostnih tveganj in izbiro ustreznih varnostnih kontrol. Izdaja 2022 je posodobila zahteve, še posebej Dodatek A. Gre za dopolnilo iz leta 2024, ki v kontekstu organizacije obravnava tudi pomen podnebnih sprememb.

Na seminarju bomo primerjali izdaji standarda iz let 2013 in 2022, predstavili spremembe zahtev iz poglavij od 4 do 10 ter poglobljeno obravnavali prenovljene kontrole iz Dodatka A. Posebno pozornost bomo namenili 11 novim kontrolam, uporabi atributov iz SIST EN ISO/IEC 27002:2023 ter praktični prilagoditvi dokumentacije, ocene tveganj in Izjave o uporabnosti (SoA).

Vsebino seminarja bomo dopolnili še s povezavo standarda z aktualnimi zakonodajnimi zahtevami, zlasti direktivo NIS2, slovenskim ZInfV-1 in GDPR. Na konkretnih primerih bomo obravnavali, kako sistem vodenja informacijske varnosti podpira upravljanje tveganj, odgovornost vodstva, obravnavo incidentov in neprekinjenost poslovanja ter kje certifikacija po ISO/IEC 27001 še ne zadošča za dokazovanje zakonske skladnosti. Seminar bo združeval strokovna pojasnila, praktična priporočila in razpravo.

Zakaj bi se seminarja udeležili:

- Pridobili boste pregled nad ključnimi spremembami izdaje 2022 in razumeli, kaj te pomenijo za vzpostavitev, presojo in izboljšanje vašega sistema vodenja informacijske varnosti. Izpostavili bomo, katere procese, evidence in varnostne kontrole je v praksi smiselno ponovno preveriti.

- Spoznali boste 11 novih kontrol in prenovljeno strukturo Dodatka A, vključno z varnostjo oblačnih storitev, spremljanjem groženj, preprečevanjem uhajanja podatkov, varnim kodiranjem in pripravljenostjo IKT na motnje.

- Izvedeli boste, kako standard ISO/IEC 27001 uporabiti kot podlago za izpolnjevanje zahtev ZInfV-1, katere obveznosti pa je treba obravnavati posebej. Odnesli boste konkretne usmeritve za posodobitev ocene tveganj, Izjave o uporabnosti (SoA), notranje presoje in vodstvene preglede.

Komu je seminar namenjen:

- odgovornim za vzpostavitev vodenja informacijske varnosti,
- odgovornim za izvedbo ocene varnostnih tveganj,
- predstavnikom vodstva,
- presojevalcem sistemov vodenja,
- vodjem projektov in vodjem oddelkov za informacijsko tehnologijo,
- organizatorjem informacijskih sistemov in varnostnim inženirjem,
- vsem, ki se ukvarjajo z vzdrževanjem sistema vodenja informacijske varnosti.

Vsebina:

1. Razvoj standarda in spremembe zahtev

- Pregled serije standardov ISO/IEC 27000
- Ključne spremembe v zadevnem standardu (SIST EN ISO/IEC 27001:2023) v primerjavi z izdajo iz leta 2013
- Spremembe zahtev sistema vodenja informacijske varnosti (poglavja 4–10)
- Dopolnilo Amd 1:2024 – Podnebne spremembe

2. Prenovljeni Dodatek A in nove varnostne kontrole

- Nova struktura in razvrstitev 93 varnostnih kontrol v 4 skupine
- Primerjava in povezava (prehod) kontrol med izdajama 2013 in 2022
- Pregled 11 novih kontrol in njihova praktična uporaba

3. ISO/IEC 27002:2022 in praktična uporaba kontrol

- Pet skupin atributov varnostnih kontrol
- Povezovanje kontrol z informacijskimi varnostnimi tveganji
- Praktični primeri izbire in prilagajanja kontrol organizaciji

4. Posodobitev in presojanje sistema vodenja informacijske varnosti

- Posodobitev ocene tveganj in načrta njihove obravnave
- Prilagoditev Izjave o uporabnosti (SoA), politik in postopkov
- Notranje presoje, vodstveni pregledi in nenehno izboljševanje SUVI

5. Povezava standarda z zakonodajnimi zahtevami

- Povezava ISO/IEC 27001 z direktivo NIS2, ZInfV-1 in GDPR
- Ključne zakonodajne zahteve za upravljanje tveganj, incidentov in neprekinjeno poslovanje
- Uporaba sistema vodenja informacijske varnosti pri zagotavljanju zakonodajne skladnosti
- Razlika med certifikacijo ISO/IEC 27001 in izpolnjevanjem zakonskih obveznosti

6. Praktični primeri in razprava

- Primeri dobrih praks in najpogostejših pomanjkljivosti
- Povezovanje tveganj, varnostnih kontrol in dokazil za presojo
- Vprašanja, odgovori in izmenjava izkušenj udeležencev

Kaj boste pridobili z udeležbo?

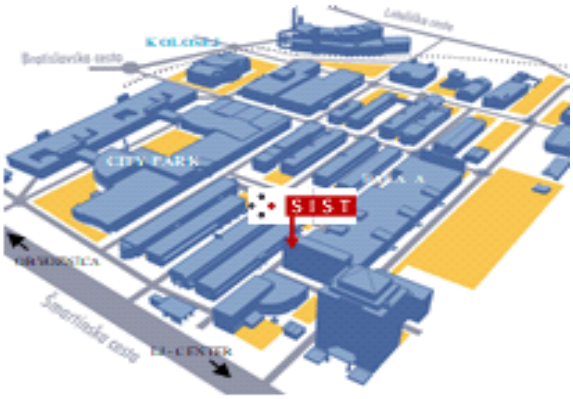
- Razumeli boste ključne spremembe v standardu SIST EN ISO/IEC 27001:2023 in njihove praktične posledice.
- Dobili boste jasne usmeritve za posodobitev dokumentacije, ocene tveganj in izjave o uporabnosti (SoA).
- Spoznali boste novo strukturo Dodatka A, 11 novih kontrol in uporabo atributov SIST EN ISO/IEC 27002:2023.
- Naučili se boste, kako povezati sistem vodenja informacijske varnosti z zahtevami NIS2, ZInfV-1 in GDPR ter prepoznati dodatne zakonske obveznosti.
- Praktične napotke za lažji, nemoten prehod na novo izdajo standarda.
- Ob koncu seminarja boste prejeli odgovore na vaša konkretna vprašanja.

Original novega prevoda standarda SIST EN ISO/IEC 27001:2023 boste udeleženci seminarja prejeli v papirni obliki.

Ponujamo tudi 30 % popust za podjetja, ki prijavijo več zaposlenih.

Kako do nas

SIST se nahaja v nakupovalnem središču BTC, na severnem delu hale A (nekdanji sedež uprave BTC). Predavalnica 2 na SIST je v 2. nadstropju. Ob vseh stavbah nakupovalnega središča so po 9. uri na voljo brezplačna parkirna mesta.



Izvajalec



Dr. Rok Bojanc že več kot 20 let deluje na področju informacijske varnosti, standardizacije, interoperabilnosti in elektronskega poslovanja. Zaposlen je v podjetju ZZI d. o. o., aktivno pa sodeluje tudi v domačih in mednarodnih tehničnih odborih za standardizacijo. Kot član mednarodne delovne skupine ISO/IEC JTC 1/SC 27/WG 1, ki se ukvarja z razvojem in vzdrževanjem standardov za sisteme vodenja informacijske varnosti (vključno s standardom ISO/IEC 27001), sodeluje tudi v tehničnih odborih pri SIST in CEN. Vodi strokovno skupino za razvoj in vzdrževanje standardov eSLOG, je koordinator Slovenskega nacionalnega foruma za eRačun in član skupine eInvoicing Technical Advisory Group pri Evropski komisiji (EK). V svoji doktorski disertaciji je razvil inovativno metodologijo za kvantitativno merjenje informacijske varnosti. Kot docent za področje računalništva in informatike poučuje na Univerzi na Primorskem (UP), Visoki šoli za poslovne vede v Ljubljani ter na Fakulteti za informacijske študije v Novem mestu. Je avtor in soavtor številnih znanstvenih ter strokovnih člankov, knjig in priročnikov s področij informacijske varnosti, računalniških omrežij, strežniških sistemov in elektronskega poslovanja, poleg tega pa redno predava na domačih in mednarodnih konferencah ter seminarjih.

PRIJAVNICA – 2026-14/1

Od zahtev do prakse: Kaj prinaša novi standard SIST EN ISO/IEC 27001:2023

1.12.2026

Ime in priimek udeleženca	
Naziv organizacije/podjetja	
Naslov	
Davčna številka	
Telefon	
E-pošta	
Datum	
Podpis in žig	

PRIJAVE: prijavnice pošljite najkasneje do 27.11.2025 na Slovenski inštitut za standardizacijo (SIST), Ulica gledališča BTC 2, SI-1000 Ljubljana, po navadni ali po elektronski pošti na seminarji@sist.si.

Število mest je omejeno. Prijavnica velja kot naročilnica.

KOTIZACIJA:
Kotizacija za udeležbo znaša 212,00 EUR + 22 % DDV:

- člani SIST in SIST/TC imajo pri kotizaciji 20 % popusta (cena z DDV in upoštevanim popustom je 206,91 EUR),
- organizacije, ki prijavijo 2 zaposlena, imajo pri kotizaciji 5 % popusta (cena z DDV in upoštevanim popustom za posameznika je 245,71 EUR),
- organizacije, ki prijavijo 3 ali več zaposlenih, imajo pri kotizaciji 30 % popusta (cena z DDV in upoštevanim popustom za posameznika je 181,05 EUR).

Popusti se ne seštevajo.

V kotizacijo so vključeni gradivo, original prevod standarda SIST EN ISO/IEC 27001 (papirna oblika), potrdilo o udeležbi in postrežba (kava, čaj, rogljički) med odmorom.

Vaša prijava na seminar je sprejeta, ko prejmete potrditev po elektronski pošti.
Račun za kotizacijo prejmete po izvedbi seminarja in ga plačate v roku, ki je naveden na računu.

ODPOVED: zadnji rok za odjavo udeleženca je 3 delovne dni pred seminarjem. V tem primeru vam kotizacije ni potrebno plačati. Pri odjavah po tem roku ali neudeležbi, je kotizacijo na osnovi izdanega računa za seminar potrebno v celoti poravnati.

V primeru premajhnega števila udeležencev si pridržujemo pravico do odpovedi seminarja. Vnaprej vplačano kotizacijo vam v tem primeru vrnemo.