Informacijska sigurnost i usklađivanje s GDPR-om – osposobljavanje i izobrazba

Informacija sigurnost, upravljanje rizicima i usklađenost sa zakonskom regulativom zaštite podataka i privatnosti neke su od najvažnijih stavaka u osiguravanju uspješnog poslovanja organizacija. Međunarodni ISO standardi predstavljaju skup konkretnih smjernica i zahtjeva sukladno najboljim svjetskim praksama za unaprjeđivanje poslovnih procesa svih vrsta organizacija.

Međunarodni standard **ISO/IEC 27001 - *Sustav upravljanja informacijskom sigurnosti* (ISMS)** omogućava uspostavljanje dobro strukturiranih procesa koji organizaciji omogućavaju postizanje visoke razine sigurnosti sustava iz internih i eksternih aspekata, osiguravanje kontinuiteta poslovanja, olakšano usklađivanje i praćenje obvezujuće zakonske regulative zaštite podataka i privatnosti (GDPR) te praćenje učinkovitosti cijelog sustava bazirano na kvalitetnom upravljanju sigurnosnim i regulatornim rizicima.

Međunarodni standard **ISO/IEC 27701 - *Sustav upravljanja informacijama o privatnosti* (PIMS)** predstavlja skup priznatih standardiziranih alata, tehnika i kontrola za zadovoljavanje organizacijskih i tehničkih mjera u usklađivanju s europskom pravnom regulativom zaštite osobnih podataka (GDPR).

TÜV Croatia, članica TÜV NORD Group omogućila je proširen portfelj osposobljavanja i izobrazbe stručnjaka vezanih uz ova značajna i sve traženija područja djelovanja u organizacijama, a koje su dostupne i u *tailor-made* formi te prilagođene individualnim potrebama pojedine organizacije.

Za sve dodatne informacije o edukacijama, certifikacijama sustava i ostalim uslugama vezanim uz standarde informacijske sigurnosti i usklađivanje s GDPR-om možete nas kontaktirati na e-mail: *edukacija@tuv-croatia.hr*

Cilj edukacije

Osiguravanje kompetencija polaznika za kvalitetnu pripremu i provedbu te kontinuirano nadziranje sustava upravljanja informacijskom sigurnosti i privatnosti u organizaciji te osiguravanje kompetencija za kontinuirano praćenje usklađenosti organizacije s regulatornim okvirom vezanim uz zaštitu podataka i privatnosti (GDPR).

Tko bi trebao sudjelovati

Sve odgovorne osobe koje su u vlastitim organizacijama zadužene za upravljanje informacijskom sigurnošću, usklađivanje projekata i organizacijskih procesa s GDPR-om, svi stručnjaci koji žele steći potrebna znanja i certifikate ISO/IEC 27001 ili ISO/IEC 27701, voditelji odjela za internu reviziju i svi koji se bave internom revizijom ili to planiraju, pravnici, te svi koji žele naučiti kako se uvodi, primjenjuje ili ocjenjuje sustav upravljanja informacijskom sigurnošću ili sustav upravljanja informacijama o privatnosti odnosno osobnim podacima.

Izobrazba i osposobljavanje

TÜV NORD Akademija polaznicima ovih edukacija omogućava izbor različitih razina stjecanja kompetencija u područjima informacijske sigurnosti i usklađivanja s GDPR-om u kontekstu svladavanja konkretnih tehnika i alata za unaprjeđivanje procesa organizacije.

Stjecanje TÜV NORD Group certifikata osposobljenosti iz ovih područja polazniku predstavlja dokaz posjedovanja potrebnih stručnih znanja za uspješno uvođenje i auditiranje sustava upravljanja informacijskom sigurnosti i privatnosti u aspektima (ovisno o položenoj razini):

1. Stručna znanja koja će organizaciji pomoći u uvođenju sustava upravljanja informacijskom sigurnosti sukladna ISO/IEC 27001 i ISO/IEC 27701 standardima
2. Tehnike i alate za kvalitetno upravljanje rizicima informacijske sigurnosti i zakonske usklađenosti vezane uz organizacijske i tehničke mjere
3. Kvalitetno provođenje nadzora, izvedbu revizija sustava, kontinuirano poboljšavanje procesa i izvještavanje uprave

Razine stjecanja kompetencija i moduli

Edukacijski moduli za stjecanje kompetencija stručnjaka za uvođenje i auditiranje sustava upravljanja informacijskom sigurnosti ISO/IEC 27001 i usklađivanja sa europskom zakonskom regulativom zaštite podataka (GDPR) putem ISO/IEC 27701 podijeljeni su na tri razine:

ISO/IEC 27001 Sustavi upravljanja informacijskom sigurnosti

1. **ISO/IEC 27001 Interni auditor**
2. **ISO/IEC 27001 Lead Implementer**
3. **ISO/IEC 27001 Lead Auditor**

ISO/IEC 27701 Sustavi upravljanja informacijama o privatnosti (usklađivanje s GDPR-om)

1. **ISO/IEC 27701 Interni auditor**
2. **ISO/IEC 27701 Lead Implementer**
3. **ISO/IEC 27701 Lead Auditor**

Navedene edukacije dostupne su na hrvatskom i engleskom jeziku i u verzijama on-site (u prostorijama TÜV Croatia, Zagreb i Sarajevo) te interaktivnog e-učenja (on-line).

Stjecanje certifikata

Na kraju svake edukacije polaznici pišu ispit koji je uključen u cijenu edukacije. Polaznici koji su uspješno položili ispit dobivaju certifikat od TÜV Croatia d.o.o. TÜV NORD Group koji je priznat kod svih međunarodnih institucija *(TÜV NORD Certificate ili CQI/IRCA TÜV NORD Certifikat, ovisno o vrsti edukacije)*, dok polaznici koji nisu uspješno položili ispit dobivaju potvrdu o prisustvovanju edukaciji (*TÜV NORD Certificate of Attendance*) uz mogućnost ponovnog pristupanja ispitu unutar godine dana.

Za sve dodatne informacije o edukacijama, certifikacijama sustava i ostalim uslugama vezanim uz standarde informacijske sigurnosti i usklađivanje s GDPR-om možete nas kontaktirati na e-mail: *edukacija@tuv-croatia.hr*

Program izobrazbe

Pregled svih modula i razina stjecanja certifikata nalazi se u navedenim tablicama **u nastavku dokumenta**.

TÜV Croatia, članica TÜV NORD Group omogućila je proširen portfelj osposobljavanja i izobrazbe stručnjaka vezanih uz ova značajna i sve traženija područja djelovanja u organizacijama, a koje su dostupne i u *tailor-made* formi te prilagođene individualnim potrebama pojedine organizacije.

Za sve dodatne informacije o edukacijama, certifikacijama sustava i ostalim uslugama vezanim uz standarde informacijske sigurnosti i usklađivanje s GDPR-om možete nas kontaktirati na e-mail: *edukacija@tuv-croatia.hr*

Program izobrazbe

Certificirani stručnjak implementacije i auditiranja sustava upravljanja informacijskom sigurnosti prema ISO/IEC 27001 standardu

ISO/IEC 27001 Sustavi upravljanja informacijskom sigurnosti Sigurnosne tehnike i zahtjevi - izobrazba i osposobljavanje			
Moduli i razine	**Interni Auditor**	**Lead Implementer**	**Lead Auditor**
Osnovni principi i koncepti sustava upravljanja ISO/IEC 27001	x	x	x
Karakteristike i povezanost ISO/IEC 27001, ISO/IEC 27002 i ISO/IEC 27701	x	x	x
Određivanje opsega sustava upravljanja informacijskom sigurnosti	x	x	x
Izrada i evaluacija plana implementacije sustava upravljanja informacijskom sigurnosti	x	x	x
Upravljanje projektom	x	x	x
Upravljanje dokumentiranim informacijama	x	x	x
Osnove upravljanja informacijama o privatnosti u organizaciji i upoznavanje sa zahtjevima standarda, tehničkim i organizacijskim mjerama te identifikacija relevantnog regulatornog okvira organizacije	x	x	x
Napredno razumijevanje zahtjeva standarda, smjernica, ciljeva kontrola i kontrola organizacijskih i tehničkih aspekata			
Primijenjene organizacijske i tehničke mjere u uvođenju i auditiranju sustava ISO/IEC 27001 sukladno ISO/IEC 27002 smjernicama		x	x
Razumijevanje organizacije i njenog konteksta te potreba i očekivanja zainteresiranih strana	x	x	x
Politike informacijske sigurnosti, odgovornosti i ovlasti		x	x
Napredno upravljanje rizicima: definiranje ciljeva, procjena i obrada rizika, operativni nadzor		x	x
Resursi, kompetencije, svijest i komunikacija	x	x	x
Nadzor, mjerenje, analiza i vrednovanje performansi sustava; Upravina ocjena	x	x	x
Nesukladnosti i korektivne radnje te trajno poboljšavanje sustava	x	x	x
Specifičnosti Aneksa A – ciljevi kontrola i kontrole u provedbi tehničkih i organizacijskih mjera		x	x
Specifičnosti dopune sustava ISO/IEC 27001 sigurnosnim tehnikama i zahtjevima sustava upravljanja privatnosti informacija ISO/IEC 27701 u usklađivanju s GDPR	x	x	x
Auditiranje / Revizija			
Osnovni principi i koncepti u auditiranju sustava upravljanja ISO/IEC 27001	x		
Napredno razumijevanje konteksta auditiranja sustava upravljanja ISO/IEC 27001			x
Osnove tehnika auditiranja i izrade audit plana	x		
Primijenjeno auditiranje i izrade audit planova			x
Osnove pripreme, provedbe i izvještavanje s audita	x		
Primijenjena priprema, provedba i izvještavanje s audita			x
Trajanje i ispit			
Trajanje	2 dana	5 dana	5 dana
Certifikacijski ispit	x	x	X

Program izobrazbe

Certificirani stručnjak implementacije i auditiranja sustava upravljanja informacijama o privatnosti prema ISO/IEC 27701 standardu

ISO/IEC 27701 Sustavi upravljanja informacijama o privatnosti Sigurnosne tehnike - izobrazba i osposobljavanje u uvođenju organizacijskih i tehničkih mjera za usklađivanje s GDPR-om			
Moduli i razine	**Interni Auditor**	**Lead Implementer**	**Lead Auditor**
Osnovni principi i koncepti sustava upravljanja ISO/IEC 27701	x	x	x
Karakteristike i povezanost ISO/IEC 27001, ISO/IEC 27002 i ISO/IEC 27701	x	x	x
Određivanje opsega sustava upravljanja informacijama o privatnosti (PIMS)	x	x	x
Izrada i evaluacija plana implementacije sustava upravljanja informacijama o privatnosti i usklađivanja s GDPR-om	x	x	x
Upravljanje projektom	x	x	x
Upravljanje dokumentiranim informacijama	x	x	x
Osnove upravljanja informacijama o privatnosti u organizaciji i upoznavanje sa zahtjevima standarda, tehničkim i organizacijskim mjerama te identifikacija relevantnog regulatornog okvira organizacije	x	x	x
Napredno razumijevanje zahtjeva standarda, smjernica, ciljeva kontrola i kontrola organizacijskih i tehničkih aspekata u usklađivanju s GDPR-om			
Organizacijske i tehničke mjere u uvođenju i auditiranju sustava ISO/IEC 27701	x	x	x
Zahtjevi specifični za sustav upravljanja informacijama o privatnosti (PIMS) vezani za normu sustava upravljanja informacijskom sigurnosti ISO/IEC 27001 - napredno upravljanje rizicima, kontekst organizacije i vrednovanje učinkovitosti sustava		x	x
Operativne smjernice specifične za sustav upravljanja informacijama o privatnosti (PIMS) vezane za normu ISO/IEC 27002 - Politike informacijske sigurnosti, Mobilni uređaji i rad na daljinu, Raskid i promjena radnog odnosa, Upravljanje imovinom, kriptografija, Fizička sigurnost i sigurnost povezana s okolišem, Sigurnost operacija, Upravljanje incidentima informacijske sigurnosti, Aspekti informacijske sigurnosti za upravljanje kontinuitetom poslovanja i Sukladnost s regulatornim i drugim obvezama	x	x	x
Dodatni zahtjevi prema normi ISO/IEC 27002 za voditelje i izvršitelje obrade osobno identificirajućih podataka - Uvjeti za prikupljanje i obradu, svrha i pravni temelj, evidencija obrade podataka, PIA, ugovori s trećim stranama; Obveze prema vlasnicima osobnih podataka, organizacijske i tehničke mjesre u osiguravanju propisanih prava ispitanicima; Tehnički aspekti integriranih i predefiniranih sustava upravljanja informacijama o privatnosti (Privacy by design i Privacy by default); Dijeljenje i prijenos osobno identificirajućih podataka trećim stranama		x	x
Specifičnosti Aneksa: Referentni ciljevi kontrola i kontrole za voditelje i izvršitelje obrade specifični za Sustav upravljanja informacijama o privatnosti (PIMS) u usporedbi za zahtjevima GDPR-a		x	x

Primjena norme ISO/IEC 27701 na norme ISO/IEC 27001 i ISO/IEC 27002	x	x	x
Auditiranje / Revizija			
Osnovni principi i koncepti u auditiranju sustava upravljanja ISO/IEC 27701	x		
Napredno razumijevanje konteksta auditiranja sustava upravljanja ISO/IEC 27701			x
Osnove tehnika auditiranja i izrade audit plana	x		
Primijenjeno auditiranje i izrade audit planova			x
Osnove pripreme, provedbe i izvještavanja s audita	x		
Primijenjena priprema, provedba i izvještavanje s audita			x
Trajanje i ispit			
Trajanje	2 dana	5 dana	5 dana
Certifikacijski ispit	x	x	X

Dobrodošli u TÜV NORD svijet!