Ovladavanje implementacijom i upravljanjem sistemom upravljanja informacijskom sigurnošću (ISMS) baziranom na ISO 27001

Rezime

Ovaj petodnevni intenzivni trening omogućuje polaznicima da razviju potrebnu stručnost kako bi pomogli organizacije u implementaciji i upravljanju sistemom upravljanja informacijskom sigurnošću (ISMS) baziranu na ISO / IEC 27001:2013. Polaznici će, također, dobiti temeljno razumijevanje najboljih praksi temeljem kojih se provode kontrole informacijske sigurnosti iz svih područja ISO 27002. Ovaj trening je u skladu s utvrđenim praksama project menadžmenta ISO 10006 (Quality Management Systems - Smjernice za upravljanje kvalitetom u projektima). Ovaj trening je također u potpunosti kompatibilan sa ISO 27003 (smjernice za primjenu u ISMS), ISO 27004 (mjerenje informacijske sigurnosti) i ISO 27005 (Upravljanje rizicima u informacijskoj sigurnosti).

Kome je trening namjenjen?

- Projekt menadžeri ili konsultanti koji žele pripremiti i podržati organizaciju u implementaciji sistema upravljanja informacijskom sigurnošću (ISMS)
- ISO 27001 auditori/revizori koji žele da u potpunosti razumiju proces implementacije sistema upravljanja informacijskom sigurnošću
- CxO i viši menadžeri odgovorni za IT menadžment u preduzeću i upravljanje rizicima preduzeća
- Članovi tima za informacijsku sigurnost
- Stručni savjetnik za informacijske tehnologije
- Tehnički stručnjaci koji se žele pripremiti za funkciju informacijske sigurnosti ili za funkciju upravljanja ISMS projektima.

Ciljevi treninga

- Razumjeti implementaciju sistema upravljanja informacijskom sigurnošću u skladu sa ISO 27001
- Steći cjelovit uvid u koncepte, pristupe, standarde, metode i tehnike potrebne za učinkovito upravljanje sistemom upravljanja informacijskom sigurnošću
- Razumjeti odnos između komponenti sistema upravljanja informacijskom sigurnošću, uključujući i upravljanje rizikom, kontrole i usklađenosti sa zahtjevima različitih interesnih grupa organizacije
- Steći potrebnu stručnost kako bi podržali organizaciju u implementaciji, upravljanju i

održavanju ISMS kako je navedeno u ISO 27001
- Steći potrebno znanje za upravljanje timom za implementaciju standarda ISO 27001
- Razviti znanja i vještine potrebne za savjetovanje organizacije o najboljim praksama u upravljanju informacijskom sigurnošću
- Unaprijediti sposobnosti za analizu i donošenje odluka u kontekstu upravljanja informacijskom sigurnošću

Agenda treninga

Dan 1: Uvod u sistem upravljanja informacijskom sigurnošću (ISMS) pojmovi kako je propisano ISO 27001; Uvođenje ISMS

- Uvod u sisteme upravljanja i procesni pristup
- Predstavljanje standarda ISO 27001, ISO 27002 i ISO 27003 i regulatorni okvir
- Temeljna načela informacijske sigurnosti
- Preliminarna analiza i utvrđivanje nivoa zrelosti postojećeg sistema upravljanja informacijskom sigurnošću prema ISO 21827
- Pisanje poslovnog slučaja i projektnog plana za implementaciju ISMS

Dan 2: Planiranje implementacije ISMS prema ISO 27001

- Definiranje opsega/djelokruga ISMS-u
- Razvoj ISMS-a i politika informacijske sigurnosti
- Izbor pristup i metodologije za procjenu rizika
- Upravljanje rizicima: identifikacija, analiza i obrada rizika (pisanje prema smjernicama iz ISO 27005)
- Izrada Izvještaja o primjenjivosti (SoA - Statement of Applicability)

Dan 3: Implementacija ISMS prema ISO 27001

- Implementacija okvira za upravljanje dokumentima
- Dizajn kontrola i pisanje procedura
- Implementacija kontrola
- Razvoj treninga i programa podizanja svijesti, kao i komuniciranje informacije o informacijskoj sigurnosti
- Incident management (na temelju smjernica iz ISO 27035)
- Operativno upravljanje/menadžment ISMS-a

Dan 4: Upravljanje, nadzor, mjerenje i poboljšanja ISMS; certifikacijski audit ISMS-a

- Kontrola i nadzor ISMS-a
- Razvoj metrika, pokazatelja uspješnosti i kontrolne tabele/dashboard u skladu s ISO 27004
- ISO 27001 interna revizija/audit
- Upravljanje analizom ISMS-a
- Implementacija programa kontinuiranog poboljšanja
- Priprema za certifikacijski audit ISO 27001

Dan 5: Certifikacijski ispit

Preduvjeti

ISO 27001 Osnovni certifikat ili osnovno poznavanje ISO 27001 se preporučljivo

Edukativni pristup

- Ovaj trening se temelji i na teoriji i praksi:
- Sesije predavanja s konkretnim primjerima temeljenim na stvarnim slučajevima
- Praktične vježbe na temeljene na potpunim studijama slučaja, uključujući interpretaciju uloga i usmena izlaganja
- Pregled vježbi kako bi se pomogla priprema ispita
- Vježba testa slična certifikacijskom ispitu
- Kako bi praktične vježbe bile učinkovite, broj polaznika je ograničen trening

Ispit i certificiranje

- "Certificirani ISO / IEC 27001 Lead Implementator" ispit u potpunosti zadovoljava zahtjeve PECB program ispitivanja i certificiranja (ECP). Ispit pokriva sljedeće oblasti:
- Oblast 1: Temeljna načela i koncepti informacijske sigurnosti
- Oblast 2: Najbolje prakse kontrola informacijske sigurnosti bazirane na ISO 27002
- Oblast 3: Planiranje ISMS prema ISO 27001
- Oblast 4: Implementacija ISMS prema ISO 27001
- Oblast 5: Ocjena rada, nadzor i mjerenje ISMS-a prema ISO 27001
- Oblast 6: Kontinuirano unaprjeđivanje ISMS-a prema ISO 27001
- Oblast 7: Priprema za ISMS certifikacijskog audita
- "Certificirani ISO / IEC 27001 Lead Implementator" ispit je dostupan je na raznim jezicima (kompletan popis jezika se može se naći na formularu aplikacije za ispit)

- Trajanje ispita: 3 sata
- Za više informacija o ispitu, pogledajte link na PECB internet portalu ISO 27001 Lead Implementer Exam
- Nakon uspješno završenog ispita, polaznici mogu se prijaviti za uvjerenja Certificiranog ISO / IEC 27001 Provisional Implementatora, Certificiranog ISO / IEC 27001 Implementatora ili Cerificiranog ISO / IEC 27001 Lead Implementatora, ovisno o nivou posjedovanog iskustva

- Potvrda se izdaje polaznicima koji su uspješno položili ispit, a odgovaraju svim drugim zahtjevima koji se odnose na odabrano uvjerenje
- Za više informacija o ISO 27001 certifikaciji i PECB procesu certifikacije, pogledajte link PECB ISO 27001 Lead Implementer

Opće informacije

- Certifikacijska naknada je uključena u cijenu ispita
- Studentski priručnik s više od 450 stranica informacija i praktičnih primjera će biti podijeljen polaznicima
- Potvrda o sudjelovanju od 31 CPD (Continuing Professional Development - kontinuirano stručno usavršavanje) kredit će biti izdan polaznicima
- U slučaju da polaznik ne položi ispit, polaznik može ponovno besplatno polagati ispit pod određenim uvjetima