**\* OVO JE BESPLATNI OGLEDNI PREDLOŽAK DOKUMENTA \***

**Prilog 3 – Kontrolni popis za interni audit prema normama ISO 27001 i ISO 22301**

# Kontrolni popis za interni audit prema normi ISO 27001

|  |  |  |  |
| --- | --- | --- | --- |
| **Točka / mjera** | **Zahtjev norme ISO 27001** | **Usklađeno Da/Ne** | **Dokaz** |
| 4.2 | Je li organizacija odredila zainteresirane strane? |  |  |
| 4.2 | Postoji li popis svih zahtjeva zainteresiranih strana? |  |  |
| 4.3 | Je li opseg dokumentiran, s jasno definiranim granicama i sučeljima? |  |  |
| 5.1 | Je su li opći ciljevi ISMS-a u skladu sa strateškim smjerom? |  |  |
| 5.1 | Osigurava li menadžment da ISMS ostvari svoje ciljeve? |  |  |
| 5.2 | Postoji li Politika informacijske sigurnosti s ciljevima ili okvirom za postavljanje ciljeva? |  |  |
| 5.2 | Jesu li zaposlenici unutar organizacije upoznati s Politikom informacijske sigurnosti? |  |  |
| 5.3 | Jesu li uloge i odgovornosti za informacijsku sigurnost dodijeljene i priopćene? |  |  |
| 6.1.2 | Je li proces procjene rizika dokumentiran, uključujući i kriterije prihvatljivosti rizika i kriterije za procjenu rizika? |  |  |
| 6.1.2, 8.2 | Jesu li prepoznati rizici, njihovi vlasnici, vjerojatnost, posljedice i razina rizika; jesu li ti rezultati dokumentirani? |  |  |
| 6.1.3 | Je li proces obrade rizika dokumentiran, uključujući opcije obrade rizika? |  |  |
| 6.1.3, 8.3 | Jesu li obrađeni svi neprihvatljivi rizici koristeći opcije i mjere iz Aneksa A; jesu li ti rezultati dokumentirani? |  |  |
| 6.1.3 | Je li Izvješće o primjenjivosti izrađeno, s obrazloženjima i statusom za svaku sigurnosnu mjeru (kontrolu)? |  |  |
| 6.1.3, 8.3 | Postoji li Plan obrade rizika odobren od strane vlasnika rizika? |  |  |
| 6.2 | Određuje li Plan obrade rizika tko je odgovoran za uvođenje koje mjere, s kojim resursima, koji su rokovi te koja se metoda procjene koristi? |  |  |
| 7.1 | Postoje li odgovarajući resursi za sve elemente ISMS-a? |  |  |
| 7.2 | Jesu li utvrđena potrebna znanja, provedene obuke i vode li se zapisi o stečenim znanjima? |  |  |
| 7.3 | Je li osoblje svjesno da postoji Politika informacijske sigurnosti, svoje uloge te posljedica nepridržavanja pravila? |  |  |
| 7.4 | Postoji li proces komunikacije povezan s informacijskom sigurnošću, uključujući odgovornosti i što je potrebno prenositi? |  |  |
| 7.5 | Postoji li postupak za upravljanje dokumentima i zapisima, uključujući tko pregledava i odobrava dokumente, gdje se i kako objavljuju, pohranjuju i štite? |  |  |
| 7.5 | Nadziru li se dokumenti vanjskog podrijetla? |  |  |
| 8.1 | Jesu li procesi koje izvode vanjski suradnici identificirani i nadzirani? |  |  |
| 9.1 | Je li utvrđeno što treba mjeriti, kojom metodom, tko je odgovoran, tko će analizirati i ocijeniti rezultate? |  |  |
| 9.1 | Jesu li rezultati mjerenja dokumentirani i prijavljeni odgovornim osobama? |  |  |
| 9.2 | Postoji li program audita koji definira vrijeme, odgovornosti, izvještavanje, kriterije za audit te opseg audita? |  |  |
| 9.2 | Jesu li interni auditi provedeni u skladu s programom audita, jesu li rezultati preneseni kroz interno izvješće o auditu i jesu li pokrenute relevantne popravne radnje? |  |  |
| 9.3 | Obavlja li menadžment pregled redovito i jesu li rezultati dokumentirani u zapisniku sa sastanka? |  |  |
| 9.3 | Je li menadžment odlučio o svim ključnim pitanjima važnim za uspjeh ISMS-a? |  |  |
| 10.1 | Reagira li organizacija na svaku nesukladnost? |  |  |
| 10.1 | Razmatra li organizacija uklanjanje uzroka nesukladnosti i poduzima li popravne radnje gdje je potrebno? |  |  |
| 10.1 | Jesu li sve nesukladnosti zabilježene, zajedno s popravnim radnjama? |  |  |
| A.5.1 | Jesu li sve potrebne Politike informacijske sigurnosti odobrene od strane menadžmenta i jesu li objavljene? |  |  |
| A.5.1 | Jesu li sve Politike informacijske sigurnosti pregledane i ažurirane? |  |  |
| A.5.2 | Jesu li sve odgovornosti informacijske sigurnosti jasno definirane, kroz jedan ili više dokumenata? |  |  |
| ***(ostatak redaka ne prikazuje se u ovom oglednom predlošku)*** | | | |
| … | … |  |  |

# Kontrolni popis za Interni audit prema normi ISO 22301

|  |  |  |  |
| --- | --- | --- | --- |
| **Točka** | **Zahtjev norme** | **Usklađeno Da/Ne** | **Dokaz** |
| 4.2.1 | Je li organizacija odredila zainteresirane strane? |  |  |
| 4.2.2 | Postoji li popis svih zahtjeva zainteresiranih strana? |  |  |
| 4.2.2 | Je li organizacija odredila proces za upravljanje primjenjivim i regulatornim zahtjevima? |  |  |
| 4.3 | Je li opseg dokumentiran, definirajući koji su proizvodi i usluge uključeni i jesu li objašnjena izuzeća? |  |  |
| 5.1 | Podržava li top menadžment aktivno aktivnosti kontinuiteta poslovanja? |  |  |
| 5.2 | Je li upravljanje kontinuitetom poslovanja (BCMS) spojivo sa svrhom organizacije? |  |  |
| 5.2 | Pokazuje li top menadžment svoju posvećenost pružanjem svih resursa i objašnjava li važnost kontinuiteta poslovanja? |  |  |
| 5.2 | Postoji li Politika kontinuiteta poslovanja i utvrđuje li ona okvir za postavljanje ciljeva? |  |  |
| 5.2 | Je li unutar organizacije objavljeno da postoji Politika kontinuiteta poslovanja? |  |  |
| 5.3 | Je li imenovana odgovorna osoba za BCMS i ima li ta osoba dovoljno ovlasti? |  |  |
| 5.3 | Jesu li uloge i odgovornosti za kontinuitet poslovanja dodijeljene i priopćene? |  |  |
| 6.1 | Je li organizacija utvrdila sve rizike i prilike? |  |  |
| 6.1 | Je li organizacija planirala mjere za rješavanje utvrđenih rizika i prilika? |  |  |
| 6.2.1 | Jesu li određeni ciljevi kontinuiteta poslovanja te jesu li priopćeni svim relevantnim zaposlenicima? |  |  |
| 6.2.1 | Jesu li ciljevi kontinuiteta poslovanja mjerljivi; prate li se i ažuriraju? |  |  |
| 6.2.2 | Je li utvrđeno sljedeće: koraci potrebni za ostvarenje ciljeva, tko je odgovoran, koji su rokovi i koji su resursi potrebni? |  |  |
| 6.3 | Provode li se potrebne promjene za BCMS planski? |  |  |
| 7.1 | Postoje li odgovarajući resursi za sve elemente BCMS-a? |  |  |
| ***(ostatak redaka ne prikazuje se u ovom oglednom predlošku)*** | | | |
| … | … |  |  |

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

(Kako biste pristupili potpunoj verziji dokumenta molimo Vas da kupite ISO 27001/ISO 22301 Paket dokumentacije za interni audit   
<https://advisera.com/27001academy/hr/iso-27001-iso-22301-paket-za-interni-audit/>)