					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P33					Naziv dokumenta: **Politika revizije i praćenja usklađenosti**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontrole 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR EU	Članci 24, 32, 33	
Direktiva EU NIS2	Članak 21(2)(g), 27	
Uredba EU DORA	Članci 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Svrha

1.1 Svrha ove politike jest uspostaviti i urediti program revizije i praćenja usklađenosti organizacije radi sljedećeg:

1.1.1 provjere djelotvornosti sigurnosnih kontrola i kontrola privatnosti

1.1.2 osiguravanja usklađenosti s primjenjivim standardima, pravnim okvirom i ugovornim obvezama

1.1.3 pravodobnog otkrivanja nesukladnosti, neučinkovitosti i rizika usklađenosti

1.1.4 potpore kontinuiranom poboljšavanju i spremnosti za certifikaciju, procjene i regulatorne nadzore

1.2 Ova politika podupire cjelovitost i zrelost sustava upravljanja informacijskom sigurnošću (ISMS) uvođenjem strukturiranih revizijskih praksi i praksi praćenja koje se temelje na riziku i dokazima.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve:

2.1.1 interne poslovne jedinice, funkcije i odjele

2.1.2 fizičke lokacije, okruženja u oblaku, SaaS platforme i ugovorene vanjske usluge

2.1.3 informacijske sustave, aplikacije, infrastrukturu i informacijsku imovinu obuhvaćenu opsegom ISMS-a

2.1.4 zaposlenike, ugovorne izvođače i pružatelje usluga trećih strana koji imaju revizijske obveze ili obveze usklađenosti

2.2 Politika obuhvaća:

2.2.1 unutarnje revizije

2.2.2 vanjske i certifikacijske revizije

2.2.3 tehničko praćenje usklađenosti

2.2.4 revizije dobavljača i trećih strana

2.2.5 korektivne i preventivne radnje (CAPA)

2.2.6 metrike, nadzorne ploče i procese izvješćivanja

2.3 Primjenjuje se na sve relevantne okvire kojima organizacija podliježe, uključujući ISO/IEC 27001, GDPR, NIS2, DORA i SOC 2 te druge.

3. Ciljevi

3.1 Provjeriti primjerenost i djelotvornost implementiranih kontrola, politika i postupaka u okviru ISMS-a i povezanih okruženja.

3.2 Identificirati i otkloniti sve nedostatke, nesukladnosti ili manjkavosti u usklađenosti prije nego što prerastu u incidente ili povrede.

3.3 Osigurati trajnu spremnost za interne upravljačke preglede, vanjske revizije i neovisnu certifikaciju.

3.4 Izraditi dokazive revizijske dokaze i revizijske tragove kao potporu upitima regulatornih tijela, pravnim postupcima ili zahtjevima klijenata odnosno partnera za pružanje potvrda.

3.5 Integrirati rezultate revizije u šire aktivnosti organizacije povezane s upravljanjem rizicima, sigurnosnim metrikama i kontinuiranim poboljšavanjem.

4. Uloge i odgovornosti

4.1 Voditelj unutarnje revizije / rukovoditelj usklađenosti

4.1.1 Planira, raspoređuje i provodi unutarnje revizije na temelju prioriteta rizika.

4.1.2 Održava registar revizija, koordinira revizijske aktivnosti i prati provedbu korektivnih radnji.

4.2 Glavni direktor za informacijsku sigurnost (CISO)

4.2.1 Osigurava da opseg revizije obuhvaća sve relevantne elemente ISMS-a i kontrole iz Priloga A.

4.2.2 Nadzire provjeru CAPA aktivnosti i integrira rezultate revizije u program informacijske sigurnosti.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku moraju pregledati najmanje jednom godišnje rukovoditelj usklađenosti i CISO ili ranije kao odgovor na:

9.1.1 promjene regulatornih, ugovornih ili certifikacijskih okvira

9.1.2 značajne nalaze revizije ili ponovljene neuspjehe kontrola

9.1.3 organizacijsko restrukturiranje ili promjene GRC sustava

9.1.4 preporuke vanjskih revizora ili povratne informacije regulatora

9.2 U postupku pregleda mora se procijeniti:

9.2.1 metodologija planiranja revizije i učestalost

9.2.2 promjene u opsegu ISMS-a ili infrastrukturi

9.2.3 ažuriranja kataloga kontrola ili pravnog registra

9.2.4 dosljednost i kvaliteta revizijskih dokaza i CAPA procesa

9.3 Sve promjene politike moraju biti:

9.3.1 dokumentirane u repozitoriju pod verzijskom kontrolom

9.3.2 odobrene od strane izvršnog rukovodstva

9.3.3 priopćene svom pogođenom osoblju i integrirane u ažurirane postupke i programe podizanja svijesti

9.4 Provjera nakon pregleda mora potvrditi da su ažurirani zahtjevi odraženi u registru revizija, alatima za usklađenost i internim nadzornim pločama za praćenje.

10. Povezane politike i poveznice

10.1 Ova je politika usklađena sa sljedećim povezanim organizacijskim politikama:

10.1.1 P1 – Politika informacijske sigurnosti: definira ISMS i uspostavlja odgovornost za usklađenost i kontinuirano poboljšavanje

10.1.2 P5 – Politika upravljanja promjenama: osigurava revizijsku sljedivost promjena infrastrukture i konfiguracije koje utječu na kontrolna okruženja

10.1.3 P6 – Politika upravljanja rizicima: integrira rezultate revizije u aktivnosti procjene i obrade rizika na razini organizacije

10.1.4 P14 – Politika zadržavanja i zbrinjavanja podataka: uređuje zadržavanje revizijskih dokaza, dnevničkih zapisa i zapisa o usklađenosti

10.1.5 P18 – Politika kriptografskih kontrola: podupire sigurnu pohranu i prijenos osjetljivih revizijskih podataka

10.1.6 P26 – Politika sigurnosti trećih strana i dobavljača: obuhvaća prava na reviziju, dokumentaciju o pouzdanosti i nadzor usklađenosti dobavljača

10.1.7 P30 – Politika odgovora na incidente: usklađuje revizije postupanja u incidentima s ciljevima osiguranja ISMS-a

10.1.8 P32 – Politika kontinuiteta poslovanja i oporavka od katastrofe: zahtijeva provjeru testiranja kontinuiteta i usklađenosti DRP-a tijekom ciklusa revizije

11. Referentni standardi i okviri

11.1 Ova je politika usklađena s globalnim standardima i pravnim zahtjevima za reviziju i kontinuiranu provjeru usklađenosti.

11.2 ISO/IEC 27001:

11.2.1 Točka 9.2 – Unutarnja revizija: zahtijeva redovite revizije ISMS-a temeljene na riziku radi procjene djelotvornosti i usklađenosti.

11.2.2 Točka 9.3 – Preispitivanje od strane uprave: rezultati revizije moraju biti ulaz u strateški pregled i poboljšavanje.

11.2.3 Točka 10.1 – Nesukladnost i korektivna radnja: nalazi revizije moraju se obrađivati kroz dokumentirane CAPA postupke.

11.3 ISO/IEC 27002:2022 – Kontrole 5.35–5.37:

11.3.1 Kontrole iz Priloga A 5.35–5.37: obuhvaćaju neovisni pregled, usklađenost s pravnim i ugovornim zahtjevima te bilježenje revizijskih aktivnosti.

11.3.2 Daju provedbene smjernice za planiranje, provedbu i poboljšavanje programa revizije i usklađenosti.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Procjene kontrola: zahtijeva rutinski pregled implementiranih sigurnosnih kontrola.

11.4.2 CA-5 – Plan aktivnosti i ključnih etapa (POA&M): usklađen je s praćenjem i otklanjanjem nalaza revizije.

11.4.3 CA-7 – Kontinuirano praćenje: podupire proaktivne, automatizirane procjene usklađenosti.

11.5 GDPR EU (2016/679):

11.5.1 Članci 24 i 32: zahtijevaju dokaz o provedbi i djelotvornosti sigurnosnih kontrola putem odgovarajućih upravljačkih struktura.

11.5.2 Članak 33: podupire potrebu za provjerljivim revizijskim tragovima u odgovoru na povredu i obavješćivanju.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Članak 21(2)(g): zahtijeva reviziju politika i postupaka kao dio minimalnih mjera upravljanja rizicima kibernetičke sigurnosti.

11.6.2 Članak 27: nacionalna nadležna tijela mogu provoditi ili zahtijevati revizije za ključne i važne subjekte.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Članak 10(2)(e): subjekti moraju provoditi unutarnje i vanjske revizije praksi upravljanja IKT rizicima.

11.7.2 Članak 25 – Zahtjevi za reviziju: propisuje periodične revizije koje provode unutarnji ili neovisni vanjski revizori uz regulatornu vidljivost.

11.8 COBIT 2019:

11.8.1 MEA01 – Praćenje, vrednovanje i procjena učinkovitosti i usklađenosti: osigurava da se djelotvornost kontrola provjerava i prijavljuje upravljačkim tijelima.

11.8.2 MEA03 – Praćenje, vrednovanje i procjena usklađenosti: zahtijeva usklađivanje organizacijskih praksi s pravnim, ugovornim i normativnim zahtjevima.