ZAVOD ZA SIGURNOST
INFORMACIJSKIH SUSTAVA

Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti

Verzija: 1.0

Sadržaj

1. Uvod

U suvremenom digitalnom okruženju, kibernetička sigurnost predstavlja temeljni aspekt zaštite nacionalnih interesa, gospodarskog razvoja i društvene stabilnosti. S obzirom na sve veće prijetnje i složenost kibernetičkih napada, Republika Hrvatska prepoznala je potrebu za uspostavom sveobuhvatnog nacionalnog okvira kibernetičke sigurnosti kroz preuzete obveze EU Direktive 2022/2555. U tom kontekstu, donesen je Zakon o kibernetičkoj sigurnosti („Narodne novine“ broj 14/2024; dalje u tekstu: ZKS), koji postavlja temelje za regulaciju i unaprjeđenje kibernetičke sigurnosti na nacionalnoj razini.

Ovaj se dokument prvenstveno primjenjuje na revizore kibernetičke sigurnosti koji su ujedno pružatelji upravljanih sigurnosnih usluga, a koji se certificiraju temeljem ovih Pravila i sukladno tome obavljaju revizije kibernetičke sigurnosti propisane ZKS-om.

1.1. Svrha dokumenta

Člankom 33. ZKS-a, definirano je izdavanje nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti. Certifikat izdaje središnje državno tijelo nadležno za tehnička područja informacijske sigurnosti (u daljnjem tekstu: ZSIS), temeljem Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti.

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti potvrđuje da su pružatelji upravljanih sigurnosnih usluga uspješno zadovoljili propisani postupak certifikacije i primijenili odgovarajuće standarde za kompetentno provođenje revizije kibernetičke sigurnosti obveznika iz ZKS-a.

Svrha ovih pravila je uspostaviti jasne kriterije i smjernice za provedbu certifikacijskog postupka, uključujući revizijske postupke, izvještavanje o pronalascima te formalno izdavanje nacionalnog sigurnosnog certifikata. Na taj se način osiguravaju dosljednost, transparentnost i učinkovitost u provedbi certifikacije revizora kibernetičke sigurnosti, čime se doprinosi jačanju kibernetičke otpornosti Republike Hrvatske.

Provedbom revizije kibernetičke sigurnosti, obveznici iz ZKS-a bit će u mogućnosti dokazati svoju usklađenost s propisanim standardima kibernetičke sigurnosti, što će povećati povjerenje korisnika, poslovnih partnera i nadležnih tijela. Osim toga, uspostava standardiziranog postupka certifikacije

postavlja temelje za kontinuirano poboljšanje sigurnosnih praksi koje će omogućiti pravovremeno prepoznavanje i otklanjanje potencijalnih prijetnji kroz proces revizije kibernetičke sigurnosti.

Ovaj dokument stoga predstavlja ključni element u operacionalizaciji odredbi ZKS-a u području provjere usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, te služi kao vodič za sve dionike uključene u proces certifikacije za reviziju kibernetičke sigurnosti i proces revizije.

Cilj ovog dokumenta je pružiti jasne smjernice za postupak certifikacije za provedbu revizije kibernetičke sigurnosti, uključujući:

- Kriterije za izdavanje nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti - Utvrđivanje uvjeta koje moraju ispunjavati revizori kibernetičke sigurnosti kako bi bili ovlašteni za provođenje revizija kibernetičke sigurnosti.
- Izdavanje certifikata - Opis izdavanja nacionalnog sigurnosnog certifikata na temelju provedenog postupka certifikacije.
- Postupke revizije - Definiranje metodologija i aktivnosti koje revizori kibernetičke sigurnosti trebaju slijediti tijekom procjene kibernetičke sigurnosti subjekata.
- Izvještavanje i dokumentaciju - Navođenje zahtjeva za izradu i dostavu izvještaja o provedenim revizijama te vođenje odgovarajuće dokumentacije.

Osim navedenog, ovaj dokument jasno propisuje pravila, tehničke zahtjeve, norme i postupke koji se primjenjuju u provedbi revizije kibernetičke sigurnosti. U skladu s važećim zakonodavnim i regulatornim okvirom, dokument definira metodologiju revizije, kriterije procjene sigurnosnih kontrola te minimalne tehničke uvjete koje je potrebno ispuniti. Nadalje, dokument sadržava smjernice za izradu izvješća o provedenoj reviziji kibernetičke sigurnosti, uključujući obvezne elemente izvješća kao što su opis revidiranog sustava, utvrđeni nalazi i procjena razine rizika.

Dokument također obuhvaća postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti, pri čemu su precizno definirani kriteriji, tijek i nadležnosti u provedbi postupka. Nadalje, uređuju se prava i obveze pružatelja upravljanih sigurnosnih usluga u vezi s provedbom revizije i održavanjem certifikata. U cilju zaštite prava sudionika, dokument predviđa mehanizme pravne zaštite, uključujući mogućnost podnošenja prigovora i korištenje drugih pravnih sredstava u skladu s važećim zakonodavstvom.

1.2. Prednosti certificiranja

Certificiranje za provođenje revizija kibernetičke sigurnosti, pored toga što potvrđuje formalni status revizora kibernetičke sigurnosti prema ZKS-u, ima ključnu stratešku i operativnu važnost za poslovne subjekte koji pružaju usluge u visoko reguliranim i sigurnosno osjetljivim sektorima. Osim formalnog priznavanja stručnosti i usklađenosti s nacionalnim i međunarodnim standardima, certificiranje pruža značajne poslovne i reputacijske prednosti. U nastavku se ističu ključni razlozi zbog kojih bi neka organizacija trebala težiti certificiranju:

- **Usklađenost s regulatornim zahtjevima -** Certificirani revizori potvrđuju svoju usklađenost s relevantnim nacionalnim i europskim propisima, uključujući zahtjeve Zakona o kibernetičkoj sigurnosti i NIS2 direktive. U sektorima gdje su revizije kibernetičke sigurnosti obvezne, posjedovanje certifikata je nužni uvjet za provođenje revizije kibernetičke sigurnosti.
- **Povećanje konkurentnosti na tržištu** - Certificiranje osigurava da organizacija može nuditi usluge revizije kibernetičke sigurnosti u skladu s najvišim standardima kvalitete, čime se značajno povećava konkurentnost na tržištu, posebno među subjektima koji su obveznici usklađivanja s propisima iz područja kibernetičke sigurnosti.
- **Stvaranje povjerenja kod klijenata i partnera** - Posjedovanje certifikata predstavlja dokaz stručnosti i sposobnosti organizacije da provodi temeljite i pouzdane revizije. Klijenti i poslovni partneri imaju veće povjerenje u organizacije koje su prošle stroge postupke certificiranja, što može rezultirati jačanjem postojećih poslovnih odnosa i privlačenjem novih klijenata.
- **Reputacijska prednost -** Certificiranje unapređuje reputaciju organizacije kao pouzdanog i stručnog partnera u području kibernetičke sigurnosti. To može rezultirati pozitivnim prepoznavanjem na tržištu i jačanjem brenda, čime organizacija osigurava prepoznatljivost i reputaciju u pružanju visokokvalitetnih revizijskih usluga.
- **Pristup novim poslovnim prilikama -** Organizacije s certifikatom često imaju prednost pri sklapanju ugovora s javnim i privatnim subjektima koji zahtijevaju visoku razinu kibernetičke sigurnosti. Certifikat omogućuje pristup novim tržištima i poslovnim prilikama, uključujući sudjelovanje u natječajima i konzultantskim projektima u sektoru kibernetičke sigurnosti.
- **Poticanje kontinuiranog razvoja i inovacija -** Proces certificiranja uključuje redovite nadzore i procjene, što pomaže organizaciji u stalnom poboljšavanju svojih postupaka i metodologija

revizija, osiguravajući da organizacija ostane u koraku s najnovijim tehnološkim razvojem i praksama u području kibernetičke sigurnosti.

- **Pridržavanje najbolje prakse -** Certificiranje pomaže organizacijama da usvoje i primijene najbolje prakse u reviziji kibernetičke sigurnosti, što smanjuje rizik od ljudske pogreške i povećava ukupnu učinkovitost revizijskih procesa.

Certificiranje za provođenje revizija kibernetičke sigurnosti predstavlja ključnu poslovnu odluku za organizacije koje žele osigurati svoj rast i održivost u sve složenijem i dinamičnijem kibernetičkom okruženju.

1.3. Definicije i pojmovi

Kibernetička sigurnost: Sve aktivnosti koje su nužne za zaštitu od kibernetičkih prijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu.

Ključni subjekti: Subjekti koji su kategorizirani u kategoriju ključnih subjekata, sukladno odredbama ZKS-a.

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti: Službeni dokument kojim se potvrđuje da je određeni subjekt ovlašten i kvalificiran za provođenje revizija kibernetičke sigurnosti, osiguravajući time visoke standarde stručnosti i povjerenja u revizorske procese. U tekstu se spominje i kao certifikat, te ostale izvedenice te riječi.

NIS2 direktiva: Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 - NIS2 direktiva je prenesena u hrvatsko zakonodavstvo ZKS-om.

Revizija kibernetičke sigurnosti: Sustavan pregled i procjena sigurnosnih mjera i praksi koje subjekt primjenjuje radi zaštite svojih mrežnih i informacijskih sustava od kibernetičkih prijetnji. Reviziju provode pružatelji upravljanih sigurnosnih usluga (PRUS) za reviziju kibernetičke sigurnosti.

Važni subjekti: Subjekti koji su kategorizirani u kategoriju važnih subjekata, sukladno odredbama ZKS-a.

Zavod za sigurnost informacijskih sustava (ZSIS): Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti. Prema ZKS-u ZSIS je nadležan za izdavanje

nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti te provedbu revizije kibernetičke sigurnosti za tijela državne uprave i druga državna tijela.

1.4. Kratice

Kratica	**Puni naziv**
CBCI	Certificate of the BCI (Business Continuity Institute)
CDCP	Certified Data Centre Professional
CDPSE	Certified Data Privacy Solutions Engineer
CEH	Certified Ethical Hacker
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CRISC	Certified in Risk and Information Systems Control
CTDC	Certified TIA-942 Design Consultant
CTIA	Cellular Telecommunications and Internet Association uključujući: CTIA Cybersecurity Certification Program ili CTIA Certification for Wireless Devices
DCFC	Data Center Foundation Certificate
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
HKO	Hrvatski kvalifikacijski okvir
IKT	Informacijska i komunikacijska tehnologija

ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OSCP	Offensive Security Certified Professional
PRUS	Pružatelji upravljanih sigurnosnih usluga (engl. *Managed Security Service Providers* – MSSP)
ZKS	Zakon o kibernetičkoj sigurnosti (NN 14/2024)
ZSIS	Zavod za sigurnost informacijskih sustava

2. Organizacijski i stručni zahtjevi

Pružatelji upravljanih sigurnosnih usluga (PRUS) koji provode revizije kibernetičke sigurnosti moraju zadovoljiti organizacijske i stručne zahtjeve kako bi osigurali kvalitetu i pouzdanost usluge. Organizacijski zahtjevi uključuju jasno definiranu strukturu pravne osobe s precizno dodijeljenim odgovornostima i ovlastima unutar revizorskog tima. Ključna je i neovisnost revizorskog tima kako bi se osigurala objektivnost i izbjegli potencijalni sukobi interesa. Uspostavljanje sustava upravljanja kvalitetom također je važno, uključujući redovite interne procjene i poboljšanja procesa revizije.

S druge strane, stručni zahtjevi obuhvaćaju posjedovanje relevantnih certifikata, poput CISSP ili CISA, a ključna je i stručnost u prepoznavanju prijetnji i ranjivosti te razumijevanje najboljih praksi u industriji. PRUS-ovi moraju imati dokazano iskustvo u provođenju revizija različitih sektora i osigurati kontinuirano usavršavanje svojih stručnjaka kroz edukacije, radionice i konferencije.

ZKS propisuje obvezu redovitih revizija za ključne subjekte, a PRUS-ovi moraju osigurati da su njihove metode i pristupi usklađeni s propisanim tehničkim zahtjevima i standardima. Važni subjekti reviziju provode samo na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti. Kada je PRUS s izdanim certifikatom za provođenje revizija kibernetičke sigurnosti kategoriziran kao ključni subjekt u sklopu ZKS-a, reviziju spomenutog ključnog subjekta provodi drugi vanjski certificirani PRUS. Odnosno ukoliko je PRUS A kategoriziran kao ključni subjekt, redovnu reviziju za njega provodi drugi PRUS, odnosno PRUS B.

Reviziju mogu provoditi isključivo članovi tima koji su zaposleni kod PRUS-a. Vanjski suradnici koji nisu u radnom odnosu s PRUS-om ne mogu sudjelovati u provođenju revizije. Više certificiranih PRUS-ova može zajednički sudjelovati u provođenju iste revizije, pod uvjetom da su svi uključeni PRUS-ovi valjano certificirani. U slučaju zajedničkog angažmana, može se sklopiti jedinstveni ugovor sa subjektom koji naručuje reviziju, ali u ugovoru mora biti jasno i nedvosmisleno naznačena osoba odgovorna za vođenje revizije i izradu izvješća. Reviziju mogu provoditi isključivo zaposlenici certificiranog PRUS-a zbog sljedećih razloga: (1) imaju jasno utvrđenu pravnu odgovornost kroz radni odnos, (2) podliježu redovnom i nenajavljenom nadzoru ZSIS-a nad PRUS-om i internim pravilima PRUS-a, čime se osigurava etičnost, stručnost i povjerljivost, (3) njihova stručna osposobljenost i rad su obuhvaćeni certifikacijskim sustavom, i (4) imaju definiran sigurnosni status i kontrolirani pristup osjetljivim informacijama.

Primjerice, PRUS A ima jednog zaposlenika, dok PRUS B zapošljava dvije osobe. Obje pravne osobe su certificirani PRUS-ovi. Oni mogu zajedno sklopiti ugovor s ključnim subjektom za provođenje revizije kibernetičke sigurnosti. U tom slučaju u „Izvješću o provedenoj reviziji“ mora biti jasno navedeno tko je odgovorna osoba za provedbu revizije.

2.1. Organizacijski zahtjevi

Organizacijski zahtjevi za PRUS-ove koji provode revizije kibernetičke sigurnosti osiguravaju uspostavljen proces upravljane sigurnosne usluge revizije kibernetičke sigurnosti, stabilnu i učinkovitu unutarnju strukturu, neovisnost u radu te dosljedno upravljanje kvalitetom procesa te informacijskom i kibernetičkom sigurnošću. PRUS-ovi moraju uspostaviti proces revizije kao svoju upravljanu sigurnosnu uslugu, te jasno definiranu organizacijsku strukturu s precizno dodijeljenim odgovornostima i ovlastima unutar revizorskog tima, kao i načinima ophođenja s informacijama o subjektu revizije tijekom cijelog njenog procesa. Svaki član tima mora imati jasno definirane uloge u procesu revizije, od planiranja do provedbe i izvještavanja. Osim toga, PRUS je dužan dokumentirati te uloge u obliku internog pravilnika ili organizacijske sheme koji se redovito ažuriraju, a proces revizije mora biti opisan procedurama i ostalim dokumentiranim informacijama.

Neovisnost revizorskog tima od presudne je važnosti za osiguranje objektivnosti procesa revizije. Sukob interesa mora biti jasno definiran i spriječen kroz interne politike. Radi očuvanja nepristranosti i povjerenja u revizijske postupke, utvrđuje se da PRUS mora biti organizacijski neovisan o svim aktivnostima koje bi mogle stvoriti stvarni ili potencijalni sukob interesa. Neovisnost se osigurava na način da ista organizacija ne može istodobno pružati usluge održavanja informacijskih sustava, upravljane sigurnosne usluge (kao što su SOC, SIEM, IT/OT sigurnost, IT podrška ili nadzor sustava) niti bilo koje druge usluge koje uključuju aktivno sudjelovanje u sigurnosnim operacijama subjekta nad kojim se provodi revizija – istovremeno ili unazad dvije godine.

U slučaju da PRUS, nakon provedene prve revizije, sklopi ugovor o pružanju usluga koje se mogu povezati s kriterijima revidiranja, obvezan je izuzeti se iz provedbe sljedeće revizije. Sukob interesa smatra se postojećim i u situacijama kada su revizorski i operativni tim unutar iste organizacije formalno odvojeni, ali podliježu istom upravljačkom tijelu ili direktoru.

Dokazivanje neovisnosti revizorskog tijela u postupku certificiranja mora obuhvatiti organizacijsku, a ne samo funkcionalnu separaciju unutar iste pravne osobe.

Prihvaćena međunarodna pravila i smjernice (ISO 17021-1, ISO/IEC 27006:2015, ISO 19011:2018) i preporuke ENISA NIS2 Technical Implementation Guidance, June 2025, version 1.0 (poglavlje 2.3) jasno propisuju obvezu održavanja takve organizacijske neovisnosti. Ova neovisnost mora biti dokumentirana u internim politikama PRUS-a, te verificirana kroz periodične nadzore od strane ZSIS-a.

Sustav upravljanja kvalitetom i informacijskom odnosno kibernetičkom sigurnošću uspostavljenog procesa revizije PRUS-a ključan je za održavanje visokih standarda u pružanju sigurnosnih usluga. PRUS-ovi su dužni implementirati formalni sustav upravljanja kvalitetom i informacijskom sigurnošću koji minimalno uključuje redovite interne procjene, identifikaciju slabosti i/ili nedostataka te mjere za poboljšanje procesa. Vezano uz sustav upravljanja kvalitetom, procjene moraju biti dokumentirane u formi revizijskih izvješća, a preporučuje se i vođenje registra neusklađenosti te predloženih korektivnih mjera. Vezano uz upravljanje informacijskom i kibernetičkom sigurnošću, PRUS-ovi su dužni implementirati napredne mjere kibernetičke sigurnosti, u skladu sa svim obvezama važnih ili ključnih subjekata koje proizlaze iz njihove kategorizacije s obzirom na pružanje upravljanih sigurnosnih usluga. ZSIS u okviru nadzora nad PRUS-om provodi provjeru postojanja i primjene navedenih sustava. Pregledom relevantne dokumentacije, provođenjem intervjua s ključnim osobljem te procjenom učinkovitosti primjene korektivnih mjera, ZSIS utvrđuje u kojoj mjeri PRUS osigurava provedbu propisanih procesa, uspostavlja mehanizme sustavnog unaprjeđenja te održava usklađenost s primjenjivim referentnim standardima i propisanim naprednim mjerama.

U nastavku se nalazi tablica koja prikazuje i detaljno objašnjava osnovne organizacijske zahtjeve koje PRUS-ovi moraju ispuniti kako bi zadovoljili uvjete za dobivanje nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti. Tablica sadrži popis zahtjeva, njihov kratak opis, način na koji ZSIS utvrđuje zadovoljavanje svakog pojedinog zahtjeva te popis relevantne dokumentacije koja se koristi za potvrdu sukladnosti. Dostavljeni certifikati pospješuju postupak analize sveukupne dokumentacije za provjeru.

Redni broj	*Zahtjev*	*Kratki opis zahtjeva*	*Način provjere*	*Dokumentacija za provjeru*
1	Uspostavljen i dokumentiran proces upravljane	Pružatelj mora imati dokumentiran i upravljan proces usluge revizije koji	Pregled procesa, popisa dokumentacije,	Krovni akti procesa, politike i operativne

	sigurnosne usluge revizije kibernetičke sigurnosti*	zadovoljava smjernice pripadajućih standarda	usklađenost istih sa standardima	procedure upravljanja procesom
2	Definirana organizacijska struktura*	PRUS mora imati dokumentiranu i ažuriranu strukturu organizacije.	Pregled organizacijske sheme i interne dokumentacije	Organizacijska shema, pravilnici
3	Jasno dodijeljene odgovornosti i ovlasti*	Sve uloge i ovlasti u revizorskom timu moraju biti jasno definirane i raspodijeljene.	Analiza dokumentacije koja opisuje uloge i odgovornosti	Opis poslova, interni pravilnici
4	Neovisnost revizorskog tima**	Revizorski timovi ne smiju biti povezani s operativnim timovima kako bi se osigurala objektivnost.	Intervjui s osobljem i pregled odvojenosti procesa	Politike i procedure, evidencija zadataka
5	Politike za sprječavanje sukoba interesa***	Postojanje politika koje definiraju i sprječavaju sukobe interesa unutar organizacije.	Pregled politika i konkretnih slučajeva primjene politika	Interne politike, evidencija o sukobima interesa
6	Sustav upravljanja kvalitetom****	Formalni sustav za osiguranje kvalitete usluga i informacijske sigurnosti kroz procesne standarde i kriterije propisanih mjera.	Pregled dokumenata sustava upravljanja kvalitetom te informacijskom i kibernetičkom sigurnošću	Standardi kvalitete i informacijske sigurnosti, te priručnici i pravilnici
7	Redovite interne procjene i poboljšanja****	Redovita procjena kvalitete, identifikacija slabosti i provedba korektivnih mjera.	Pregled izvješća o internim procjenama, Izvješća o samoprocjeni ili reviziji kibernetičke sigurnosti, Izjave o	Izvješća o internim auditima, Izvješće o samoprocjeni ili reviziji

		sukladnosti i korektivnim mjerama	kibernetičke sigurnosti, planovi korektivnih mjera, Izjava o sukladnosti

* Ako je organizacija certificirana prema ISO 9001:2015 s opsegom koji obuhvaća i procese revizije kibernetičke sigurnosti, ili je certifikacijsko tijelo aktivno akreditirano prema ISO/IEC 17021-1:2015 s relevantnim opsegom odnosno ISO/IEC 27001:2022 za provedbe revizije informacijske odnosno kibernetičke sigurnosti, ZSIS-u dostavlja, uz propisanu dokumentaciju, odgovarajući dokaz iz kojeg je nedvojbeno razvidno da opseg pokriva poslove i procese koji se odnose na provedbu revizije kibernetičke sigurnosti (za ISO 9001:2015 - aktivan certifikat izdan od akreditiranog certifikacijskog tijela; za ISO/IEC 17021-1:2015 potvrda o akreditaciji na kojoj je razvidno da akreditacija obuhvaća i ISO/IEC 27001:2022).

** Ako je organizacija certificirana prema standardu ISO/IEC 17021-1:2015 ili drugom ekvivalentnom certifikatu, u skladu s ovim zahtjevom ZSIS-u dostavlja uz propisanu dokumentaciju i potvrdu o akreditaciji.

*** Ako je organizacija certificirana prema standardima ISO 37301:2021 ili je certifikacijsko tijelo aktivno akreditirano prema ISO/IEC 17021-1:2015 s relevantnim opsegom provedbe revizija informacijske odnosno kibernetičke sigurnosti ili drugim ekvivalentnim standardima, u skladu s ovim zahtjevom ZSIS-u dostavlja uz propisanu dokumentaciju i aktivan certifikat izdan od za taj standard akreditirane certifikacijske kuće ili potvrdu o akreditaciji. Iz certifikata ili potvrde o akreditaciji treba biti nedvojbeno razvidno da certifikacija ili akreditacija pokriva poslove i procese koji se odnose na provedbu revizije kibernetičke sigurnosti.

**** Ako je organizacija certificirana prema standardu ISO 9001:2015 ili drugom ekvivalentnom certifikatu, u skladu s ovim zahtjevom ZSIS-u dostavlja uz propisanu dokumentaciju i potvrdu o certifikaciji iz koje je nedvojbeno razvidno da certifikacija pokriva poslove i procese koji se odnose na provedbu revizije kibernetičke sigurnosti.

Iznimno od prethodno navedenog, istekom roka od tri godine od dana stupanja na snagu ovih Pravila, PRUS je obvezan prilikom podnošenja zahtjeva za certifikaciju, uz ostalu propisanu dokumentaciju temeljem kojih se vrši provjera ispunjenja organizacijskih zahtjeva, dostaviti dokaz kako je organizacija certificirana prema standardima ISO 9001:2015 i ISO/IEC 17021-1:2015.

2.2. Stručni zahtjevi

Svi članovi revizorskog tima moraju imati odgovarajuće obrazovanje i stručne kvalifikacije koje ih osposobljavaju za provedbu revizije u skladu s važećim normama, propisima i metodologijom.

Članovi revizorskog tima moraju imati završeno visoko obrazovanje (razina 6. sv ili 6. st HKO-a i razina 7.1. sv ili 7.1. st HKO-a) iz relevantnog područja. Relevantna područja uključuju, ali nisu ograničena na: računarstvo, informacijske tehnologije, informacijsku sigurnost, studije sigurnosti, pravo i upravljanje s fokusom na sigurnosne aspekte, te druga područja ako sadrže značajnu komponentu iz područja kibernetičke sigurnosti ili revizija informacijskih sustava. Obrazovne isprave izdane izvan Republike Hrvatske moraju biti prevedene na hrvatski jezik od ovlaštenog sudskog tumača i priznate od nadležnog tijela u Republici Hrvatskoj (nostrifikacija), sukladno Zakonu o priznavanju inozemnih obrazovnih kvalifikacija.

Obrazovanje mora biti stečeno na akreditiranoj visokoškolskoj ustanovi, a dokazi o završenom studiju - diploma i dopunska isprava o studiju ili ekvivalent - moraju biti dostupni za potrebe provjere od strane certifikacijskog tijela.

Revizija kibernetičke sigurnosti zahtijeva stručan i sustavan pristup koji uključuje angažman kvalificiranog osoblja s odgovarajućim tehničkim znanjima, iskustvom i profesionalnim certifikatima. Članovi revizorskog tima PRUS-a trebaju posjedovati temeljito razumijevanje informacijskih sustava, uključujući rad operativnih sustava, mrežne arhitekture i sigurnosnih tehnologija poput vatrozida, enkripcije i sustava za detekciju i prevenciju napada. Iskustvo u upravljanju sigurnosnim alatima, analizom rizika i provođenjem sigurnosnih kontrola dodatno osnažuje sposobnost revizora da prepoznaju ranjivosti i ocijene postojeće mjere zaštite.

Kako bi se osigurala profesionalna razina kompetencija u provedbi revizije kibernetičke sigurnosti, nužno je da članovi revizorskog tima raspolažu relevantnim stručnim i tehničkim znanjima koja odgovaraju sustavima koji se revidiraju. To uključuje posjedovanje jednog ili više relevantnih stručnih certifikata visokih razina i s položenim ispitom, a koji su izdani od strane međunarodno priznatih organizacija ili akreditiranih certifikacijskih tijela. Certifikati moraju pokrivati područja koja su povezana s kriterijima revizije, uključujući, ali ne ograničeno na: ICT sigurnost, informacijsko i kibernetičko upravljanje rizicima, industrijsku sigurnost (OT), upravljanje kontinuitetom poslovanja, sigurnost opskrbnog lanca, sigurnost podatkovnih centara i srodna područja. Paralelno s time, od revizora se očekuje i poznavanje metodologije provedbe revizija, što se dokazuje certifikatima poput CISA, ISO/IEC 27001 Lead Auditor i drugim srodnim kvalifikacijama koje pokrivaju sustave upravljanja i revizijske postupke.

Model kompetencija može biti ostvaren kroz jednu osobu koja posjeduje obje vrste znanja – tehničku stručnost u području informacijske i kibernetičke sigurnosti te kompetencije za provođenje revizija sustava upravljanja. Takav integrirani pristup osigurava konzistentnost i učinkovitost u provedbi revizije. Alternativno, PRUS može koristiti dva stručnjaka: jednog s izraženim tehničkim kompetencijama i drugog s izraženim revizorskim znanjima, čime se također zadovoljava zahtjev za pokrivanjem obje komplementarne domene znanja. Stručnjaci koji su članovi revizorskog tima moraju imati minimalno pet godina radnog iskustva u okviru provođenja sličnih vrsta revizije u području mrežnih i informacijskih sustava odnosno kibernetičke sigurnosti. Stručnjak PRUS-a mora imati najmanje pet godina relevantnog radnog iskustva u području informacijske i kibernetičke sigurnosti te u okviru provođenja sličnih vrsta revizija – odnosno najmanje 5 godina radnog iskustva iz oba područja. U slučaju kada su revizorske aktivnosti podijeljene između dvije osobe – jedna s tehničkim, a druga s revizorskim kompetencijama – svaka od njih mora pojedinačno imati najmanje pet godina iskustva u svojem području stručnosti. Voditelj revizorskog tima mora imati dokazanu praksu vođenja timova u barem tri završene iste ili slične revizije iz područja informacijske i kibernetičke sigurnosti u posljednje tri godine.

Uz formalne certifikate, nužno je da se kompetencije dokazuju i praktičnim iskustvom, što uključuje sudjelovanje u relevantnim projektima, provedene samoprocjene, prethodna radna iskustva te dokumentirani rezultati provedenih revizija ili audita. Pregled životopisa, referenci i primjera prethodnog rada čini sastavni dio procjene podobnosti stručnjaka za obavljanje revizije kibernetičke sigurnosti.

Kontinuirano profesionalno usavršavanje ključno je za održavanje visoke razine stručnosti. Revizori moraju redovito sudjelovati na radionicama, konferencijama i industrijskim forumima kako bi ostali u tijeku s najnovijim trendovima i tehnikama u području kibernetičke sigurnosti. PRUS mora osigurati uspostavu formalnih programa obuke i certifikacije za svoje zaposlenike, uključujući periodične provjere znanja i vještina kako bi se održala njihova sposobnost za provedbu kvalitetnih revizija.

Tijekom postupka certifikacije, ključno je kroz intervju s osobljem procijeniti razumijevanje ključnih sigurnosnih standarda, tehničku osposobljenost, sposobnost identificiranja rizika i razumijevanje regulatornih zahtjeva. Ovaj proces omogućuje uvid u stvarno stanje vještina i znanja članova revizorskog tima te osigurava da su svi aspekti kibernetičke sigurnosti adekvatno obuhvaćeni i ocijenjeni.

Standard poput ISO 19011, koji pruža smjernice za reviziju sustava upravljanja, ključan je za uspostavu strukture i metodologije koje će omogućiti učinkovitu procjenu sigurnosnih kontrola. Nužno je da PRUS ima formalno dokumentirane postupke revizije u skladu s ISO 19011, te shodno navedenom pripremljenu izjavu o usklađenosti koja može biti uključena u interni priručnik kvalitete. Osim spomenutoga, mnoga akreditirana tijela i edukacijski centri nude tečajeve za obuku članova revizorskog tima temeljenih na ISO 19011 (poput "ISO/IEC 27001:2022 Lead Auditor Training", "Internal Auditor Training – Based on ISO 19011" ili "ISO 19011 Guidelines Auditor Training"). Potrebno je da članovi revizorskog tima PRUS-a imaju potvrdu koja potvrđuje da su osposobljeni za provođenje revizija u skladu s načelima ISO 19011 , pri čemu ista ne predstavlja certifikat ISO 19011, već dokaz da je revizor educiran o načinu provedbe revizija u skladu sa smjernicama propisanim standardom ISO 19011.

PRUS mora uspostaviti i dokumentirati matricu kompetencija revizijskog tima koja pokriva:

- tehničke kompetencije (informacijska sigurnost, OT/IT sustavi, industrijska sigurnost, sigurnost aplikacija, mreže, kriptografija, upravljanje incidentima itd.),
- upravljačke i organizacijske kompetencije (upravljanje rizicima, kontinuitet poslovanja, zakonodavstvo, upravljanje dobavljačima, SLA itd.),
- revizorske kompetencije (revizijska metodologija, uzorkovanje, intervjuiranje, izvještavanje, ponašanje u auditu),
- osobne karakteristike (objektivnost, nepristranost, etičnost, komunikacijske vještine, jezične vještine).

U nastavku se nalazi tablica koja prikazuje i objašnjava stručne zahtjeve koje PRUS-ovi i stručnjaci koji su članovi revizorskog tima moraju ispuniti kako bi dobili nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti. Tablica sadrži popis ključnih zahtjeva, njihov kratak opis, način na koji ZSIS utvrđuje zadovoljavanje svakog pojedinog zahtjeva te popis relevantne dokumentacije koja se koristi za verifikaciju.

Redni broj	*Zahtjev*	*Kratki opis zahtjeva*	*Način provjere certifikacijskog tijela*	*Dokumentacija za provjeru**
1	Osposobljenost stručnjaka za	Osoblje mora imati potvrdu o usvojenim znanjima i	Provjera potvrde o osposobljenosti	Kopija potvrde**

	provođenje audita upravljanih sustava	osposobljenosti za audite upravljanih sustava		
2	Relevantni međunarodni certifikati za stručnjake	Osoblje mora posjedovati certifikate***	Provjera certifikata zaposlenika kroz evidenciju i validaciju certifikacijskih tijela.	Evidencija certifikata/potvrda, kopije certifikata
3	Praktično iskustvo u provođenju revizija	Zaposlenici trebaju imati iskustvo u procjeni ranjivosti i sigurnosnih mjera, audita iz područja informacijske sigurnosti i samoprocjena kibernetičke sigurnosti	Analiza povijesti projekata, intervjui s osobljem.	Projekti, revizijska izvješća, potvrde, životopisi i ostalo
4	Program kontinuiranog profesionalnog razvoja	Uspostava formalnih programa obuke i certifikacije za osoblje.	Provjera planova i zapisa o održanim obukama.	Planovi i evidencije obuka
5	Sudjelovanje na industrijskim konferencijama i forumima	Redovito sudjelovanje osoblja na relevantnim industrijskim događajima.	Evidencija sudjelovanja na konferencijama i relevantnim industrijskim događajima.	Potvrde s konferencija, evidencije sudjelovanja i ostalo

* Dokumentacija koja sadržava osobne podatke fizičkih osoba se ne dostavlja ZSIS-u, već ista mora biti dostupna prilikom procesa opisanog u „Faza 2 – Revizorska posjeta“.

** Potvrda poput ISO 19011 – dokaz da je revizor educiran prema smjernicama

*** Certifikati poput OSCP, CEH, GCIH, GCIA, CISSP, CTIA, CISA, ISO 27001 Lead Auditor, CRISC, CDPSE, CBCI, ISO 22301 LA, ISA/IEC 62443 Risk, DCFC, CTDC, CDCP ili drugi ekvivalentni certifikati.

2.3. Tehničko-sigurnosni zahtjevi

PRUS je obavezan primijeniti odgovarajuće mjere sigurnosti kako bi se osigurala zaštita podataka o provedenim i tekućim revizijama, a sve u skladu s minimalnim zahtjevima koje propisuje Uredba o kibernetičkoj sigurnosti („Narodne novine“ broj 135/2024; dalje u tekstu Uredba) za napredne razine mjera u članku 42. stavak 3. Informacijski sustavi na kojima se čuvaju i obrađuju takvi podaci moraju biti usklađeni s ovim sigurnosnim standardima, čime se osigurava povjerljivost, integritet i dostupnost podataka.

Kao dokaz sukladnosti, uz Zahtjev za certificiranje (Prilog A ovih Pravila) PRUS prilaže i Izjavu o utvrđenom stupnju usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima (Prilog D ovih Pravila) za informacijski sustav na kojemu PRUS planira čuvati i obrađivati podatke o revizijama kibernetičke sigurnosti koje će provoditi.

PRUS mora osigurati zaštićeni prijenos i obradu prethodno navedenih podataka. Zabranjeno je pohranjivanje i obrada navedenih podataka na informacijskoj infrastrukturi koja nije pod izravnim nadzorom PRUS-a (uključujući pohranu u oblak) ukoliko navedeni podaci nisu prethodno zaštićeni. Podaci se smatraju zaštićenima ako su prije pohrane adekvatno kriptirani i dostupni samo ovlaštenim osobama.

Za ispunjavanju prethodno navedenog zahtjeva PRUS je dužan utvrditi stupanj usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Uredbom, a sukladno Smjernicama za provedbu samoprocjene kibernetičke sigurnosti. Prethodno navedeni postupak potrebno je provesti nad informacijskim sustavom koji se koristi/će se koristiti za obradu i pohranu podataka vezanih uz reviziju kibernetičke sigurnosti. U slučaju da je navedeni informacijski sustav povezan sa ostalim sustavima PRUS-a, potrebno je imati dokumentaciju koja opisuje vezu između sustava na fizičkoj i logičkoj razini kao jasnu liniju razgraničenja – veza kontrolirana putem POL-007: Uspostava obaveznih mjera zaštite mreže, odnosno kroz NIST SP 800-53 kontrola AC-4 Information flow enforcement.

U postupku certifikacije službene osobe ZSIS-a provjeravaju usklađenost informacijskog sustava s prethodno navedenim zahtjevima.

3. Provedba revizije kibernetičke sigurnosti

U okviru ovog dokumenta definirana su pravila vezana za tehničke zahtjeve, norme i postupke koji se primjenjuju u provedbi revizije kibernetičke sigurnosti. Njima se također propisuju i obvezni elementi koje mora sadržavati izvješće o provedenoj reviziji, čime se osigurava dosljednost i kvaliteta u provedbi revizija te omogućuje učinkovita procjena stanja kibernetičke sigurnosti subjekata.

U nastavku su navedeni detaljni postupci i kriteriji koje je potrebno primijeniti pri provedbi revizije.

3.1. Tehnički zahtjevi, norme i postupci

Detalji tehničkih zahtjeva, normativa i metodologije za provođenje revizija kibernetičke sigurnosti definirani su u dokumentu "*Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima*", koji je sastavni dio ovog dokumenta i označen kao *Prilog B*. Navedeni dokument pruža detaljan pregled tehničkih standarda, zahtjeva za implementaciju, kriterija za procjenu i smjernica za provedbu revizija kibernetičke sigurnosti.

Revizija kibernetičke sigurnosti provodi se u skladu s ZKS-om i Uredbom s naglaskom na njezin Prilog II „*Mjere upravljanja kibernetičkim sigurnosnim rizicima*“ iz kojega proizlaze kontrole mjera opisane u prilogu C „*Katalog kontrola*“ ovih Pravila (dalje u tekstu: Prilog C), te u Prilogu B „*Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima*“ ovih Pravila (dalje u tekstu: Prilog B) koji povezuje mjere i kontrole sa definiranim bodovnim pragovima ocjena.

Prilog B pruža strukturirani pristup evaluaciji mjera upravljanja kibernetičkim rizicima, uključujući:

- Kriterije za procjenu sukladnosti subjekta s tehničkim zahtjevima iz gore navedenih standarda.
- Kontrole temeljene na mjerama propisanim u Prilogu II – Mjere upravljanja kibernetičkim sigurnosnim rizicima Uredbe.

Svi postupci i zahtjevi opisani u Prilogu B obvezujući su za subjekte koje podliježu procjeni stanja kibernetičke sigurnosti. Opisani postupci i zahtjevi predstavljaju temelj za objektivno i konzistentno provođenje revizija te osiguravaju primjenu standardiziranog pristupa u procjeni sigurnosnih mjera i sustava upravljanja kibernetičkim sigurnosnim rizicima.

3.1.1. Plan revizije

Revizor je obavezan izraditi i dokumentirati plan i program revizije prije početka revizijskog postupka, a isti mora biti usklađen s metodologijom temeljenom na kompletnom opsegu Priloga C te u skladu s Prilogom B i smjernicama ISO 19011.

Plan i program revizije mora sadržavati najmanje:

- ciljeve, kriterije i opseg revizije,
- datum(i), vrijeme i trajanje pojedinih aktivnosti,
- revizorski tim i njegove uloge,
- podatke o organizaciji klijenta i kontaktima,
- opis lokacija koje će biti obuhvaćene,
- planirane metode i tehnike (npr. intervju, pregled dokaza, tehničko testiranje),
- identifikaciju područja rizika i fokus revizije,
- način bilježenja nalaza i dokumentiranja dokaza,
- obvezu poštivanja povjerljivosti, neovisnosti i kodeksa ponašanja,
- obvezu komunikacije rezultata s odgovornim osobama.

Uz to, program revizije treba se nadograđivati tijekom revizije ovisno o zatečenom stanju i razvoju nalaza (dinamički plan).

3.2. Obvezni sadržaj izvješća o provedenoj reviziji kibernetičke sigurnosti

U svrhu standardizacije i unaprjeđenja procesa izvještavanja o provedenim revizijama kibernetičke sigurnosti, ovim Pravilima se propisuje obvezni sadržaj i struktura izvješća o provedenoj reviziji kibernetičke sigurnosti. Cilj je osigurati konzistentnost, jasnoću i sveobuhvatnost informacija koje su ključne za procjenu stanja kibernetičke sigurnosti unutar subjekta.

U nastavku je definiran obvezni dio izvješća o provedenoj reviziji kibernetičke sigurnosti, koji uključuje sve elemente potrebne za sveobuhvatno informiranje relevantnih dionika. Revizori su se obvezni pridržavati ove strukture kako bi osigurali usporedivost izvješća i omogućili pravovremenu identifikaciju rizika i područja za poboljšanje.

Obvezni dijelovi izvješća su:

- Naslovnica s osnovnim informacijama,

- Uvod s opisom ciljeva i opsega revizije,
- Sažetak ključnih pronalazaka i preporuka,
- Detaljan prikaz nalaza po mjerama,
- Zaključak,
- Potpis revizora,
- Prilozi s relevantnim dokazima.

3.2.1. Naslovnica s osnovnim informacijama

Naslovnica izvješća o provedenoj reviziji kibernetičke sigurnosti mora sadržavati osnovne identifikacijske podatke i ključne informacije kako bi se jasno identificirala svrha i autorstvo izvješća. Na naslovnici su obvezni sljedeći elementi:

- Naziv subjekta
    - Puni naziv subjekta za koji je provedena revizija.
    - Ukoliko je primjenjivo, može se dodati i naziv odjela ili poslovne jedinice unutar subjekta.
- Naslov izvješća
    - Precizan naziv koji jasno odražava sadržaj izvješća, npr.: "Izvješće o provedenoj reviziji kibernetičke sigurnosti Zavoda za sigurnost informacijskih sustava".
- Datum izdavanja izvješća
    - Točan datum kada je izvješće završeno i predano relevantnim dionicima.
    - Predaja izvješća relevantnim dionicima označava službeni trenutak dovršetka revizorskog procesa.
- Revizor
    - Naziv pravne osobe, adresa sjedišta, osobni identifikacijski broj (OIB) i kontakt podaci (telefon, e-pošta).
    - Imena i prezimena članova revizorskog tima, uz navođenje njihovih stručnih titula ili certifikata.
- Period revizije
    - Specifikacija vremenskog razdoblja tijekom kojeg je revizija provedena, uključujući početni i završni datum (npr. 15.07.2024. – 02.08.2024.).
    - Pruža kontekst za interpretaciju nalaza u odnosu na poslovne i sigurnosne događaje tijekom tog perioda.

- Klasifikacija izvješća
    - Oznaka razine povjerljivosti izvješća, u skladu s klasifikacijskom shemom subjekta revizije.
    - Ovaj element pomaže u pravilnom upravljanju distribucijom izvješća. PRUS je obavezan sa subjektom sklopiti Ugovor o povjerljivosti (NDA) – u ugovoru mora biti naznačena klasifikacija izvješća.
- Verzija izvješća
    - Ukoliko su tijekom revizijskog procesa napravljene izmjene ili dodatne verzije izvješća, naslovnica treba sadržavati broj verzije (npr. Verzija 1.0).

3.2.2. Uvod s opisom ciljeva i opsega revizije

Uvodni dio izvješća o provedenoj reviziji kibernetičke sigurnosti pruža osnovne informacije o opsegu i metodologiji revizije. Cilj uvoda je postaviti temelj za razumijevanje nalaza i preporuka, s fokusom na jasno definirane mjere koje su bile predmet revizije.

Svrha i ciljevi revizije

Svrha revizije je ocijeniti stanje kibernetičke sigurnosti unutar subjekta kroz analizu jasno definiranih kontrola propisanih ovim Pravilima na osnovu Priloga II. Mjere upravljanja kibernetičkim sigurnosnim rizicima (dalje u tekstu: Mjere) Uredbe. Revizija ima za cilj provjeriti učinkovitost i usklađenost implementiranih i dokumentiranih sigurnosnih mjera s propisanim standardima i politikama iz Priloga 2 Uredbe. Fokus je na procjeni specifičnih kontrola koje su unaprijed definirane u okviru revizijskog procesa.

Glavni ciljevi uključuju:

- Procjena usklađenosti provodi se s unaprijed definiranom listom kontrola – svaka kontrola je temeljito ispitana kako bi se utvrdila njezina implementacija i učinkovitost.
- Identifikacija odstupanja i rizika – revizija ima za cilj otkriti potencijalna odstupanja od propisanih kontrola i identificirati rizike koji iz toga proizlaze.

Opseg revizije

Opseg ove revizije strogo je definiran i obuhvaća:

- Predmet revizije: Mjere kibernetičke sigurnosti koje su definirane Uredbom, a koje uključuju područja poput upravljanja pristupima, zaštite podataka, praćenja sigurnosnih događaja i drugih ključnih sigurnosnih aspekata.

- Geografski opseg: Sve relevantne lokacije subjekta koje su bile uključene u reviziju, ovisno o njihovoj važnosti za informacijsku infrastrukturu (uključujući lokaciju udomljenja IKT opreme subjekta).
- Vremenski opseg: Revizija obuhvaća analizu događaja, aktivnosti i primijenjenih kontrola unutar unaprijed definiranog vremenskog razdoblja.

Metodologija

Revizija se provodi korištenjem strukturiranog pristupa temeljenog na analizi unaprijed definiranih kontrola. Pri tome se primjenjuju sljedeće metode:

- Analiza dokumentacije i evidencija: pregled relevantnih dokumenata, poput sigurnosnih politika, procedura, zapisnika o incidentima, dnevnički i drugi zapisi (logovi datoteka) koji podržavaju provođenje kontrola, procjene rizika.
- Intervjui s ključnim osobljem: provedba razgovora s odgovornim osobama kako bi se potvrdila implementacija kontrola u praksi.
- Tehničke provjere: ovisno o specifičnostima kontrola mjera, provedba tehničkih provjera, uključujući ispitivanje postavki sustava, sigurnosnih alata i ostalih tehničkih elemenata. Revizor je ovlašten, prema vlastitoj prosudbi i ako to smatra potrebnim, provesti jednu ili više navedenih vrsta tehničkih provjera radi osiguranja usklađenosti sa zahtjevima.
- Procjena usklađenosti i učinkovitosti: svaka kontrola mjera ocjenjuje se prema unaprijed definiranim kriterijima, kako bi se osiguralo objektivno i konzistentno ocjenjivanje.
- Kategorizacija nalaza: identificiranim pronalascima dodjeljuje se ocjena sukladno uputama za ocjenjivanje u nastavku:

Ocjena	Dokumentacija	Implementacija
1	Dokumentacija ili ne postoji ili nije formalno usvojena; ključni dokumenti, poput politike, nisu definirani.	Proces nije strukturiran, aktivnosti se provode *ad-hoc*, a postupci su neregularni i nepraćeni.
2	Postoji osnovna dokumentacija koja nije redovito ažurirana i pokriva samo osnovne elemente kontrole.	Proces je neformalno uspostavljen i provodi se sporadično, bez potpune dosljednosti ili formalne strukture.
3	Dokumentacija je formalno odobrena, ažurirana s definiranim iznimkama; većina elemenata dokumentacije je jasna.	Proces je formaliziran i strukturiran, provodi se redovito; postoje dokazi za većinu aktivnosti, uz manje iznimke (<10%).

4	Dokumentacija je potpuna, ažurirana i uključuje sve ključne elemente i procese; manje iznimke (<3%).	Proces je potpuno implementiran s dokazima za sve aktivnosti, uključujući praćenje metrike i izvještavanje; manje iznimke (<5%).
5	Dokumentacija je u potpunosti usklađena, redovito ažurirana i kontinuirano se poboljšava; iznimke <0,5%.	Proces je implementiran na najvišoj razini, s naprednim praćenjem, redovitim poboljšanjima i minimalnim iznimkama (<1%).

Ocjena se dodjeljuje svakoj kontroli posebice, a zadovoljenje podmjere ovisi o uvjetima propisanima u Prilogu B Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima. Podmjere u ovom dokumentu opisuju mjere označene decimalnim brojevima drugog reda (npr. 1.1., 1.2., 2.1. itd.) iz Priloga II Mjere upravljanja kibernetičkim sigurnosnim rizicima Uredbe.

Tablica iznad predstavlja pomoćni alat koji služi kao podrška pri ocjenjivanju u skladu sa smjernicama iz Priloga C – Katalog kontrola. Njezin cilj je olakšati strukturirano i dosljedno provođenje revizija kibernetičke sigurnosti s propisanim kontrolama, omogućujući jasniji pregled ključnih elemenata za ocjenjivanje.

Prilikom provođenja revizije, rezultati se kategoriziraju dodjeljivanjem dviju ocjena: jedna ocjena odnosi se na dokumentaciju, dok se druga ocjena odnosi na implementaciju kontrola mjera. Ocjena dokumentacije procjenjuje kvalitetu i potpunost potrebnih dokumenata, poput shema, pravilnika i drugih relevantnih zapisa koji potvrđuju usklađenost sa sigurnosnim standardima. S druge strane, ocjena implementacije procjenjuje stvarnu provedbu sigurnosnih mehanizama na informacijskom sustavu, odnosno jesu li ti mehanizmi zaista ispravno implementirani i funkcioniraju li kako je predviđeno. Obje komponente ključne su za cjelovitu procjenu sigurnosti sustava, a u izvješću se navodi samo jedna ocjena (K).

Ocjena kontrole (K) određuje se kao aritmetička sredina ocjene dokumentacije kontrole (DK) i ocjene implementacije kontrole (IK).

$$K = \frac{DK + IK}{2}$$

Zadovoljavanje pojedinih kontrola sukladno dobivenoj ocjeni kontrole (K) i zadovoljavanje zahtjeva podmjere propisano je u Prilogu B ovih Pravila. Ocjena pojedine mjere (M) određuje se kao aritmetička sredina ocjena podmjera (P) iz te mjere.

$$M = \frac{\sum_{i=1}^{n} Pi}{n}, n \in N$$

3.2.3. Sažetak ključnih pronalazaka i preporuka

Sažetak ključnih nalaza i preporuka je dio izvješća koji služi za brzo informiranje uprave i drugih dionika o najvažnijim rezultatima revizije (engl. *executive summary*). Mora biti koncizan, jasan i usmjeren na identificirane nesukladnosti i njihov značaj.

Na početku sažetak mora jasno čitatelja obavijestiti kako se u postupku revizije kibernetičke sigurnosti provjerava usklađenost uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim ZKS-om i Uredbom, shodno navedenome svaki sažetak mora sadržavati slijedeći tekst:

> Sukladno Zakonu o kibernetičkoj sigurnosti (NN 14/2024) subjekt je kategoriziran kao <ključni/važni> subjekt, te prema rezultatima nacionalne procjene rizika proizašle iz Uredbe o kibernetičkoj sigurnosti (NN 135/2024) utvrđena je <niska/srednja/visoka> razina kibernetičkih sigurnosnih rizika. Sukladno utvrđenoj razini kibernetičkih sigurnosnih rizika za subjekt je utvrđena obaveza provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima sukladno Uredbi.

Obavezna struktura Sažetka:

- Kontekst sažetka
    - Na početku sažetka treba biti kratak uvod koji objašnjava svrhu revizije i ciljeve.
- Tablični pregled nalaza
    - Ključne nalaze i preporuke potrebno je prikazati u formatu tablice radi preglednosti. Tablica treba sadržavati najmanje sljedeće stupce:
        - Naziv nadzirane mjere
            - Sukladno Mjerama iz Priloga II. Uredbe.
        - Ocjena stanja mjere
            - Ocjena stanja mjere se uzima u obzir samo u slučaju da su zadovoljene sve podmjere unutar mjere upravljanja kibernetičkim sigurnosnim rizicima. U slučaju pada jedne ili više podmjera ocjena stanja mjere je 0.

        - Kratki opis nalaza
            - Sažetak nesukladnosti ili odstupanja pronađenih tijekom revizije.
- Ključna poruka
    - Nakon tablice, ukratko se navode glavne poruke za upravljačko tijelo/donosioce odluke koje sažimaju stanje kibernetičke sigurnosti i prioritete za rješavanje.
    - Na primjer: "Revizija je pokazala da su ključne kontrole kibernetičke sigurnosti djelomično zadovoljavajuće. Glavni izazovi uključuju nepravilno upravljanje incidentima i neadekvatno ažuriranje softvera, što subjekt izlaže povećanom riziku od sigurnosnih prijetnji. Preporučuje se hitna implementacija formalnih procedura za odgovor na incidente te postavljanje automatiziranog sustava ažuriranja."
- Prioriteti za djelovanje
    - Na kraju se navodi kratka lista prioriteta koje bi subjekt morao provesti. Lista ne sadrži detalje i preporuke za djelovanje. Ovo može biti u obliku numerirane liste, poput primjerice slijedećega:
        1. Razviti i implementirati formalnu proceduru za upravljanje incidentima.
        2. Automatizirati sustav ažuriranja softvera kako bi se smanjili sigurnosni rizici.
        3. Redovito provoditi kvartalne provjere korisničkih privilegija.

Ovaj dio izvješća treba biti pisan jednostavnim i razumljivim jezikom, bez tehničkih detalja, kako bi bio lako shvatljiv širokom krugu dionika, uključujući ne-tehničko osoblje. Korištenje tabličnog prikaza i sažetaka omogućuje brz uvid u kritične točke i olakšava donošenje odluka.

3.2.4. Detaljan prikaz nalaza po mjerama

Detaljan prikaz nalaza po mjerama ključni je dio izvješća u kojem se pruža detaljna analiza svake pojedine mjere podskupa mjera obuhvaćene revizijom. Cilj ovog dijela je prikazati detaljne informacije o nalazima revizije, uključujući kontekst, specifične nesukladnosti, uzroke, posljedice i tehničke detalje.

Ovaj dio strukturira se prema definiranim mjerama koje se obrađuju kronološkim redoslijedom, slijedom od prve pa sve do posljednje. Svaka mjera obuhvaća detaljnu analizu mjera iz podskupa mjera, koje se također navode prema unaprijed određenom redoslijedu. Unutar svake mjere iz podskupa, kontrole su strukturirane prema razini kritičnosti, s naglaskom na prioritizaciju najvažnijih.

Kritične kontrole, koje predstavljaju najveći sigurnosni rizik u slučaju neprovođenja, obrađuju se prioritetno. U izvješću se navode sve kontrole iz podskupa mjere. Ova hijerarhijska struktura omogućuje fokus na najvažnije nalaze, dok istovremeno osigurava cjelovit pregled svih područja revizije.

Obavezna struktura Detaljnog prikaza nalaza po mjerama:

- Uvod u odjeljak
    - Na početku Detaljnog prikaza navodi se njegov cilj i struktura.
- Nazivi mjera
    - Nazivi mjera iz podskupa
        - Opis pojedinačnih kontrola
            - Svaka kontrola dobiva vlastiti pododjeljak s detaljnim informacijama
            - Elementi uključuju:
                - Identifikator i naziv kontrole.
                - Opis kontrole: Kratko objašnjenje svrhe i uloge kontrole u okviru kibernetičke sigurnosti subjekta.
                - Ocjena kontrole: Dodijeljena ocjena na skali od 1 do 5.
                - Nalazi: Detaljan opis nesukladnosti, uključujući specifične slabosti i odstupanja od očekivanog stanja.
                - Uzrok nesukladnosti: Objašnjenje uzroka koji su doveli do identificiranih slabosti (npr. nedostatak resursa, nejasne procedure, tehnička ograničenja).
                - Posljedice nesukladnosti: Analiza potencijalnog utjecaja na sigurnost, uključujući moguće rizike (npr. povećani rizik od neovlaštenog pristupa ili gubitka podataka).
                - Dokazi i reference: Ako je primjenjivo navode se dokumenti, zapisi ili testovi koji podupiru nalaz.

Primjer izgleda detaljnog prikaza kontrole:

Naziv kontrole: POL-001 - Postojanje strateškog akta kibernetičke sigurnosne politike

Opis kontrole: Ova kontrola osigurava da subjekt ima formalno usvojen strateški akt kibernetičke sigurnosne politike, odobren od strane upravljačkog tijela. Ovaj dokument definira ključne principe, ciljeve i smjernice za upravljanje kibernetičkom sigurnošću, čime postavlja temelj za učinkovitu zaštitu resursa i podataka.

Ocjena kontrole: 3.

Nalazi: Subjekt ima formalno izrađen strateški akt kibernetičke sigurnosne politike, koji je odobren od strane upravljačkog tijela. Dokument pokriva većinu ključnih područja kibernetičke sigurnosti, uključujući upravljanje rizicima, zaštitu podataka i odgovor na incidente. Međutim, tijekom revizije uočeno je sljedeće:

- Dokument nije ažuriran posljednje dvije godine, iako je politika formalno definirala da se revizija treba provoditi godišnje.
- Politika ne uključuje specifične smjernice za sigurnost udaljenog rada, što je postalo ključno u trenutnim operativnim uvjetima.
- Nisu dostupni zapisi o formalnoj distribuciji i obuci zaposlenika u vezi s ovim dokumentom.

Uzrok/ci nesukladnosti:

- Nedostatak resursa ili neadekvatan nadzor nad provođenjem redovitih revizija dokumenta.
- Politika nije ažurirana kako bi se prilagodila novim radnim uvjetima, poput sve većeg udjela udaljenog rada.
- Nedostatak formalne distribucije: Procedura za obavještavanje zaposlenika o sadržaju i važnosti dokumenta nije dovoljno jasno definirana.

Posljedice nesukladnosti:

- Zastarjeli strateški akt ne odražava trenutne prijetnje i operativne izazove, što može rezultirati slabijim odgovorom na sigurnosne incidente.
- Neinformirani zaposlenici povećavaju rizik od nesvjesnih sigurnosnih propusta.
- Usvojiti proceduru za redovitu reviziju dokumenta i definirati odgovornu osobu ili tim koji će pratiti provedbu te obavještavati upravljačko tijelo o statusu.

Uvesti formalni proces distribucije dokumenta i obuke zaposlenika kako bi se osiguralo da svi zaposleni razumiju ključne smjernice i postupke definirane u politici.

Izraditi zapisnike o distribuciji i obukama kako bi se mogla dokumentirati usklađenost sa zahtjevima politike.

Dokazi i reference:

Pregled kibernetičke sigurnosne politike (verzija iz 2021.).

Izvještaji upravljačkog tijela o odobravanju politike.

Interni zapisnici o distribuciji politika i obukama zaposlenika (nisu pronađeni za predmetni dokument).

Dodatna napomena: Dio „3.2.4. Detaljni prikaz nalaza po mjerama" mora biti jasan, logično strukturiran i usmjeren na pružanje korisnih informacija koje subjekt može odmah primijeniti za unapređenje svog sigurnosnog sustava. Korisno je unijeti standardiziranu strukturu za svaku kontrolu kako bi se osigurala dosljednost i olakšalo razumijevanje nalaza.

3.2.5. Zaključak

Zaključak predstavlja završni dio izvješća u kojem se daje refleksija na provedeni proces revizije i pruža ocjena općeg stanja kibernetičke sigurnosti subjekta. Ovaj dio ne ponavlja detalje sažetka ključnih nalaza, već pruža sveukupnu procjenu zrelosti sigurnosnih mjera i sposobnosti subjekta da odgovori na postojeće i buduće sigurnosne izazove. Osim ocjene trenutnog stanja, zaključak služi kao temelj za postavljanje dugoročnih ciljeva u poboljšanju kibernetičke sigurnosti.

U zaključku se prvo daje opća ocjena razine sigurnosti subjekta, pri čemu se ističu ključna područja snage i slabosti subjekta identificirana tijekom revizije. Naglašava se važnost usklađenosti s definiranim sigurnosnim mjerama i njihov utjecaj na cjelokupnu sigurnosnu strategiju subjekta.

Zaključak uključuje i kratak osvrt na razinu spremnosti subjekta da provede potrebne promjene i prilagodbe u skladu s preporukama revizije. Na kraju, zaključak treba usmjeriti pažnju na dugoročne ciljeve subjekta u kontekstu kibernetičke sigurnosti.

3.2.6. Potpis revizora

Zaključno, izvješće mora sadržavati potpis revizora kako bi se potvrdila vjerodostojnost nalaza i preporuka. Potpis i službeni podatci revizora trebaju biti jasno istaknuti na kraju izvješća, neposredno

prije priloga. Potpis revizora treba sadržavati njegov vlastoručni potpis uz puno ime i prezime, stručnu titulu ili certifikate te datum izdavanja izvješća. Ako je izvješće rezultat timskog rada, moraju se navesti svi članovi revizorskog tima koji su sudjelovali u provođenju revizije zajedno s ulogom koju su imali u provedbi revizije, uz naznaku odgovorne osobe.

3.2.7. Prilozi s relevantnim dokazima

Prilozi su sastavni dio izvješća i služe za pružanje dodatnih informacija koje podržavaju nalaze revizije. Oni su ključni za osiguravanje transparentnosti revizijskog procesa, omogućujući detaljan uvid u korištenu dokumentaciju, provedene intervjue i tehničke analize te osiguravaju osnovu za razumijevanje izvješća. Označavaju se rimskim brojevima i navode u istom redoslijedu kako su referencirani u glavnom tekstu, pri čemu moraju biti jasno organizirani i lako upotrebljivi. Svi prilozi trebaju odgovarati glavnim nalazima izvješća, omogućujući detaljno razumijevanje revizijskog procesa bez preopterećenja osnovnog teksta tehničkim ili dodatnim informacijama

Svako izvješće o provedenoj reviziji kibernetičke sigurnosti obavezno mora sadržavati tri priloga: popis pregledanih dokumenata i evidencija, popis intervjuiranih osoba, te detalje tehničkih analiza.

3.2.7.1. Popis pregledanih dokumenata i evidencija (Prilog I)

Prilog I sadrži iscrpan popis svih dokumenata, zapisa i drugih materijala koji su pregledani tijekom revizije. Ovo uključuje, ali nije ograničeno na:

- Sigurnosne politike i procedure,
- Izvještaje o incidentima,
- Dnevničke zapise (logove),
- Zapise o održavanju softvera i ažuriranjima,
- Evidenciju o obukama zaposlenika,
- Procjena rizika.

Ovaj popis omogućuje dionicima da jasno vide koji su izvori informacija korišteni za donošenje zaključaka i ocjena u izvješću. Uz svaki naziv potrebno je navesti i verziju dokumenta s datumom njegove izrade ili odobrenja odnosno neki drugi identifikator koji nedvosmisleno ukazuje na materijal koji je pregledan.

3.2.7.2. Popis intervjuiranih osoba (Prilog II)

Prilog II uključuje popis osoba koje su sudjelovale u reviziji kroz intervjue ili pružanje informacija. Uz imena i prezimena intervjuiranih osoba, navode se njihove uloge u subjektu i područja i/ili kontrole za koje su dali informacije. Ovaj prilog osigurava pregled nad relevantnim dionicima koji su pridonijeli revizijskom procesu te olakšava praćenje odgovornosti i komunikaciju.

3.2.7.3. Detalji tehničkih analiza (Prilog III)

Prilog III pruža dodatne tehničke informacije koje su ključne za razumijevanje specifičnih nalaza. Ovo uključuje tehničke testove poput penetracijskih testova, analizu postavki sigurnosnih sustava, rezultate skeniranja ranjivosti ili druge tehničke provjere provedene tijekom revizije. Prilog može uključivati i vizualne prikaze, poput snimki zaslona, dijagrama ili grafova, koji ilustriraju nalaze.

Ukoliko je tijekom provedbe mjere korišten automatizirani alat za identifikaciju i procjenu ranjivosti informacijskog sustava, preporučuje se da se rezultati takvog skeniranja dokumentiraju i pridruže ovom prilogu kao zasebna cjelina. U svrhu transparentnosti i sljedivosti provedenih aktivnosti, uz izvješće je potrebno navesti naziv korištenog alata, verziju, datum izvršenog skeniranja te, ako je primjenjivo, opseg sustava koji je bio predmetom skeniranja.

Ako je u okviru informacijskog sustava organizacije implementiran i aktivno korišten neki od alata za nadzor i detekciju prijetnji (poput SIEM, EDR, NDR ili IDS sustava), obvezno je kao dio dokumentacije priložiti reprezentativne dnevničke zapise tih alata.

Takvi zapisi moraju jasno dokazivati stvarnu sposobnost sustava za pravovremeno otkrivanje i reagiranje na sigurnosne prijetnje. Primjeri uključuju, ali nisu ograničeni na: evidentirane alarme o sumnjivim ili zlonamjernim aktivnostima, detaljne zapise o tijeku analize incidenta, automatske ili ručne radnje poduzete u svrhu blokiranja ili ublažavanja prijetnje, kao i vremenske oznake koje potvrđuju pravodobnost reakcije.

Organizacija je dužna osigurati da priloženi dnevnički zapisi budu u obliku koji omogućuje revizoru provjeru vjerodostojnosti podataka, uključujući informacije o izvoru, vrsti događaja, klasifikaciji prijetnje, radnjama poduzetima na temelju otkrivanja i relevantnim metapodacima.

3.3. Postupak najave i izvješćivanja

3.3.1. Najava revizije

PRUS-ovi su dužni unaprijed najaviti svaku planiranu reviziju kibernetičke sigurnosti ZSIS-u najmanje 10 radnih dana prije planiranog datuma revizije. Najava se dostavlja u elektroničkom obliku na adresu elektroničke pošte *najave_rks@zsis.hr* ili u pisanom obliku na službenu adresu ZSIS-a, uz jasno naznačene datume, mjesto, i predmet revizije.

Najava mora sadržavati i podatke o subjektu kod kojeg će se provoditi revizija, uključujući naziv pravnog subjekta i osnovne kontakt podatke. Ako dođe do promjena u planiranom terminu ili drugim ključnim informacijama najavljene revizije, PRUS je dužan obavijestiti ZSIS. Takva obavijest mora se poslati najkasnije 2 radna dana od nastupanja promjene.

ZSIS zadržava pravo tražiti dodatne informacije o najavljenoj reviziji te sudjelovati u promatranju revizije ukoliko to smatra nužnim. U takvom slučaju, PRUS je obvezan omogućiti prisustvo promatrača bez narušavanja neovisnosti revizije.

3.3.2. Čuvanje i dostupnost izvješća o reviziji kibernetičke sigurnosti

PRUS je dužan čuvati cjelovite izvještaje o rezultatima provedenih revizija kibernetičke sigurnosti u minimalnom trajanju od tri godine od završetka revizije. Izvješća o provedenoj reviziji kibernetičke sigurnosti moraju biti dostupna u slučaju nadzora od strane ZSIS-a. ZSIS ima ovlasti provjeravati potpunost izvješća, utvrditi sadrži li izvješće nedosljednosti te pregledavati dokaze koji podupiru nalaze revizije. Takvi dokazi uključuju, ali nisu ograničeni na zapisnike, fotografije, izjave ili druge relevantne materijale koji potvrđuju vjerodostojnost nalaza. Sva prateća dokumentacija mora biti jasno označena datumom, kako bi se osigurala vremenska usklađenost, te mora biti pregledno strukturirana radi lakše analize i korištenja.

4. Postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti

Ovo poglavlje propisuje postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti (dalje u tekstu: Certifikat). Certifikat je ključan za osiguravanje standardiziranog, transparentnog i vjerodostojnog postupka kojim se potvrđuje sposobnost PRUS-a za provođenje revizija kibernetičke sigurnosti u skladu s ZKS-om, te nacionalnim i međunarodnim standardima.

Postupak izdavanja certifikata nije postupak europske kibernetičke sigurnosne certifikacije u smislu Uredbe (EU) 2019/881 i Uredbe (EU) 2025/37 već je riječ o postupku predviđenom ZKS-om.

U postupku izdavanja certifikata definira se tko može podnijeti zahtjev, koji su uvjeti za njegovo dobivanje te postupak procjene kandidata, uključujući organizacijske i stručne zahtjeve, tehničke sposobnosti i usklađenost s regulativama kao što je navedeno u poglavlju 2. ovih Pravila. Ova pravila također uključuju smjernice o održavanju certifikata, periodičnim nadzorima i uvjetima za obnovu.

Postupak opoziva certifikata opisuje situacije u kojima certifikat može biti opozvan, poput neispunjavanja propisanih standarda, neetičkog ponašanja ili nedostatka stručnosti.

Ovo poglavlje osigurava da postupci izdavanja i opoziva certifikata budu jasni, pravični i usklađeni s relevantnim zakonskim i tehničkim zahtjevima.

PRUS prihvaća da se sve odluke u postupku certifikacije temelje na ispunjavanju propisanih uvjeta i standarda te ih prihvaća kao takve. Dostupna pravna zaštita propisana je ovim Pravilima, te isključuje mogućnost podnošenja tužbe protiv certifikacijskog tijela, a vezano uz ishod certifikacijskog postupka.

4.1. Postupak izdavanja certifikata

4.1.1. Pokretanje postupka

PRUS koji želi pokrenuti postupak certifikacije mora podnijeti zahtjev putem službenog Obrasca za prijavu certifikacije, koji je priložen ovom dokumentu kao Prilog A. Popunjen obrazac mora biti dostavljen ZSIS-u u elektroničkom obliku na adresu elektroničke pošte *certificiranje_rks@zsis.hr* ili u pisanom obliku na adresu sjedišta ZSIS-a.

Obrazac za prijavu certifikacije sadrži ključne podatke o PRUS-u, uključujući:

- Naziv pravnog subjekta i sjedište,
- Kontakt informacije (telefon, e-mail, adresa za korespondenciju),
- Izjava o sukladnosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima (Prilog IV Uredbe),
- Popis referenci.

Uz popunjeni obrazac, PRUS mora priložiti sljedeću dokumentaciju:

- Izvadak iz sudskog, obrtnog, strukovnog ili drugog registra kojim se dokazuje registracija pravnog subjekta u Republici Hrvatskoj,
- Dokaz o tehničkoj opremljenosti i resursima za provođenje revizija,
- Interni pravilnik o neovisnosti i nepristranosti revizora,
- Informacije o PRUS-u:
    - Opis područja stručnosti i djelatnosti,
    - Organizacijska shema;
        - opisi poslova,
        - interni pravilnici,
    - Politike za sprječavanje sukoba interesa,
    - Izvješća o internim revizijama - u sklopu provjere kvalitete internog procesa revizije,
    - Akreditacija prema međunarodnim standardima - ukoliko posjeduje s uključenim opsegom akreditacije,
    - Izjavu da raspolaže stručnjacima osposobljenim po unaprijed definiranim zahtjevima i broj stručnjaka.

Nepotpuna ili netočna prijava bit će vraćena podnositelju na ispravak, uz rok od 10 radnih dana za dopunu dokumentacije. U slučaju isteka roka bez dopune, prijava će se smatrati povučenom. Za sve tvrdnje navedene u Obrascu za prijavu certifikacije potrebno je dostaviti i dokaz ukoliko ga PRUS posjeduje, tako primjerice za tvrdnju da je PRUS certificiran prema standardu ISO/IEC 17021-1:2015 PRUS mora dostaviti i kopiju certifikata koja navedeno potvrđuje. Osobni certifikati djelatnika PRUS-a moraju biti dostupni na uvid prilikom „Revizorske posjete“.

Po primitku ispunjenog obrasca i pripadajuće dokumentacije, ZSIS imenuje stručni radni tim koji provodi preliminarnu provjeru kako bi ocijenio ispunjava li PRUS osnovne uvjete za ulazak u postupak certifikacije. Ova provjera uključuje:

- Analizu dostavljenih dokumenata,
- Pregled internih politika i procedura PRUS-a vezanih za provođenje revizija.

Po potrebi, prije preliminarne provjere može se održati pripremni sastanak između ZSIS-a i PRUS-a koji je podnio prijavu, radi pojašnjavanja zadovoljavanja osnovnih uvjeta.

Ako preliminarna provjera pokaže nedostatke, podnositelj će biti obaviješten u roku od 10 radnih dana o potrebnim dodatnim koracima ili ispravcima. U slučaju zadovoljavajuće preliminarne provjere, podnositelj će biti službeno obaviješten o prelasku na sljedeću fazu postupka certifikacije.

4.1.2. Certificiranje PRUS-a

Nakon što PRUS uspješno prođe preliminarnu provjeru, ZSIS započinje postupak certificiranja kroz temeljitu i sveobuhvatnu analizu dostavljene dokumentacije. Ovaj proces osigurava usklađenost PRUS-a sa propisanim standardima, te se tijekom provedbe provjerava korištenje metoda i alata koje PRUS planira primjenjivati u svojem radu kao i uspostavljeni planovi za edukaciju osoblja. ZSIS također provodi procjenu kompetencija članova tima kako bi se osiguralo da svi zaposlenici PRUS-a koji će biti zaduženi za provođenje revizija kibernetičke sigurnosti posjeduju odgovarajuća znanja i vještine potrebne za učinkovitu provedbu istih. Na kraju slijedi završna evaluacija, kojom se donosi nepristrana odluka o certifikaciji, temeljena na objektivnim kriterijima i rezultatima prethodnih provjera.

4.1.2.1. Faza 1 – analiza dokumentacije

Prva faza procesa certifikacije nakon preliminarne provjere sastoji se od temeljite i sveobuhvatne analize dokumentacije koju je PRUS dostavio. Ova faza ima ključnu ulogu u procjeni osnovnih kompetencija PRUS-a za provođenje revizija u skladu s važećim standardima, normama i zakonodavnim zahtjevima. Cilj detaljne analize dokumentacije jest osigurati da PRUS posjeduje sve potrebne procedure, pravila i politike te da je njihova implementacija jasno definirana i lako dokaziva.

Pregled dokumenata uključuje interne dokumente poput pravilnika, procedura i politika PRUS-a, kao i tehničke dokumente koji se odnose na metode i alate za provođenje revizija. Posebna pažnja

posvećuje se jasnoći, konzistentnosti i usklađenosti dokumenata s relevantnim standardima, kao što su međunarodne ISO/IEC norme, te s nacionalnim zakonodavnim okvirom.

Na početku se provodi analiza internih dokumenata PRUS-a. Pored jasno dokumentiranog procesa revizija pravilnici i procedure trebaju sadržavati jasne opise metodologije za provođenje revizija, uključujući faze planiranja, provođenja, izvještavanja i završavanja revizijskih aktivnosti. Svaki dokument mora jasno identificirati uloge i odgovornosti pojedinih članova tima, kako bi se osigurala transparentnost procesa i spriječile potencijalne nejasnoće ili sukobi interesa. ZSIS provjerava je li ovim pravilnicima omogućena konzistentna provedba revizije i jesu li u skladu s najboljim praksama u industriji.

Poseban naglasak stavlja se na politike koje osiguravaju nepristranost i neovisnost revizora. ZSIS analizira mjere koje PRUS primjenjuje kako bi spriječio sukob interesa, poput pravila o izbjegavanju osobnih i profesionalnih poveznica s potencijalnim klijentima koji mogu biti predmet revizije. Također se procjenjuje jesu li politike/pravila povjerljivosti adekvatne za zaštitu osjetljivih informacija tijekom i nakon provođenja revizija. Sve procedure za upravljanje povjerljivim informacijama moraju biti jasno definirane i u skladu s propisima o zaštiti podataka.

Osim formalnih pravilnika, ZSIS pregledava tehničke dokumente koji se odnose na specifične metode i alate koje PRUS planira koristiti. Dokumentacija mora sadržavati detaljne opise korištenih metodologija za procjenu sukladnosti, analizu rizika i izvještavanje o nalazima. U slučaju da PRUS koristi specijalizirane softverske alate ili tehnologije, provodi se evaluacija njihove funkcionalnosti i usklađenosti s relevantnim standardima.

Važan aspekt analize dokumentacije jest potvrditi da PRUS ima uspostavljene adekvatne planove za edukaciju i kontinuirano stručno usavršavanje članova revizorskog tima. Planovi moraju sadržavati informacije o redovitom osposobljavanju članova revizorskog tima, uključujući tehničke obuke, certifikacije i sudjelovanje na stručnim skupovima. Ovo je važno kako bi PRUS mogao održavati visoku razinu stručnosti i kompetentnosti članova revizorskog tima. Uz navedeno provjeravaju se i dostavljeni dokazi o provedenim internim i vanjskim edukacijama.

Ako se tijekom pregleda dokumentacije utvrde nejasnoće, nedostaci ili nesukladnosti, PRUS-u se omogućuje prilika za ispravak ili dopunu dokumentacije kako bi se zadovoljili propisani standardi i zahtjevi procesa certifikacije. Rok za dostavljanje traženih ispravaka iznosi do šest mjeseci. U slučaju da PRUS u zadanom roku ne dostavi tražene ispravke ili ne pruži adekvatno obrazloženje kašnjenja,

proces certifikacije može biti privremeno obustavljen. Privremena obustava podrazumijeva zamrzavanje daljnjih aktivnosti povezanih s certifikacijom do trenutka kada PRUS dostavi potrebnu dokumentaciju ili ispravi utvrđene nedostatke. Za vrijeme trajanja obustave, PRUS će biti obaviješten o specifičnim razlozima obustave, potrebnim koracima za nastavak procesa te dodatnim rokovima, ako su primjenjivi. Ako se nedostaci ne otklone ni u naknadno definiranom razdoblju, proces certifikacije može se zaključiti kao neuspješan. U takvom slučaju, PRUS ne može podnijeti zahtjev za ponovno pokretanje certifikacijskog postupka u razdoblju od šest mjeseci od dana donošenja rješenja.

4.1.2.2. Faza 2 – Revizorska posjeta

Korak 1

Tijekom revizorske posjete, u prvom koraku provodi se detaljan pregled PRUS-a s ciljem potvrde da stvarno stanje implementacije odgovara podacima dostavljenima u dokumentaciji. ZSIS u ovoj fazi procjenjuje ispunjava li PRUS sve zahtjeve vezane uz proces i resurse potrebne za kvalitetno i kontinuirano provođenje revizija kibernetičke sigurnosti. Poseban naglasak stavlja se na provjeru upravljanja osposobljavanjem osoblja, što uključuje sustavno utvrđivanje potreba za edukacijom u različitim segmentima revizijskog procesa, organiziranje i provođenje edukacija i obnove certifikata/potvrda o osposobljenosti te dokumentiranje svih aktivnosti kontinuiranog osposobljavanja. Ovim se korakom osigurava da PRUS ima uspostavljene i aktivne mehanizme za jačanje kapaciteta i razvoja znanja svog tima.

Korak 2

Ovisno o zahtjevima i okolnostima, procjena može uključivati detaljniji ili sažetiji pristup, s ciljem osiguravanja da PRUS raspolaže kvalificiranim kadrom sposobnim za profesionalno i stručno provođenje revizija.

U drugom koraku fokus revizorske posjete je na detaljnoj procjeni kompetencija osoblja PRUS-a. Ova procjena provodi se uvidom u prateću dokumentaciju i putem intervjua sa zaposlenicima. ZSIS analizira dokumentirane procese osposobljavanja te provjerava zapise koji potvrđuju stručnost zaposlenika, uključujući certifikate, potvrde o završenim edukacijama te druge relevantne dokaze. Posebna pažnja posvećuje se i razini poznavanja zakonodavnog okvira u području revizije

kibernetičke sigurnosti. Cilj je osigurati da svi članovi osoblja PRUS-a posjeduju odgovarajuća znanja i vještine za učinkovito obavljanje svojih dužnosti unutar revizijskog procesa.

Uz organizacijske i stručne sposobnosti provjeravaju se i moralna i profesionalna pouzdanost članova revizorskog tima i PRUS-a. Naime, zbog pristupa sustavima, podacima i okruženju kritične infrastrukture ključnih subjekata, službenim osobama ZSIS-a tokom ove faze potrebno je dati na uvid:

- uvjerenje da se ne vodi kazneni postupak za kaznena djela koja se progone po službenoj dužnosti izdanu od nadležnog općinskog suda – za svakog člana revizorskog tima i
- uvjerenje da se ne vodi kazneni postupak za kaznena djela koja se progone po službenoj dužnosti izdanu od nadležnog općinskog suda – za pravnu osobu PRUS-a.

Navedena uvjerenja ne smiju biti starija od šest mjeseci. PRUS je dužan ova uvjerenja čuvati u svojoj internoj evidenciji i u svakom trenutku omogućiti njihovu dostupnost nadzornom tijelu ZSIS-a na zahtjev.

U slučaju da nakon izdavanja uvjerenja dođe do promjene okolnosti u odnosu na pojedinog člana revizorskog tima, a zbog kojih izmijenjenih okolnosti ne bi bilo izdano uvjerenje kako se ne vodi kazneni postupak, PRUS je obvezan ukloniti pojedinog člana revizorskog tima iz aktivne liste revizora odnosno obustaviti svako daljnje postupanje ukoliko se izmijenjene okolnosti odnose na pravnu osobu PRUS-a te bez odgađanja o tome izvijestiti ZSIS.

4.1.2.3. Faza 3 – završna evaluacija i donošenje odluke

Završna evaluacija i donošenje odluke predstavljaju posljednju, ali izuzetno važnu fazu u procesu certifikacije. U ovoj fazi ZSIS na temelju svih prikupljenih informacija i rezultata prethodnih faza donosi informiranu i nepristranu odluku o certifikaciji PRUS-a. Završna procjena osigurava da su sve analize, provjere i praktične procjene provedene temeljito, a da PRUS zadovoljava sve postavljene kriterije.

Proces završne evaluacije započinje sveobuhvatnim pregledom dokumentacije i izvještaja prikupljenih tijekom svih prethodnih koraka certifikacije. To uključuje analizu rezultata detaljne provjere dokumentacije i procjene kompetencija osoblja. ZSIS pažljivo pregledava svaki aspekt kako bi osigurao da su kriteriji zadovoljeni i da su sve eventualne nesukladnosti identificirane u

prethodnim fazama ispravljene. U ovoj fazi, svi nalazi organiziraju se u strukturirani završni izvještaj koji omogućava jasnu procjenu kompetencija PRUS-a.

Jedan od ključnih zadataka ZSIS-a tijekom završne procjene jest provjera dosljednosti između onoga što je PRUS dostavio kao dokaze o svojoj sposobnosti i onoga što je uočeno tijekom procesa certifikacije. Posebna pažnja posvećuje se usklađenosti PRUS-a s relevantnim normama, zakonodavnim zahtjevima i specifičnim smjernicama koje se odnose na područje kibernetičke sigurnosti. Ako se u ovoj fazi primijeti nedosljednost, ZSIS može zahtijevati dodatne dokaze ili pojašnjenja prije donošenja konačne odluke.

Završna procjena uzima u obzir analizu dokaza od strane službene osobe ZSIS-a koji nije sudjelovao u procesu certifikacije. Dok su jedna ili više službenih osoba ZSIS-a bili uključeni u procese certifikacije i prikupljanja podataka, završnu procjenu donosi neovisni stručnjak ZSIS-a na temelju prikupljenih dostupnih dokaza, čime se dodatno osigurava nepristranost i objektivnost u procesu procjene.

Tijekom završne evaluacije ZSIS također procjenjuje ukupni rizik povezan s certifikacijom PRUS-a. Ova procjena uključuje analizu potencijalnih izazova i slabosti koje bi mogle ugroziti sposobnost PRUS-a za dosljedno i učinkovito provođenje revizija u skladu s propisanim standardima. Ako ZSIS utvrdi da postoji značajan rizik koji nije adekvatno riješen, može odlučiti odgoditi izdavanje certifikata dok PRUS ne poduzme potrebne korektivne mjere.

Čelnik ZSIS-a će konačnu odluku o certifikaciji donijeti u pravilu u roku od šest mjeseci od dana zaprimanja ispunjenog obrasca (Prilog A) i pripadajuće dokumentacije, a na temelju završne procjene neovisnog stručnjaka ZSIS-a. Odluka se dokumentira u službenom aktu koji obuhvaća sljedeće elemente:

- Zaključak evaluacije – sažetak nalaza iz svih faza certifikacije.
- Status organizacije – potvrda o uspješnom ispunjavanju kriterija.
- Preporuke za daljnje aktivnosti – ako PRUS dobije certifikat, uključuju se preporuke za održavanje usklađenosti, godišnjih nadzora i obaveznog praćenja ključnih promjena u procesu revizija.

Ako PRUS zadovolji sve zahtjeve, ZSIS izdaje certifikat koji potvrđuje sposobnost za provođenje revizija kibernetičke sigurnosti u skladu s propisanim standardima. Certifikat vrijedi tri godine, uz

uvjet provođenja periodičnih nadzora, propisanih u poglavlju „4.3.1. Redovni nadzor“, od strane ZSIS kako bi se osiguralo održavanje standarda.

Izdavanjem certifikata od strane ZSIS-a, PRUS stječe status revizora kibernetičke sigurnosti za ključne i važne subjekte u skladu s člankom 32., stavkom 2., podstavkom 1. ZKS u Republici Hrvatskoj.

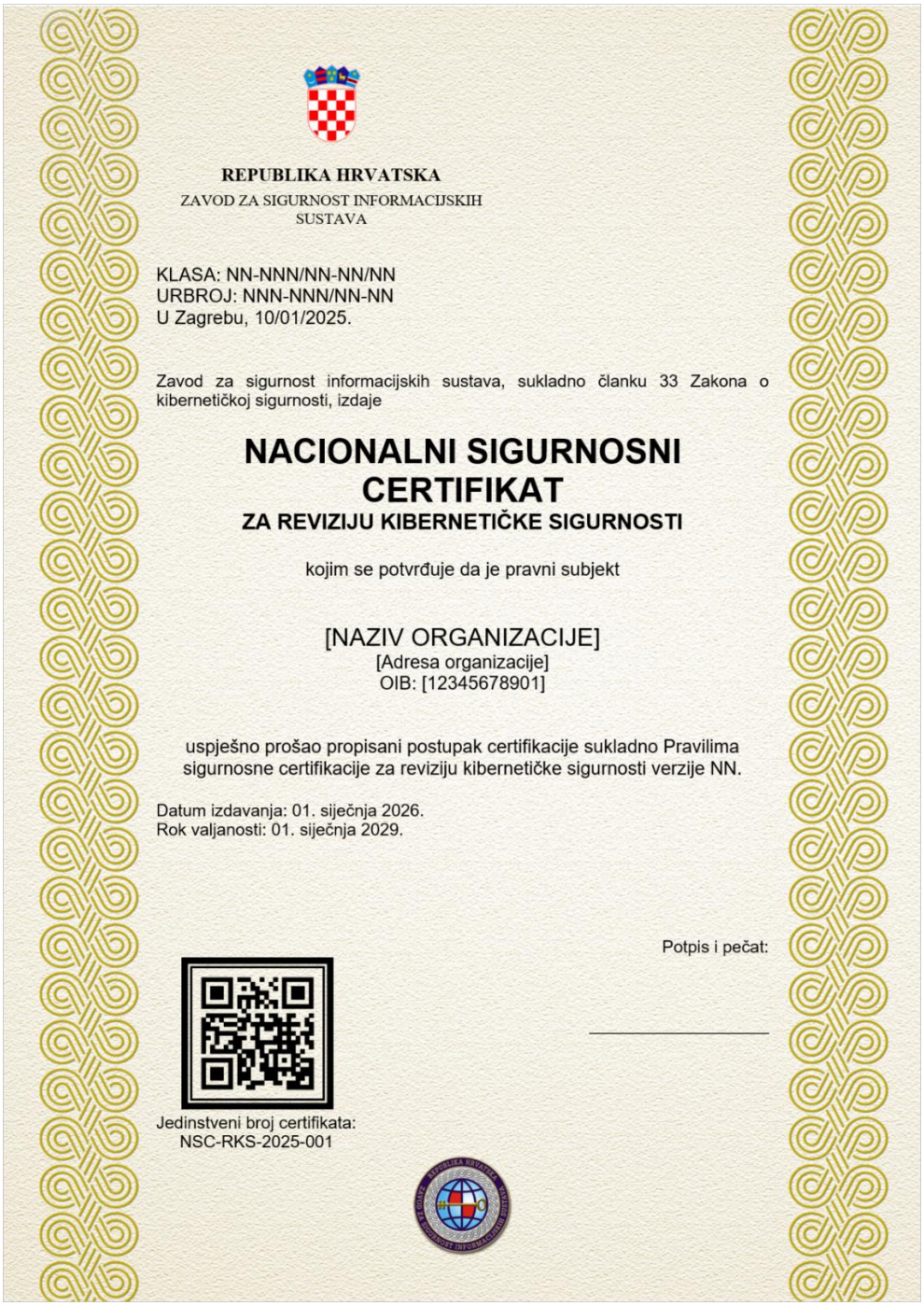
U slučaju da PRUS ne zadovolji uvjete, ZSIS izdaje obrazloženu odluku o odbijanju certifikacije. PRUS ima pravo na žalbu u propisanom roku ili na ponavljanje određenih faza certifikacijskog procesa nakon provedbe potrebnih korektivnih mjera. U ovim slučajevima ZSIS pruža smjernice za ispravljanje utvrđenih nedostataka.

4.1.3. Struktura i izgled certifikata

U nastavku je detaljno opisan izgled i sadržaj certifikata, uključujući sve ključne elemente. Certifikat se sastoji od:

- naslova dokumenta,
- podataka o izdavatelju certifikata,
- broja certifikata,
- podataka o certificiranoj organizaciji,
- vrste certifikata,
- datuma izdavanja i roka valjanosti,
- potpisa i pečata,
- QR koda za provjeru valjanosti certifikata.

Izgled certifikata prikazan je na donjoj slici, koja ilustrira sve njegove ključne elemente i strukturu. Prikaz služi kao smjernica za izradu službenog certifikata.



REPUBLIKA HRVATSKA
ZAVOD ZA SIGURNOST INFORMACIJSKIH SUSTAVA

KLASA: NN-NNN/NN-NN/NN
URBROJ: NNN-NNN/NN-NN
U Zagrebu, 10/01/2025.

Zavod za sigurnost informacijskih sustava, sukladno članku 33 Zakona o kibernetičkoj sigurnosti, izdaje

NACIONALNI SIGURNOSNI CERTIFIKAT
ZA REVIZIJU KIBERNETIČKE SIGURNOSTI

kojim se potvrđuje da je pravni subjekt

[NAZIV ORGANIZACIJE]
[Adresa organizacije]
OIB: [12345678901]

uspješno prošao propisani postupak certifikacije sukladno Pravilima sigurnosne certifikacije za reviziju kibernetičke sigurnosti verzije NN.

Datum izdavanja: 01. siječnja 2026.
Rok valjanosti: 01. siječnja 2029.

Potpis i pečat:

Jedinstveni broj certifikata:
NSC-RKS-2025-001

4.1.4. Žalbe

U slučaju da ZSIS odbije izdavanje certifikata, PRUS ima pravo pokrenuti žalbeni postupak. Ovaj postupak osigurava transparentnost, pravičnost i mogućnost ponovne procjene odluke o certificiranju kroz jasno definirane korake.

Žalba se izjavljuje ZSIS-u u roku od 15 dana od dana zaprimanja Odluke o odbijanju certifikacije. Žalba se dostavlja ZSIS-u u pisanom obliku neposredno, putem ovlaštenog pružatelja poštanskih usluga, na adresu sjedišta ZSIS-a ili elektroničkom poštom na adresu *zalbe_rks@zsis.hr*.

Žalba mora sadržavati osnovne podatke o organizaciji, presliku odluke ZSIS-a o neizdavanju certifikata te detaljno obrazloženje razloga zbog kojih se osporava odluka. Žalba također mora sadržavati sve relevantne dokaze ili dokumentaciju koji podržavaju tvrdnje PRUS-a, kao što su dodatni podaci ili analize koje PRUS smatra ključnima za preispitivanje odluke. Žalba mora biti potpisana od strane ovlaštene osobe PRUS-a.

Po zaprimanju žalbe, ZSIS je obvezan potvrditi primitak PRUS-u u roku od tri radna dana. Ova potvrda uključuje informacije o tome kada je žalba zaprimljena te jedinstveni broj predmeta koji će se koristiti za praćenje žalbenog postupka. ZSIS zatim provodi preliminarni pregled žalbe kako bi se utvrdilo je li izjavljena u propisanom roku te sadrži li sve potrebne elemente. Ako žalba nije potpuna, PRUS dobiva obavijest o potrebi dopune dokumentacije, s rokom od pet radnih dana za dostavljanje nedostajućih podataka.

Nakon što se utvrdi da je žalba izjavljena u roku te da sadrži sve potrebne podatke i dokumentaciju, ZSIS formira neovisno povjerenstvo za razmatranje žalbi. Ovo povjerenstvo sastoji se od stručnjaka ZSIS-a koji nisu bili uključeni u postupak izdavanja certifikata koji je rezultirao donošenjem odluke o odbijanju certifikacije, čime se osigurava nepristranost i objektivnost u žalbenom postupku. Povjerenstvo analizira sve navode iz žalbe, dostavljene dokumente, uključujući originalne nalaze iz postupka certifikacije i priložene dokaze. Ako je potrebno, povjerenstvo može zatražiti dodatne informacije ili objašnjenja od PRUS-a.

Tijekom žalbenog postupka, povjerenstvo može provesti dodatne procjene, uključujući reviziju pojedinih dijelova postupka certifikacije, dodatne intervjue s osobljem PRUS-a ili pregled dokumentacije koja nije bila dostupna u prvotnom postupku. Cilj dodatnih procjena je osigurati da se svi navodi žalbe temeljito razmotre i da se donese objektivna i na stvarnom stanju utemeljena odluka o žalbi.

Po završetku razmatranja, povjerenstvo daje preporuku čelniku ZSIS-a o tome treba li prvobitnu odluku potvrditi ili poništiti. Čelnik ZSIS-a donosi konačnu odluku na temelju preporuke povjerenstva. Odluka o žalbi uključuje detaljno obrazloženje razloga za odbijanje žalbe ili, u slučaju usvajanja žalbe, mjere koje će se poduzeti u cilju izdavanja certifikata. Odluka se dostavlja PRUS-u putem službenog kanala kojim je PRUS podnio žalbu.

4.1.5. Pritužbe

Subjekt nad kojim PRUS provodi reviziju može ZSIS-u u slučaju ako nije zadovoljan Izvješćem o provedenoj reviziji kibernetičke sigurnosti ili ako dvoji o profesionalnosti, stručnosti ili zadovoljavanju drugih uvjeta PRUS-a podnijeti pritužbu ZSIS-u.

Subjekt može podnijeti pritužbu tijekom postupka revizije, a najkasnije 15 radnih dana od dana primitka Izvješća o provedenoj reviziji kibernetičke sigurnosti. Pritužba mora biti dostavljena ZSIS-u u pisanom obliku putem ovlaštenog pružatelja poštanskih usluga na adresu sjedišta ZSIS-a ili elektroničkim putem na adresu elektroničke pošte *prituzbe_rks@zsis.hr* predviđenu za ovakve postupke.

Smatra se da je Izvješće o provedenoj reviziji kibernetičke sigurnosti dostavljeno subjektu od strane PRUS-a u trenutku kad ga subjekt zaprimi putem poštanske dostave, elektroničke pošte ili osobnim uručenjem.

Subjekt je dužan, prije podnošenja pritužbe, na primjeren način upoznati PRUS sa svojim primjedbama i nastojati sporazumno riješiti predmetni problem.

Prilikom podnošenja pritužbe, subjekt je obvezan detaljno obrazložiti razloge osporavanja izvješća te navesti specifične okolnosti koje dovode u pitanje profesionalnost, stručnost ili ispunjavanje drugih propisanih uvjeta koje PRUS mora zadovoljiti. Pritužba mora sadržavati sve relevantne dokaze ili dokumentaciju koja podržava tvrdnje subjekta, kao što su dodatni podaci ili analize koje subjekt smatra ključnim za svoje postupke. Pritužba mora biti potpisana od strane ovlaštene osobe subjekta. Po zaprimanju pritužbe, ZSIS je obvezan potvrditi primitak pritužbe u roku od tri radna dana. Ova potvrda uključuje informacije o tome kada je pritužba zaprimljena te jedinstveni broj predmeta koji će se koristiti za praćenje procesa pritužbe.

ZSIS zatim provodi preliminarni pregled pritužbe kako bi utvrdio je li izjavljena u propisanom roku te sadrži li sve potrebne elemente, između ostalih i je li subjekt PRUS-u ukazao na svoje primjedbe, te moguće dodatne podatke ili analize na koje se ukazuje, a koji su morali postojati tijekom postupka revizije PRUS-a kod subjekta, odnosno najkasnije u trenutku izrade Izvješća.

Ako subjekt na svoje primjedbe nije ukazao PRUS-u, ta se pritužba neće razmatrati. Ako pritužba nije potpuna, subjekt dobiva obavijest o potrebi dopune dokumentacije s rokom od pet radnih dana za dostavljanje nedostajućih podataka.

Nakon što se utvrdi da je pritužba izjavljena u roku te da sadrži sve potrebne podatke i dokumentaciju, ustrojstvena jedinica ZSIS-a nadležna za certificiranje razmotrit će pritužbu. Analizirat će sve dostavljene dokumente, uključujući originalne nalaze iz postupka izdavanja Izvješća, samu pritužbu i priložene dokaze. Ako je potrebno ZSIS može zatražiti dodatne informacije ili obrazloženja od subjekta i PRUS-a.

Rješavajući pritužbu ZSIS može provesti nenajavljeni nadzor kod PRUS-a protiv kojeg je podnesena pritužba. Tijekom obavljanja nenajavljenog nadzora primjenjuju se odredbe ovih Pravila („4.3.2. Nenajavljeni nadzor“).

Subjekt, podnositelj pritužbe, biti će službeno obaviješten o ishodu postupka. Obavijest će sadržavati detaljno obrazloženje, uključujući razloge za odbijanje pritužbe ili u slučaju pozitivnog ishoda, mjere koje će biti poduzete.

Pritužbu može podnijeti i bilo koja druga zainteresirana strana u postupku, kao i PRUS u slučaju pritužbe na rad službene osobe ZSIS-a u postupku certifikacije PRUS-a.

4.1.6. Registar certificiranih pružatelja upravljanih sigurnosnih usluga

Ovim Pravilima propisuje se postupak vođenja, ažuriranja i objavljivanja Registra certificiranih pružatelja upravljanih sigurnosnih usluga za reviziju kibernetičke sigurnosti (u daljnjem tekstu: Registar) koji je u nadležnosti ZSIS-a. Registar se uspostavlja s ciljem osiguravanja transparentnosti, vjerodostojnosti i dostupnosti podataka o svim certificiranim pružateljima upravljanih sigurnosnih usluga (PRUS-ovima).

Registar se vodi u digitalnom obliku, koristeći standardiziranu tabličnu strukturu koja omogućava jednostavno ažuriranje i pretraživanje podataka. Registar se nalazi na službenim stranicama ZSIS-a, gdje je javno dostupan svim zainteresiranim stranama.

Svaki PRUS koji je certificiran od strane ZSIS-a unosi se u Registar odmah po izdavanju certifikata. Upis u Registar obavlja se na temelju certifikata koji predstavlja službeni akt o certifikaciji i sadrži sve relevantne podatke o PRUS-u i području djelovanja.

Registar se objavljuje u tabličnom obliku, a svaki unos sadrži sljedeće obavezne informacije:

- Identifikacijski broj certifikata: Jedinstveni broj certifikata dodijeljenog organizaciji.
- Naziv organizacije: Puni pravni naziv certificiranog PRUS-a.

- OIB PRUS-a.
- Datum izdavanja certifikata: Datum kada je certifikat izdan.
- Datum isteka certifikata: Datum do kojeg je certifikat valjan, osim u slučaju ranijeg opoziva.
- Status certifikata: Trenutni status certifikata (aktivan, suspendiran, opozvan).
- Kontakt informacije: Osnovni podaci za kontakt PRUS-a (adresa, telefon, e-mail).
- Napomene: Ostale relevantne informacije (npr. ograničenja, verzija Pravila po kojoj je izdan certifikat i ostalo).

ZSIS je odgovoran za ažuriranje Registra, osiguranje njegove dostupnosti i transparentnosti informacija te za periodičnu provjeru točnosti podataka. Sve promjene u statusu certifikata, poput obnove, suspenzije ili opoziva, moraju se evidentirati u Registru u roku od tri radna dana od nastanka promjene. ZSIS je dužan osigurati da Registar bude kontinuirano dostupan na službenim stranicama, uz primjenu tehničkih mjera za očuvanje integriteta i sigurnosti podataka. ZSIS je obvezan provoditi godišnji pregled Registra kako bi se osiguralo da su svi unosi točni i usklađeni s važećim statusom certificiranih organizacija.

Certificirani PRUS-ovi imaju obvezu obavijestiti ZSIS o svim promjenama koje mogu utjecati na točnost podataka unesenih u Registar. To uključuje promjene kontaktnih informacija, promjene u opsegu usluga koje pružaju ili pravne promjene, poput promjena naziva, statusa ili vlasništva. PRUS-ovi su dužni dostaviti obavijest o takvim promjenama u roku od pet radnih dana od njihova nastanka. Pravovremena dostava ovih informacija ključna je za održavanje ažurnosti i točnosti podataka u Registru te za očuvanje povjerenja u certificirane organizacije.

ZSIS osigurava točnost i ažurnost svih podataka unutar Registra na temelju dostavljene dokumentacije. Certificirane organizacije odgovorne su za istinitost i točnost informacija koje pružaju ZSIS-u radi upisa ili ažuriranja podataka. Ako se utvrdi netočnost ili neusklađenost podataka, ZSIS zadržava pravo ispraviti pogreške ili staviti napomenu o navedenom u Registar dok se ne otklone nepravilnosti. Ovaj pristup osigurava pouzdanost Registra kao alata za provjeru certificiranih organizacija.

Podaci iz Registra smiju se koristiti isključivo u svrhu provjere statusa certificiranih organizacija i njihovog opsega djelovanja. Zabranjeno je koristiti informacije iz Registra za komercijalne, oglašivačke ili druge svrhe koje nisu odobrene od strane ZSIS-a. Svaka zloupotreba informacija iz Registra predstavlja povredu pravila i može rezultirati poduzimanjem odgovarajućih pravnih mjera.

4.2. Postupak suspenzije i opoziva certifikata

Postupak opoziva certifikata je formalni proces kojim se preispituje valjanost certifikata dodijeljenog PRUS-u, a na temelju sumnji u njegovu sposobnost dosljednog ispunjavanja propisanih standarda i uvjeta certificiranja. Tijekom postupka, ZSIS analizira dokaze, razmatra očitovanja PRUS-a i donosi odluku o daljnjem statusu certifikata. Izdani certifikat moguće je privremeno staviti pod suspenziju do otklanjanja utvrđenih nesukladnosti provođenjem korektivnih mjera, dok opoziv certifikata označava trajno poništenje certifikata zbog utvrđenih nepravilnosti, nesukladnosti ili drugih razloga koji ugrožavaju povjerenje u PRUS i kvalitetu njegovih usluga. Opoziv ima za cilj zaštitu standarda, korisnika i integriteta certificiranja.

PRUS ne smije prelaziti okvire opsega revizije koji je određen mjerama i kontrolama ovog dokumenta i njegovih priloga. Ukoliko ZSIS utvrdi opseg koji prelazi navedene granice, PRUS-u može biti opozvan certifikat.

4.2.1. Faza 1 – Pokretanje postupka

Pokretanje postupka opoziva certifikata predstavlja prvi korak u procesu kojim ZSIS započinje formalnu proceduru preispitivanja valjanosti certifikata dodijeljenog određenom PRUS-u.

Postupak opoziva može biti pokrenut iz različitih razloga, uključujući, ali ne ograničavajući se na, nepridržavanje propisanih standarda i normi, sustavne nedosljednosti u provođenju revizorskih aktivnosti ili zaprimljene prijave trećih strana koje ukazuju na ozbiljne propuste, nepravilnosti ili neusklađenost u radu PRUS-a. Povod za pokretanje postupka može biti i samoinicijativna procjena ZSIS-a, primjerice tijekom redovnih ili izvanrednih nadzora, kada se utvrde elementi koji dovode u pitanje usklađenost PRUS-a s uvjetima certificiranja.

ZSIS je obvezan prije formalnog pokretanja postupka prikupiti osnovne dokaze i informacije koji pružaju inicijalnu osnovu sumnje za povredu uvjeta. U tom kontekstu, provodi se analiza dostupnih podataka, uključujući prethodne revizijske izvještaje, rezultate nadzornih aktivnosti ili informacije iz vanjskih izvora, poput pritužbi klijenata ili regulatornih tijela.

Pokretanjem postupka, ZSIS ne prejudicira konačnu odluku o opozivu certifikata, već započinje formalni proces ispitivanja kako bi se utvrdila točnost i težina sumnji.

4.2.2. Faza 2 – Izdavanje obavijesti

Izdavanje obavijesti o pokretanju postupka opoziva predstavlja drugi korak u procesu, kojim ZSIS formalno obavještava certificirani PRUS o pokretanju postupka opoziva certifikata. Ova obavijest ima ključnu ulogu u osiguravanju transparentnosti postupka i prava PRUS-a na očitovanje i obranu.

Obavijest se izdaje u pisanom obliku i mora sadržavati precizne i jasne informacije o razlozima zbog kojih se postupak opoziva pokreće. ZSIS u obavijesti navodi konkretne nalaze ili okolnosti koje su dovele do sumnji u usklađenost PRUS-a s uvjetima certifikacije. To uključuje detaljan opis uočenih nepravilnosti, nesukladnosti s normama i standardima ili drugih okolnosti koje bi mogle ugroziti valjanost certifikata. Uz to, prilažu se svi relevantni dokazi ili dokumenti koji potkrepljuju navedene razloge, kao što su izvještaji iz nadzora, analize ili prijave trećih strana.

Cilj obavijesti je ne samo informirati PRUS o postupku, već i omogućiti mu da pravodobno pripremi očitovanje i dostavi dodatnu dokumentaciju ili dokaze koji bi mogli osporiti navode iz obavijesti. ZSIS u obavijesti definira rok za očitovanje PRUS-a, koji u pravilu iznosi 15 radnih dana od dana primitka obavijesti. PRUS se obavještava o propisanom načinu dostave očitovanja, uz navođenje prihvatljivih komunikacijskih kanala.

Uz navedeno, obavijest mora sadržavati i podatke o kontakt osobi unutar ZSIS-a koja je zadužena za postupak, kako bi PRUS mogao postaviti eventualna dodatna pitanja ili razjasniti nejasnoće. Ovim se osigurava otvorena komunikacija između PRUS-a i ZSIS-a te omogućuje potpuna informiranost svih uključenih strana.

4.2.3. Faza 3 – Procjena očitovanja i donošenje odluke

Procjena očitovanja započinje nakon što PRUS dostavi svoj odgovor na obavijest o pokretanju postupka opoziva. ZSIS detaljno analizira sve dostavljene informacije, uključujući pisano očitovanje, priložene dokaze i sve relevantne dokumente koje je PRUS dostavio u svrhu svoje obrane. Fokus ove analize je na procjeni jesu li očitovanja i dokazi PRUS-a dovoljni za otklanjanje sumnje u postojanje nepravilnosti ili nesukladnosti sa standardima certificiranja. ZSIS ocjenjuje točnost, vjerodostojnost i konzistentnost dostavljenih podataka te provodi dodatne provjere, ako je potrebno, kako bi se utvrdila istinitost navoda PRUS-a.

Ako ZSIS utvrdi da su priloženi dokazi nepotpuni ili nedovoljno jasni, može zatražiti dodatne informacije od PRUS-a. Ovo uključuje mogućnost organiziranja dodatnih sastanaka, intervjua ili

revizija kako bi se razjasnile nejasnoće ili proturječnosti. ZSIS može angažirati i neovisne stručnjake kako bi se osigurala objektivnu i profesionalnu procjenu tehničkih ili specijaliziranih aspekata slučaja.

Nakon što se prikupi i analizira cjelokupna dokumentacija, ZSIS donosi Odluku utemeljenu na rezultatima svih prethodnih faza postupka, uključujući nalaze iz nadzornih aktivnosti, informacije iz obavijesti, očitovanja PRUS-a i dodatne analize. ZSIS može donijeti sljedeće odluke: odluku o opozivu certifikata, odluku o privremenoj suspenziji certifikata ili obustaviti postupak opoziva:

- Do opoziva certifikata PRUS-a dolazi ako su utvrđene nesukladnosti ili povrede uvjeta certificiranja ozbiljne i neotklonjive.
- Do privremene suspenzije certifikata uz uvjet provedbe korektivnih mjera dolazi ako se procijeni da nesukladnosti mogu biti otklonjene u razumnom roku. Privremena suspenzija certifikata može trajati najdulje godinu dana, ali ne dulje od vremena važenja certifikata. Privremena suspenzija certifikata završava potvrdom valjanosti certifikata i time obustavom postupka opoziva ako se nadzorom kroz naknadnu reviziju utvrdi da je u ostavljenom roku PRUS u bitnome ispunio korektivne mjere. U slučaju da naknadnom revizijom utvrđene nesukladnosti ili povrede uvjeta certificiranja nisu otklonjene, certifikat koji je bio privremeno suspendiran se opoziva.
- Do obustave postupka opoziva dolazi ako očitovanje i dostavljeni dokazi uvjerljivo potvrde da PRUS zadovoljava sve uvjete certificiranja.

Postupak opoziva certifikata mora biti dokumentiran, odluka sadržavati detaljno obrazloženje o razlozima donošenja. Odluka ZSIS-a uključuje obrazloženje razloga za opoziv, suspenziju ili obustavu postupka, kao i konkretne korake koje PRUS treba poduzeti u slučaju da mu se omogući provedba korektivnih mjera. Odluka se dostavlja PRUS-u u pisanom obliku, uz jasne upute o pravima PRUS-a na žalbu ili ponovni postupak, ovisno o ishodu.

Donošenjem odluke postupak opoziva ulazi u završnu fazu, u kojoj se PRUS informira o ishodu i, ako je primjenjivo, poduzimaju odgovarajuće mjere za opoziv certifikata ili nastavak nadzora.

U slučaju opoziva certifikata, PRUS gubi pravo na prijavu za novu certifikaciju u razdoblju od jedne godine od datuma opoziva. Tijekom ovog razdoblja, PRUS ne smije obavljati revizijske aktivnosti niti podnositi zahtjev za ponovno certificiranje. Nakon isteka jednogodišnjeg roka, PRUS može podnijeti novi zahtjev za certifikaciju, uz uvjet da ispunjava sve propisane kriterije i dostavi dokaze o otklanjanju prethodnih nesukladnosti koje su dovele do opoziva certifikata.

4.3. Nadzor nad PRUS-om

Cilj ovog poglavlja je definirati postupke i obveze vezane uz nadzor nad certificiranim PRUS-ovima kako bi se osigurala kontinuirana usklađenost sa zahtjevima Pravila tijekom čitavog razdoblja valjanosti certifikata.

4.3.1. Redovni nadzor

Certificirana pravna osoba, odnosno PRUS obvezan je podvrgnuti se redovitim nadzorima tijekom razdoblja valjanosti certifikata. Ovi nadzori služe kako bi se osigurala usklađenost s postavljenim standardima te se posebno usmjeravaju na provjeru kvalitete provedenih revizija. U tom procesu se detaljno analizira jesu li sve revizije obavljene prema zadanim kriterijima kvalitete i stručnosti.

Tijekom nadzora također se provjerava zadržavanje svih kompetencija koje su bile ključne za dobivanje certifikata. Ovo uključuje ocjenu tehničkih, organizacijskih i stručnih kapaciteta kako bi se osiguralo da PRUS i dalje ispunjava sve propisane zahtjeve.

ZSIS utvrđuje termine za provedbu godišnjih nadzora te o istima obavještava PRUS najmanje 30 dana prije predviđenog početka redovnog nadzora. PRUS je dužan pravovremeno pripremiti i dostaviti svu traženu dokumentaciju s ciljem osiguravanja učinkovitog i nesmetanog provođenja nadzornog postupka. Redovni nadzor u pravilu se provodi dva puta unutar tri godine, prvi puta nakon 12 mjeseci od dana certificiranja i drugi puta nakon 24 mjeseca od dana certificiranja.

4.3.1.1. Provedbeni nadzor

Provedbeni nadzor je postupak u kojem ZSIS redovito provjerava usklađenost rada PRUS-a s uvjetima temeljem kojih je izdan certifikat. Ova vrsta nadzora provodi se kako bi se osiguralo kontinuirano pridržavanje standarda, očuvanje kvalitete rada i dosljedna primjena propisanih procedura tijekom cijelog razdoblja valjanosti certifikata.

Aktivnosti provedbenog nadzora se provode u sklopu redovnog nadzora, te je PRUS unaprijed obaviješten o datumu i opsegu nadzora, osim u iznimnim situacijama kada je zbog opravdanih razloga potrebno provesti nenajavljeni nadzor opisan pod točkom 4.3.2. Nenajavljeni nadzor. ZSIS analizira postupke certificiranog subjekta, uključujući način provođenja revizija, kako bi se utvrdilo ispunjavaju li svi aspekti njihova rada zahtjeve certifikata.

Tijekom nadzora također se provjerava jesu li sustavi i procesi PRUS-a i dalje u skladu s uvjetima koji su bili temelj za certifikaciju. Poseban naglasak stavlja se na zadržavanje profesionalnih i tehničkih sposobnosti, kao i na osiguranje povjerljivosti i sigurnosti podataka o revizijama, čime se štiti integritet certificiranog procesa. Stručni zahtjevi osoblja koje je PRUS zadovoljio kod izdavanja certifikata moraju biti očuvani u svakom trenutku, međutim, nije nužno da su nositelji stručnih zahtjeva kod nadzora isti zaposlenici kao i kod izdavanja certifikata. Nadzor se može provoditi nad aktualnom revizijom koju PRUS trenutačno realizira, ali može uključivati i retrospektivni pregled prethodno završenih revizija s ciljem osiguravanja dosljednosti u kvaliteti rada i potpune usklađenosti s certifikacijskim zahtjevima.

4.3.2. Nenajavljeni nadzor

Nenajavljeni nadzor provodi se u slučajevima kada ZSIS zaprimi pritužbu ili stekne osnovanu sumnju da PRUS ne postupa u skladu s propisanim pravilima i zahtjevima certifikata. Cilj nenajavljenog nadzora je brza i učinkovita provjera istinitosti navoda i sumnji, temeljem kojih je nenajavljeni nadzor pokrenut, te osiguravanje otklanjanja eventualnih nepravilnosti.

Fokus nenajavljenog nadzora usmjeren je isključivo na područja koja su predmet pritužbe ili sumnje. ZSIS analizira specifične aspekte rada certificiranog PRUS-a koji su identificirani kao potencijalno sporni, uključujući postupke, dokumentaciju i primjenu standarda. Ako je potrebno, nadzor može obuhvatiti i promatranje aktivnosti u realnom vremenu kako bi se utvrdila njihova usklađenost u skladu sa točkom 4.3.1.1. Provedbeni nadzor.

Nenajavljeni nadzor provodi se u svrhu osiguranja integriteta certificiranog procesa i povjerenja u sustav certifikacije. Certificirani PRUS dužan je omogućiti potpuni pristup informacijama i resursima koji su relevantni za nadzor, a sve u skladu s načelima transparentnosti i odgovornosti.

PRUS se nakon provedene nenajavljene provjere obavještava o nalazima i rezultatima nadzora, a u slučaju utvrđivanja neusklađenosti može se naložiti hitno poduzimanje korektivnih mjera.

4.3.3. Postupci praćenja sigurnosnih incidenata

PRUS je obavezan primijeniti odgovarajuće mjere sigurnosti kako bi se osigurala zaštita podataka o provedenim i tekućim revizijama, a sve u skladu s minimalnim zahtjevima koje propisuje Uredba za ključne subjekte. Informacijski sustavi na kojima se čuvaju i obrađuju ti podaci moraju biti usklađeni s ovim sigurnosnim standardima, čime se osigurava povjerljivost, integritet i dostupnost podataka.

PRUS je dužan bez odgode obavijestiti ZSIS u slučaju bilo kakve kompromitacije informacijskog sustava na kojem se čuvaju podaci o provedenim revizijama. Ovo uključuje obavijest o svakoj povredi podataka, mogućoj kompromitaciji dokumentacije koja se odnosi na proces revizije, kao i detalje o poduzetim radnjama za otklanjanje računalno-sigurnosnog incidenta. PRUS mora pružiti sve relevantne informacije o incidentu, uključujući prirodu povrede, opseg utjecaja i mjere koje su poduzete ili se planiraju poduzeti kako bi se osigurala sigurnost sustava i spriječile daljnje povrede.

ZSIS analizira prijavljene incidente i, ovisno o ozbiljnosti, može zahtijevati detaljno izvješće o provedenim radnjama za sanaciju. ZSIS može zahtijevati dodatnu provjeru i nadzor u slučaju da PRUS neadekvatno odgovara na incidente, kao i uvesti pojačane nadzorne mjere sve dok se ne dokaže puna usklađenost.

4.3.4. Korektivne mjere i praćenje njihove provedbe

Tijekom nadzora, ZSIS identificira sve nedostatke u sigurnosnim mjerama ili praksama PRUS-a te ih dokumentira u službenom izvješću. PRUS je dužan u zadanom roku provesti sve potrebne korektivne mjere kako bi se otklonili utvrđeni nedostaci iz odredbe 4.2.3. ovih Pravila. Rok za provedbu može ovisiti o vrsti i težini nesukladnosti.

ZSIS provodi dodatne provjere ili zahtijeva dokumentaciju kako bi se potvrdilo da su sve korektivne mjere ispunjene. U nekim slučajevima, može biti potrebna i naknadna revizija na licu mjesta.

4.4. Obnova certifikata

Obnova certifikata provodi se prema istim pravilima i postupcima kao i izdavanje novog certifikata, slijedeći standardni proces izdavanja certifikata opisan pod točkom 4.1. Postupak izdavanja certifikata.

PRUS je obvezan podnijeti zahtjev za obnovu certifikata najmanje šest mjeseci prije njegovog isteka kako bi se osiguralo pravovremeno provođenje postupka certificiranja i izbjegao prekid valjanosti certifikata. U slučaju kašnjenja s podnošenjem zahtjeva, PRUS preuzima odgovornost za mogućnost isteka certifikata prije završetka postupka obnove, što može rezultirati nemogućnošću obavljanja revizijskih aktivnosti do izdavanja novog certifikata.

5. Prava i obveze pružatelja upravljanih sigurnosnih usluga

U okviru postupka izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti nužno je definirati prava i obveze PRUS-ova kako bi se zajamčila transparentnost samog postupka izdavanja i opoziva certifikata te osigurala pravna sigurnost sudionika samog postupka. U tom smislu, u okviru ovog poglavlja propisuju se prava i obveze PRUS-ova, a koja nisu već ranije navedena u ovim Pravilima.

5.1. Pristup dokumentaciji i poslovnim prostorima PRUS-a u postupku certifikacije i nadzora

U tijeku postupka certifikacije i nadzora PRUS je dužan ZSIS-u staviti na raspolaganje cjelokupnu potrebnu vjerodostojnu dokumentaciju te omogućiti pristup informacijskim sustavima i pružiti sve druge potrebne informacije. PRUS je dužan ZSIS-u osigurati pristup i korištenje poslovnih prostorija u svrhu utvrđivanja ispunjava li PRUS sve propisane uvjete u pogledu organizacijskih i stručnih uvjeta te tehničko-sigurnosnih zahtjeva i staviti na raspolaganje odgovarajuću opremu i osoblje. ZSIS će pri tome voditi računa da postupak certificiranja provodi tako da ne ometa ili na najmanji mogući način ometa uobičajeni tijek rada PRUS-a.

U slučaju da PRUS ne postupa sukladno prethodno navedenoj obvezi ZSIS će obustaviti postupak certifikacije zbog nedostatka informacija i podataka potrebnih za donošenje odluke o certifikaciji. Opisano postupanje PRUS-a tijekom nazora će dovesti do suspenzije certifikata.

5.2. Prestanak važenja postojećih certifikata

5.2.1. Izmijenjeni uvjeti certificiranja

Certificirani PRUS-ovi obvezuju se uskladiti svoje sigurnosne prakse s novim standardima ili izmijenjenim uvjetima certificiranja koje certifikacijsko tijelo uvede. Certifikacijsko tijelo osigurava prijelazni period tijekom kojeg certificirane tvrtke mogu provesti potrebne promjene kako bi se uskladile s novim uvjetima. Prijelazni period ZSIS objavljuje prilikom objave novih uvjeta certificiranja, a u ovisnosti o izmjenama.

Certifikacijsko tijelo pravodobno obavještava sve PRUS-eve o izmjenama i pruža smjernice za usklađivanje sa svim novim zahtjevima ili preporukama. U prijelaznom razdoblju izdani certifikati i dalje su aktivni, te unutar 10 radnih dana od obavijesti PRUS mora dostaviti dokaz da je započeo s

procesom implementacije potrebnih promjena. U slučaju da PRUS ne dostavi dokaz certifikat se stavlja u status suspenzije, sve do dostavljenih dokaza o početku procesa implementacije. Unutar roka prijelaznog perioda PRUS mora dostaviti potvrdu o potpunoj usklađenosti sa izmijenjenim uvjetima, a u suprotnom njegov se certifikat stavlja u status suspenzije.

Nakon isteka roka prijelaznog perioda, certifikacijsko tijelo može pokrenuti redovni nadzor nad PRUS-om kako bi potvrdio usklađenost s novim uvjetima.

5.2.2. Gubitak sposobnosti za provođenje revizija kibernetičke sigurnosti

PRUS je obvezan bez odgode obavijestiti ZSIS u slučaju gubitka sposobnosti provođenja revizija zbog nedostatka resursa, stručnog osoblja ili drugih okolnosti koje utječu na njegovu usklađenost s uvjetima certificiranja. U takvom slučaju, certifikat PRUS-a stavlja se u status suspenzije do ponovne usklađenosti, pri čemu PRUS mora dostaviti plan i rokove za otklanjanje nesukladnosti. Razdoblje suspenzije ne može biti dulje od jedne godine, niti može prijeći rok važenja samog certifikata. Ako PRUS ne uspostavi punu usklađenost unutar predviđenog roka, certifikat se opoziva.

U slučaju da PRUS ne obavijesti ZSIS o gubitku sposobnosti provođenja revizija, a ZSIS samostalno utvrdi nesukladnost kroz nadzor ili druge mehanizme provjere, ZSIS pokreće postupak za opoziv certifikata. Tijekom tog postupka, PRUS ima mogućnost očitovanja i dostave dokaza o usklađenosti unutar roka koji odredi ZSIS. Ako PRUS ne dokaže svoju sposobnost unutar zadanog roka, certifikat se opoziva.

5.3. Pravo PRUS-a na zaštitu podataka

PRUS ima pravo na zaštitu poslovnih podataka označenih poslovnom tajnom, koje u tijeku postupka certificiranja ili provedbe nadzora stavlja na raspolaganje ZSIS-u, sukladno s nacionalnim i europskim zakonskim propisima koji uređuju područje zaštite podataka.

Tijekom postupka certifikacije PRUS je dužan staviti na raspolaganje interne dokumente kao i omogućiti pristup informacijskim sustavima u svrhu dokazivanja ispunjenja propisanih uvjeta za izdavanje certifikata. Kako bi se podaci zaštitili, ZSIS je dužan postupati s dobivenim podacima s dužnom pažnjom poštujući pri tome propise koji uređuju područje zaštite podataka.

5.4. Pravo na nepristranost, neovisnost i informiranost

Po zahtjevu PRUS-a za izdavanje certifikata, postupak provode i odluke donose o PRUS-u neovisne i nepristrane službene osobe ZSIS-a vodeći računa u svakoj fazi postupka na mogući sukob interesa. U slučaju sumnje na mogući sukob interesa, neovisno bio on osobne ili poslovne prirode, a koji bi mogao utjecati na objektivno i nepristrano odlučivanje, službena osoba ZSIS-a koja sudjeluje u postupku certifikacije ili nadzora će se izuzeti iz postupka čim sazna za mogući sukob interesa.

Tijekom postupka PRUS ima pravo dobiti informacije o tijeku i trenutnoj fazi postupka certifikacije.

6. Prijelazne i završne odredbe

Ovo poglavlje opisuje uvjete i postupke prijelaza na nove verzije standarda, pravila i procedura certificiranja te sadrži dodatne zakonske odredbe važne za tumačenje i primjenu ovog dokumenta. Ove odredbe osiguravaju kontinuitet i jasnoću u slučaju izmjena te završne upute za sve uključene strane.

6.1. Izmjene i dopune pravila certificiranja

Sve izmjene i dopune Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti objavljuju se na mrežnim stranicama ZSIS-a i dostavljaju PRUS-ovima putem službenih kanala.

6.2. Tumačenje pravila certificiranja

U slučaju nejasnoća ili različitih interpretacija, odredbe ovog dokumenta tumače se u korist održavanja visokih standarda kibernetičke sigurnosti i osiguravanja nepristranosti u certifikacijskim postupcima.

ZSIS ima pravo na tumačenje pravila certificiranja te pružanja službenog obrazloženja, mišljenja i uputa svim PRUS-ovima koji zatraže pojašnjenje.

U slučaju sukoba između ovih pravila i specifičnih uvjeta pojedinih standarda, primjenjuju se pravila ili standardi koje ZSIS propisuje.

6.3. Primjena i revizija dokumenta

Ovaj dokument se primjenjuje do donošenja odgovarajuće europske sheme kibernetičke sigurnosne certifikacije koja obuhvaća revizije kibernetičke sigurnosti, uz obvezu ZSIS-a na periodične revizije kako bi se osigurala usklađenost s zakonodavnim promjenama, tehnološkim inovacijama i sigurnosnim standardima.

ZSIS provodi redovitu reviziju dokumenta te u slučaju potrebnih izmjena, izrađuje ažuriranu verziju pravila certificiranja. Svi PRUS-ovi se pravodobno obavještavaju o reviziji dokumenta i ključnim promjenama koje bi mogle utjecati na njihovu usklađenost.

6.4. Završne napomene

Sve službene obavijesti u vezi s tumačenjima Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti dostavljaju se PRUS-ovima putem elektroničke pošte i objavljuju na mrežnoj stranici ZSIS-a.

6.5. Stupanje na snagu

Ova Pravila stupaju na snagu danom donošenja i objavljuju se na mrežnim stranicama Zavoda za sigurnost informacijskih sustava.

7. Popis priloga

Oznaka	Naziv priloga
Prilog A	Obrazac za prijavu certifikacije
Prilog B	Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima
Prilog C	Katalog kontrola
Prilog D	Izjava o utvrđenom stupnju usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima

KLASA: 005-13/25-02/01
URBROJ: 509-30-02/41-25-27
U Zagrebu, 21. kolovoza 2025.

REPUBLIKA HRVATSKA – ZAVOD ZA SIGURNOST INFORMACIJA – ZAGREB

RAVNATELJ
Predrag Božinović
Predrag Božinović