RIZICI KORIŠTENJA UMJETNE INTELIGENCIJE U RADU DRŽAVNOG UREDA ZA REVIZIJU

1. Ljudska autonomija i nadzor

Rizik 1: Pretjerano povjerenje u UI sustave

Opis rizika: UI sustavi mogu biti pristrani jer algoritmi mogu odražavati pristranosti skupova podataka na kojima su trenirani, što može dovesti do pogrešnih revizijskih zaključaka i narušavanja načela objektivnosti i pouzdanosti informacija te narušavanja etičkih načela.

Posljedice u reviziji:

- pogrešni revizijski zaključci
- pasivno prihvaćanje pogrešnih nalaza
- smanjena kvaliteta revizijskog rada
- narušavanje revizijskih načela (objektivnost, pouzdanost)
- narušavanje ugleda Ureda u javnosti
- gubitak profesionalnog skepticizma
- regulatorna neusklađenost
- izostanak kritičkog razmišljanja kod donošenja zaključaka

Mjere za smanjenje rizika:

- naglašavanje da UI sustav nikada ne preuzima odgovornost
- obvezan ljudski nadzor i profesionalne prosudbe revizora
- edukacija o ograničenjima i pogreškama UI sustava
- poticanje kritičkog osporavanja rezultata UI sustava
- kontrola kvalitete podataka koji se koriste za treniranje UI sustava
- korištenje samo službenih i provjerenih podataka
- testiranje točnosti i pouzdanosti UI sustava
- detektiranje eventualnih anomalija

Rizik 2: Potvrđujuća pristranost

Opis rizika: Revizor koristi UI sustav kako bi potvrdio već formirano mišljenje, a zanemaruje suprotne nalaze, što može dovesti do nepotpunih ili netočnih zaključaka, smanjivanja objektivnosti revizijskih postupaka i donošenja pogrešnih odluka.

Posljedice u reviziji:

- povreda profesionalnog skepticizma
- povreda etičkih načela neovisnosti i objektivnosti
- pogrešno tumačenje dokaza
- propusti u otkrivanju nepravilnosti
- neotkrivanje propusta i nepravilnosti
- pogrešna procjena rizika zbog nedovoljnog testiranja rizičnih područja
- neadekvatni dokazi (biraju se uzorci koji podržavaju očekivane rezultate ili zanemarivanje kontradiktornih informacija)

- loša kvaliteta izvješća

Mjere za smanjenje rizika:

- obveza razmatranja alternativnih objašnjenja
- timska rasprava o rezultatima koji su dobiveni putem UI sustava
- dokumentiranje razloga prihvaćanja ili odbacivanja nalaza generiranih putem UI sustava
- edukacija revizora o prepoznavanju vlastitih kognitivnih pristranosti i pravilnijoj upotrebi UI sustava
- česte rotacije članova revizijskih timova

Rizik 3: Smanjenje profesionalne pažnje

Opis rizika:
UI sustav može dovesti do smanjene razine kognitivne uključenosti, gdje se revizor manje angažira u analizi zbog prekomjernog povjerenja i oslanjanja na UI sustave.

Posljedice u reviziji:

- izražavanje neodgovarajućeg revizijskog mišljenja
- neotkrivanje pogrešaka ili eventualnih prijevara
- nedostatna dubina revizijskih postupaka
- formalno, ali ne i suštinsko provođenje procedura i revizijskih postupaka
- nedovoljno dokumentirana profesionalna prosudba
- smanjena sposobnost samostalnog stručnog prosuđivanja
- slabljenje analitičnih kompetencija revizora
- smanjeno kritičko razmišljanje revizora
- prekomjerno povjerenje u UI sustave

Mjere za smanjenje rizika:

- jasno definiranje da je odgovornost uvijek na revizoru
- periodične interne provjere učinkovitosti i pouzdanosti UI sustava
- dokumentiranje vlastitih analiza i zaključaka revizora unatoč korištenju UI sustava
- edukacija revizora za kritičko vrednovanje rezultata dobivenih od UI sustava
- provođenje rasprave među članovima revizijskih timova o rezultatima dobivenim korištenjem UI sustava

2. Tehnička robusnost i sigurnost

Rizik 1: Netočni, nepotpuni ili uvjerljivo pogrešni rezultati (halucinacije)

Opis rizika: UI sustav može generirati netočne podatke, pogrešne interpretacije ili izmišljene reference, pri čemu rezultat djeluje uvjerljivo i stručno.

Posljedice u reviziji:

- pogrešni revizijski nalazi
- netočne procjene rizika
- pogrešni zaključci revizora
- pogrešno usmjeravanje revizijskih postupaka

- pogrešne reference/upute na zakone ili standarde

Mjere za smanjenje rizika:
- obvezna verifikacija svih rezultata dobivenih UI sustavima od strane revizora
- zabrana korištenja rezultata dobivenih putem UI sustava kao samostalnog revizijskog dokaza
- provjera podataka, zaključaka i informacija s izvornim dokumentima ili iz različitih izvora te drugim analitičkim metodama
- jasno dokumentiranje da je UI sustav korišten kao pomoćni alat

Rizik 2: Nepouzdanost i pogreške sustava

Opis rizika: UI sustav može davati nekonzistentne ili pogrešne rezultate.

Posljedice u reviziji:
- netočni ili nepotpuni revizijski nalazi, što može dovesti do pogrešnih zaključaka
- pogrešne procjene rizika
- donošenje netočnih zaključaka temeljenih na nepouzdanim podacima

Mjere za smanjenje rizika:
- redovito testiranje i validacija modela
- *fail-safe* i *fallback* mehanizmi (rezervna rješenja)
- edukacija revizora o ograničenjima sustava
- dokumentiranje uporabe UI sustava

Rizik 3: Sigurnosni napadi / Neuspjeh sustava

Opis rizika: UI sustav može biti kompromitiran (hakiran), zloupotrebljen ili može zakazati zbog tehničkih pogrešaka, nedostataka ili neadekvatnog održavanja.

Posljedice u reviziji:
- gubitak pouzdanosti sustava
- povreda povjerljivosti podataka
- operativni prekid rada UI sustava
- curenje povjerljivih podataka

Mjere za smanjenje rizika:
- sigurnosni protokoli i zaštita od kibernetičkih napada
- redovita kontrola sustava i planiranje sigurnosnih mjera
- edukacija revizora o kibernetičkoj sigurnosti i načinu rada UI sustava

3. Privatnost i upravljanje podacima

Rizik 1: Povreda povjerljivosti i zaštita podataka

Opis rizika: Unošenje povjerljivih ili osobnih podataka u neodobrene ili vanjske UI sustave.

Posljedice u reviziji:

- gubitak kontrole nad podacima
- unošenje identifikacijskih podataka bez prethodnog uklanjanja osobnih oznaka
- prijenos podataka trećim stranama bez odobrenja
- neovlašten pristup podacima (kibernetički napad)
- neovlašteno otkrivanje podataka putem generiranih odgovora
- sudski sporovi i tužbe za naknadu štete
- povreda privatnosti zaposlenika ili osoba zaposlenih u subjektima revizije
- smanjeno povjerenje u rad revizora

Mjere za smanjenje rizika:

- stroga zabrana korištenja neodobrenih UI sustava
- korištenje UI sustava isključivo u sigurnim, internim okruženjima
- edukacija o zaštiti podataka
- tehničke kontrole (ograničenja pristupa, logiranje/prijave u sustav)
- implementacija enkripcije i sigurnosnih protokola za prijenos i pohranu podataka
- zabrana unošenja podataka iz revizijske dokumentacije u neodobrene UI sustave

Rizik 2: Zastarjelost ili neadekvatnost podataka

Opis rizika: UI sustavi mogu raditi na zastarjelim, nepotpunim ili kontekstualno neprimjerenim podacima, što može dovesti do davanja nepreciznih ili pogrešnih preporuka i procjena. Ako se UI sustavi oslanjaju na neaktualne informacije, njihove odluke mogu biti neusklađene s važećim propisima i trenutnim okolnostima.

Posljedice u reviziji:

- korištenje zastarjelih/neažuriranih podataka može dovesti do pogrešnih zaključaka te naknadnog ispravljanja izvješća
- gubitak povjerenja javnosti
- negativni medijski pritisak
- narušavanje ugleda Ureda
- neusklađenost s važećim i aktualnim propisima

Mjere za smanjenje rizika:

- jasno definiranje izvora i vremenskog obuhvata podataka
- uspostava procesa redovitog ažuriranja podataka i modela UI sustava
- praćenje promjena u regulatornom i zakonskom okviru
- korištenje samo službenih i provjerenih izvora podataka
- edukacija zaposlenika o pravilnom korištenju UI sustava
- obvezna provjera aktualnosti informacija
- ograničavanje uporabe UI sustava na pomoćne analitičke funkcije odnosno kao podrška zaposlenicima kod donošenja odluka ili zaključaka

4. Transparentnost

Rizik 1: Nedostatak objašnjivosti/efekt *„Black box“*

Opis rizika: Nemogućnost razumijevanja načina donošenja odluka od strane UI sustava. Kod složenih modela nije jasno na temelju kojih podataka i veza je UI sustav došao do određenog zaključka.

Posljedice u reviziji:

- nemogućnost objašnjenja revizijskih nalaza
- nemogućnost provjere ispravnosti odluke
- slabljenje revizijskog traga
- sigurnosni rizici (podložnost manipulaciji)
- otežana obrana nalaza pred Hrvatskim saborom ili javnošću
- nemogućnost utvrđivanja odgovornosti u slučaju pogreške
- ovisnost o tehnologijama bez razumijevanja ili koje se ne razumiju

Mjere za smanjenje rizika:

- korištenje alata s većom razinom transparentnosti i objašnjivosti
- dokumentiranje ulaznih podataka, pretpostavki i ograničenja UI sustava
- nekorištenje UI sustava za ključne zaključke bez jasnog obrazloženja
- provjeravanje i obrazlaganje rezultate UI sustava vlastitim profesionalnim prosudbama
- korištenje UI sustava koji do zaključaka dolazi samo na temelju učitane dokumentacije
- korištenje UI sustava koji omogućuju uvid u logiku donošenja zaključaka

5. Raznolikost, nediskriminacija i pravednost

Rizik 1: Algoritamska pristranost

Opis rizika: UI modeli uče na podacima koji mogu sadržavati strukturne, institucionalne ili društvene pristranosti.

Posljedice u reviziji:

- selektivno označavanje/odabir subjekata
- reprodukcija postojećih pogrešnih obrazaca
- ugrožavanje objektivnosti i nepristranosti u postupcima revizije
- favoriziranje određenih skupina, regija ili sektora

Mjere za smanjenje rizika:

- korištenje UI sustava isključivo kao jednog od više analitičkih alata
- redovita evaluacija rezultata UI sustava s aspekta pristranosti
- ljudska korekcija i profesionalna prosudba u tumačenju rezultata
- zabrana automatiziranog rangiranja subjekata bez dodatne analize
- revizor zadržava konačnu odgovornost za odluke i zaključke
- periodička provjera učinkovitosti i neutralnosti algoritama
- redovito brisanje podataka koji bi mogli uzrokovati nastanak pristranosti

6. Odgovornost

Rizik 1: Erozija odgovornosti

Opis rizika: Nije jasno tko odgovara za pogreške ili štetu koju prouzroči UI sustav.

Posljedice u reviziji:

- nedostatak odgovornosti
- nejasno definirane uloge i odgovornosti među zaposlenicima i nadređenima mogu uzrokovati nesigurnost u postupanju i smanjenju učinkovitosti rada Ureda
- narušavanje povjerenje javnosti u rad Ureda

Mjere za smanjenje rizika:

- jasno definiranje odgovornosti revizora
- revizijski trag i revizija korištenja UI sustava
- transparentna komunikacija o korištenju UI sustava

Rizik 2: Ugrožavanje neovisnosti rada Ureda

Opis rizika: Ovisnost o komercijalnim UI sustavima čiji interesi, modeli ili podaci nisu pod kontrolom Ureda, što može ugroziti revizijsku samostalnost i povećati rizik od manipulacije rezultatima.

Posljedice u reviziji:

- narušena objektivnost i pouzdanost revizijskih nalaza
- povreda povjerljivih podataka prikupljenih u radu revizora
- donošenje pogrešnih ili neosnovanih zaključaka
- slabija kvaliteta revizijskog nadzora
- moguće kršenje propisa o zaštiti podataka i UI regulative
- smanjena stručna autonomija revizora
- utjecaj vanjskih inženjera za razvoj softvera UI sustava na procese odlučivanja

Mjere za smanjenje rizika:

- institucionalno odobravanje UI sustava
- procjena utjecaja pružatelja tehnologije UI sustava
- dokumentiranje odluka o odabiru UI sustava i razloga zašto je određeni alat prihvaćen ili odobren
- donošenje smjernica za korištenje UI sustava
- redovito provođenje procjene utjecaja UI sustava na neovisnost i etiku
- edukacija zaposlenika o ograničenjima i rizicima UI sustava
- zadržati ljudsku profesionalnu prosudbu kao konačni korak u odlučivanju
- sprječavanje vanjskog utjecaja na UI sustave

Rizik 3: Reputacijski i pravni rizik

Opis rizika: Pogrešna ili netransparentna uporaba UI sustava može narušiti povjerenje javnosti te dovesti do sumnji u profesionalnost i integritet revizorskog rada.

Posljedice u reviziji:

- autorsko pravne tužbe zbog neovlaštene uporabe ili reprodukcije zaštićenog sadržaja (materijala zaštićenih autorskim pravima)
- povreda propisa o zaštiti osobnih podataka
- pogrešna ili netransparentna uporaba UI sustava može se smatrati kršenjem profesionalnih standarda revizorske struke
- nepravilna uporaba UI sustava može dovesti do otkrivanja povjerljivih ili osobnih podataka
- gubitak povjerenja javnosti u rad revizora

Mjere za smanjenje rizika:

- transparentno navođenje korištenja UI sustava u internim postupcima
- zabrana „skrivene“ uporabe UI sustava
- jasna komunikacija da UI sustavi ne zamjenjuje rad revizora
- edukacija revizora o etičkim i profesionalnim standardima korištenja UI sustava
- uspostava mehanizama nadzora i kontrole kako bi se osigurala odgovornost
- dosljednost u primjeni UI sustava

Rizik 4: Normativni i regulatorni rizik

Opis rizika: Neusklađenost s važećim zakonima, etičkim kodeksom ili međunarodnim standardima zbog promjena u propisima, pogrešne interpretacije ili nedovoljne integracije regulatornih pravila u poslovne procese.

Posljedice u reviziji:

- pogrešni revizijski zaključci zbog oslanjanja na UI sustave
- pogrešna procjena rizika
- povreda autorskih i intelektualnih prava kroz korištenje UI sustava
- povreda propisa o zaštiti osobnih podataka
- neusklađenost s regulativom i standardima struke
- postojanje sumnje u izražavanje mišljenja o obavljenoj reviziji
- ugrožavanje ugleda Ureda i kršenja profesionalnih standarda revizije

Mjere za smanjenje rizika:

- redovito ažuriranje procedura i internih akata
- praćenje pravne regulative
- osiguravanje da svi novi UI sustavi prolaze formalni proces odobrenja koji uključuje pravnu i etičku evaluaciju i provjeru
- provođenje edukacija revizora

7. Društvena i okolišna dobrobit

Rizik 1: Dezinformacije i manipulacija

Opis rizika: UI sustav može širiti netočne, nepotpune i štetne informacije.

Posljedice u reviziji:

- negativni utjecaji na društvo

- dezinformiranje javnosti
- smanjenje povjerenja u rad Ureda

Mjere za smanjenje rizika:

- procjena društvenog utjecaja
- edukacija zaposlenika i javnosti
- ograničavanje primjene UI sustava u osjetljivim područjima