Foreign Investors Council

Komentari Saveta stranih investitora na Nacrt pravilnika o opštoj metodologiji za procenu rizika u informaciono-komunikacionim sistemima od posebnog značaja

29. maj 2026. godine

I. Opšti komentari i sugestije

Predlog: Imajući u vidu član 11, stav 4., član 54. stav 1 i član 55. stav 4. Zakona o informacionoj bezbednosti, predlažemo da dokument ne bude podzakonski akt, već smernice o opštoj metodologiji za procenu rizika u informaciono-komunikacionim sistemima od posebnog značaja.

Obrazloženje:

Odredbom člana 11. stav 4. Zakona o informacionoj bezbednosti ("Službeni glasnik RS", broj 91/25, u daljem tekstu: ZIB), propisano je da se akt o proceni rizika izrađuje u skladu sa opštom metodologijom za procenu rizika u prioritetnim i važnim IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a. Odredbom člana 54. stav 1 ZIB propisuje obavezu donošenja podzakonskih akata u roku od 12 meseci od donošenja ZIB, dok je odredbom člana 55. stav 4. definisana obaveza Nacionalnog CERT-a da u roku od devet meseci od dana stupanja na snagu ZIB, donese opštu metodologiju za procenu rizika u IKT sistemima od posebnog značaja.

Ukazujemo da ne postoji ovlašćujuća odredba za donošenje pravilnika, odnosno da ZIB-om nije izričito dato ovlašćenje Regulatornom telu za elektronske komunikacije i poštanske usluge, kao organizaciji u kojoj se obavljaju poslovi Nacionalnog CERT-a, da ovu materiju uredi podzakonskim aktom.

Pravilnik kao podzakonski akt ima obavezujući normativni karakter i može se donositi samo kada postoji jasan i izričit zakonski osnov, dok smernice služe za stručno usmeravanje, pojašnjenje i ujednačenu primenu zakona bez stvaranja novih obaveznih pravila. U prilog prethodno navedenom, i sam nacrt akta koristi izraze "preporučuje se" više puta.

U tom smislu, smatramo da su smernice pogodniji instrument jer omogućavaju fleksibilnost, praktičnu primenu i brže prilagođavanje tehničkim i organizacionim promenama u oblasti informacione bezbednosti. Time se istovremeno čuva pravna sigurnost, izbegava prekoračenje zakonskog ovlašćenja i obezbeđuje dosledna primena zakona u praksi.

Ukoliko bi predmetna materija bila uređena pravilnikom, to bi moglo dovesti do toga da nadzor nad svim IKT sistemima zahteva primenu ove metodologije u punom obimu, odnosno izradu analize rizika za sve elemente i na isti način kako je to predviđeno metodologijom, što bi u praksi bilo teško ostvarivo. U nacrtu pravilnika je izabrana metoda procene rizika zasnovane na sistemima, dok nisu opisane, odnosno predviđene metode procene rizika zasnovane na procesima i zasnovane na scenarijima. Smatramo da metode koje nisu obrađene u nacrtu pravilnika ne treba isključiti, jer će u određenim slučajevima biti prigodnije za izradu akta o proceni rizika.

I. Pojedinačni članovi

1. Predlog

Relevantni član: **Prilog 1 Tabela 1.**

Predlog izmene: U tabeli 1: *Registar resursa*, smatramo da je potrebno dodati kolonu „Značaj/Kritičnost“ i uskladiti sa tačkom 5.2. Registra resursa, gde je navedeno: „*Registar resursa sa najmanje sledećim podacima: naziv, kategorija, vlasnik i procena vrednosti po CIA triadi*“.

Obrazloženje (opis problema): Potrebno je adekvatno vrednovanje imovine u pogledu značaja/kritičnosti, te predlažemo unošenje predloženog gde bi se upisivao nivo kritičnosti: kritično, visoko, srednje, nisko i sl.

---

2. Predlog

Relevantni član: **Prilog 1 Tačka 2. Korišćeni pojmovi**

Predlog izmene: Predlažemo da u tački 2. definicija incidenta glasi:

„Svaki događaj ili skup događaja koji ugrožava ili može da ugrozi raspoloživost, integritet, i/ili poverljivost podataka koji se čuvaju prenose ili obrađuju ili usluge koje se pružaju, odnosno koje su dostupne putem IKT sistema.“

Obrazloženje (opis problema): U tački 5.4. se navodi da kriterijum za procenu uticaja mora uključivati posledice po poverljivost, integritet i raspoloživost (isto važi za tačku 5.2. Registar resursa sa najmanje sledećim podacima: naziv, kategorija, vlasnik i procena vrednosti po CIA triadi.) dok se u tački 2. pominje da incident pored ova tri ključna parametra obuhvata još i autentičnost i neporecivost.

Potrebno je uskladiti ova dva aspekta kako bi bili usklađeni i kako ne bi dolazilo do dvojakog tumačenja, te je predlog da se iz definicije za incident izbace pojmovi autentičnost i neporecivost.

---

3. Predlog

Relevantni član: **Prilog 1 Tačka 3. Tim/Radna grupa za sprovođenje procene rizika**

Predlog izmene: Uvesti obavezu formalnog imenovanja vlasnika metodologije procene rizika i funkcije odgovorne za nezavisnu proveru kvaliteta procene.

Obrazloženje (opis problema): Trenutno je predviđeno formiranje tima, ali nije jasno razdvojena operativna implementacija i kontrolna funkcija. U velikim IKT sistemima ovakva separacija je ključna za izbegavanje konflikta interesa i za regulatornu usklađenost.

---

4. Predlog

Relevantni član: **Prilog 1 Tačka 4.1. Definisanje opsega (konteksta) za analizu rizika**

Predlog izmene: Dodati obavezu eksplicitnog definisanja kritičnih poslovnih funkcija (critical business services) i mapiranja na IKT sisteme.

Obrazloženje: Trenutni fokus je na sistemima i resursima, ali bez formalnog povezivanja sa poslovnim funkcijama, postoji rizik da procena ne odražava stvarni poslovni impact (impact na business).

---

5. Predlog

Relevantni član: **Prilog 1 Tačka 4.1.1. Opis sistema**

Predlog izmene: Izbaciti član.

Obrazloženje (opis problema): Opisi sistema i procesa po pravilu predstavljaju deo procesne dokumentacije kompanije, a ne same analize rizika. Analiza rizika može da se pozove na postojeću dokumentaciju te vrste, ali smatramo da njen cilj ne bi trebalo da bude izrada takvih dokumenata u slučajevima kada oni već postoje. Smatramo da navedeni deo nije u direktnoj funkciji procene rizika, dok bi izrada detaljnih opisa sistema, uključenih komponenti i ograničenja u okviru kojih se procena sprovodi mogla predstavljati značajan administrativni posao, bez garancije dovoljnog nivoa tačnosti i ažurnosti podataka.

---

6. Predlog

Relevantni član: **Prilog 1 Tačka 4.1.2. Opis informacionih sistema**

Predlog izmene: Izbaciti član

Obrazloženje (opis problema): Informacije o pojedinačnim sistemima, njihovoj arhitekturi i sličnim elementima vode se u dokumentaciji odvojenoj od analize rizika. Analiza rizika može da se pozove na ta dokumenta prilikom definisanja opsega, ali njen cilj nije da ih izrađuje ako već ne postoje. Njena eventualna preporuka može biti da se takva dokumentacija uspostavi kao mera za ublažavanje identifikovanog rizika, ali nije neophodno da nastaje pre svake analize rizika. Takođe smatramo da za potrebe Akta o proceni rizika može biti dovoljno navesti sisteme, njihove vlasnike i nivo kritičnosti, dok bi detaljni opisi informacionih sistema trebalo da postoje nezavisno od samog procesa procene rizika.

---

7. Predlog

Relevantni član: **Prilog 1 Tačka 4.3. Identifikacija pretnji**

Predlog izmene: Uvesti obavezu dokumentovanja izvora pretnji (threat intelligence), uključujući interne i eksterne izvore (CERT, ISAC, vendor advisories).

Obrazloženje: Metodologija predviđa katalog pretnji, ali ne zahteva korišćenje aktuelnih podataka o pretnjama. Smatramo da bi za velike operatore statički katalog pretnji mogao biti nedovoljan za adekvatnu procenu rizika, zbog čega bi bilo korisno dodatno urediti pitanje dokumentovanja i korišćenja izvora informacija o pretnjama.

---

8. Predlog

Relevantni član: **Prilog 1 Tačka 4.4. Analiza rizika – rangiranje i vrednovanje**

Predlog izmene: Predlažemo da se termin „verovatnoća događanja“ zameni terminom „verovatnoća materijalizacije rizika“ ili „verovatnoća ostvarenja rizika“, zato što smatramo da su ovi izrazi precizniji i stručno pravilniji u kontekstu upravljanja rizicima.

Obrazloženje (opis problema): Smatramo da je termin „verovatnoća događanja“ je previše opšti i može se odnositi na bilo koji događaj, dok u analizi rizika nije svako događanje relevantno, već samo ono koje vodi ka nastanku štetne posledice. Nasuprot tome, stava smo da „verovatnoća materijalizacije rizika“ jasnije ukazuje na mogućnost da se identifikovana pretnja ili neželjeni scenario stvarno ostvari, što preciznije odražava suštinu procene rizika.

Takođe, termin „verovatnoća ostvarenja rizika“ usklađen je sa uobičajenom terminologijom koja se koristi u oblasti informacione bezbednosti, upravljanja rizicima i kontrole poslovnih procesa. Na taj način se obezbeđuje veća terminološka doslednost, jasnije tumačenje propisa i preciznija primena u praksi.

---

9. Predlog

Relevantni član: **Prilog 1 Tačka 4.4.4. Određivanje prihvatljivog rizika**

Predlog izmene: Predlažemo izmenu naziva tačke 4.4.4. „Određivanje prihvatljivog rizika“ tako da glasi: „Određivanje prihvatljivog nivoa rizika“.

Obrazloženje (opis problema): Smatramo da bi termin „prihvatljiv nivo rizika“ bio precizniji, imajući u vidu da se u praksi ne prihvata sam rizik kao takav, već određeni nivo rizika koji se smatra prihvatljivim.

---

10. Predlog

Relevantni član: **Prilog 1 Tačka 4.4.5. Izrada registra rizika, Tabela 7: *Registar rizika***

Predlog izmene: Predlaže se dopuna Tabele 7 dodatnim poljima za opis scenarija rizika, inherentni i preostali rizik, vlasnika rizika i status implementacije mere

Obrazloženje (opis problema): Iako tabela sadrži pretnju i resurs, ne predviđa polje za opis rizika. U praksi, samo navođenje resursa i generičke pretnje često nije dovoljno za razumevanje konteksta rizika, pa je potrebno uključiti opis scenarija rizika u registru rizika. Radi potpunijeg razumevanja i efikasnijeg upravljanja, predlaže se i proširenje tabele kolonama za inherentni i preostali rizik, vlasnika rizika na poslovnom nivou (ne samo IT) i status implementacije mere. Razdvajanje inherentnog i preostalog rizika u različite dokumente otežava upravljanje, dok je integrisani prikaz standard u upravljanju rizicima.

---

11. Predlog

Relevantni član: **Prilog 1 Tačka 4.5. Postupanje sa rizikom**

Predlog izmene: Uvesti obavezu formalnog odobravanja prihvatanja rizika na adekvatnom nivou upravljanja (npr. executive/board za visoke rizike).

Obrazloženje: Metodologija prepoznaje vlasnika rizika, ali ne razdvaja nivoe odlučivanja. Za visoke i veoma visoke rizik, smatramo da je potrebno odlučivanje na višem upravljačkom nivou zbog poslovnih implikacija.

---

12. Predlog

Relevantni član: **Prilog 1 Tačka 4.5.5. Komuniciranje rizika**

Predlog izmene: U tački 4.5.5. navodi se da operator IKT sistema od posebnog značaja treba da utvrdi vremenski okvir za donošenje odluke o načinu postupanja sa rizikom u odnosu na nivo ozbiljnosti *(Tabela 9).* Smatramo da je potrebno redefinisati tako da se vremenski okvir odnosi na rok za primenu mere, a ne na rok za donošenje odluke. Dodatno, predlažemo da se nivo rizika ne vezuje automatski za rok realizacije mera na način kako je trenutno navedeno, već da za svaki identifikovani rizik postoji posebna odluka o načinu njegovog adresiranja, u okviru koje će biti definisan primeren rok za sprovođenje mera.

Obrazloženje (opis problema): Smatramo da bi bilo primerenije da se definišu rokovi za implementaciju mera i ublažavanje/mitigaciju rizika, a ne rokovi za donošenje odluke o načinu postupanja sa rizikom, što je u skladu sa svetskom praksom upravljanja rizicima. U suprotnom, može doći do situacije da značajan deo vremena bude utrošen na samo donošenje odluke, bez blagovremene realizacije mera. Takođe, crveni nivo rizika ne mora nužno da povlači automatsko ili hitno tretiranje rizika, jer su obim štete, verovatnoća ostvarivanja i posledice specifične za svaki pojedinačni slučaj. Upravljanje rizicima zahteva procenat prihvatljivog nivoa rizika, kapacitete organa i dostupne resurse, pa je opravdano da se rok za realizaciju mera ne određuje apriorno na osnovu samo nivoa rizika, već u okviru

konkretnog odlučivanja o načinu adresiranja rizika. Time se osigurava racionalna i proporcionalna raspodela sredstava i pravovremeno, ali ne nužno hitno, rešavanje svakog rizika.

---

13. Predlog

Relevantni član: **Prilog 1 Tačka 4.6. Praćenje rizika**

Predlog izmene: U tački 4.6 navodi se da se preispitivanje rizika sprovodi jednom godišnje. Predlažemo da se razmotri smanjenje perioda na kvartalno ili polugodišnje.

Obrazloženje (opis problema): Smatramo da je preispitivanje rizika jednom godišnje veoma dug period, naročito uzimajući u obzir značaj i važnost IKT sistema od posebnog značaja.

---

14. Predlog

Relevantni član: **Prilog 1 Tačka 5.3. Identifikacija pretnji**

Predlog izmene: Predlaže se dopuna tačke na sledeći način (označeno crvenom):

Dokumentovana identifikacija pretnji relevantnih za resurse u opsegu procene, sa naznakom izvora pretnje i ciljanog resursa. Operator IKT sistema od posebnog značaja može koristiti sopstveni katalog pretnji ukoliko pokriva iste osnovne kategorije pretnji kao Katalog pretnji iz ove metodologije. Evidencija relevantnih pretnji koje su procenjene da imaju uticaj na resurs može se voditi i u okviru finalnog registra rizika.

Obrazloženje (opis problema): Evidentiranje veze resurs–pretnja na dva odvojena mesta (lista pretnji i registar rizika) može dovesti do nepotrebnog dupliranja dokumentacije i usporavanja aktivnosti. Relevantne pretnje će svakako biti obuhvaćene u konačnoj tabeli rizika, pa vođenje ove veze odvojeno, bez dodatnog konteksta o tome zašto je određena pretnja relevantna u konkretnom slučaju, odnosno bez odgovarajućeg opisa u nazivu i opisu rizika, može predstavljati nepotrebno dupliranje evidencije.

---

15. Predlog

Relevantni član: **Prilog 2 Tačka 5.7. Rizici zaštite podataka o ličnosti**

Predlog izmene: Predlog da se tačka 5.7. izmeni tako da glasi:

„Zakon o zaštiti podataka o ličnosti zasniva se na pretpostavci da je uvek jasno gde se nalaze podaci o ličnosti, ko ih obrađuje i ko je odgovoran za njihovu obradu.

Korišćenje distribuiranih i geografski dislociranih IKT okruženja može otežati identifikaciju stvarne lokacije gde se podaci o ličnosti obrađuju, kao i razgraničenje uloga učesnika obrade podataka, utvrđivanje primenljivog prava i nadležnost regulatornih organa za zaštitu podataka o ličnosti.

Prenos podataka o ličnosti u druge države, odnosno omogućavanje prava pristupa licima van teritorije Republike Srbije može dovesti do rizika neusklađenosti sa propisima iz oblasti zaštite podataka o ličnosti – zakonitost prenosa (da li postoji primereni nivo zaštite države u koju se prenose podaci o ličnosti), primena odgovarajućih mera zaštite, ostvarivanja prava lica čiji se podaci obrađuju i dr.“

Obrazloženje (opis problema): Smatramo da je potrebno preciznije definisati deo vezan za rizik iz oblasti zaštite podataka o ličnosti imajući u vidu značaj ovih podataka.
