Institut za ekonomsku diplomatiju vas poziva na praktičnu radionicu

Akt o proceni rizika IKT sistema – izrada prema novom Zakonu

METODOLOGIJA IZRADE – POPIS I VREDNOVANJE IKT IMOVINE, IDENTIFIKACIJA PRETNJI I RANJIVOSTI, CIA ANALIZA, PROCENA VEROVATNOĆE I POSLEDICA, NUMERIČKO BODOVANJE, FORMULE ZA PRORAČUN RIZIKA, MATRICA 5×5, REGISTAR RIZIKA, IZBOR MERA ZAŠTITE, PLAN TRETMANA, PROCENA REZIDUALNOG RIZIKA I IZRADA ZAVRŠNOG AKTA.

Amfiteatar Arhiva Jugoslavije, 23. decembar 2026. godine od 10h

Zakonodavni okvir: Zakon o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025) i Pravilnik o opštoj metodologiji za procenu rizika u informaciono-komunikacionim sistemima od posebnog značaja („Sl. glasnik RS“, br. 63/2026).

Novi zakonodavni okvir postavlja zahteve pred operatore IKT sistema od posebnog i važnog značaja, a izrada kvalitetnog Akta o proceni rizika predstavlja jedan od ključnih koraka u uspostavljanju sistema informacione bezbednosti i dokazivanju usklađenosti sa propisima. Međutim, najveći izazov nije samo poznavanje zakonskih odredaba, već njihova **konkretna primena: od popisa i klasifikacije imovine, preko matematičkog proračuna rizika, do izbora kontrola i dokumentovanja preduzetih mera.**

Zato smo pripremili EKSKLUZIVNU, intenzivnu, praktično orijentisanu stručnu obuku, tokom koje će biti sistematično prikazan **postupak izrade Akta o proceni rizika IKT sistema, uz primenu CIA metodologije, matrice rizika 5×5 i GAP analize.**

Poseban akcenat biće na praktičnom vrednovanju IKT resursa, utvrđivanju kritičnih tačaka sistema i povezivanju rezultata procene rizika sa merama informacione bezbednosti, ISO/IEC 27001 kontrolama i planovima kontinuiteta poslovanja i oporavka.

Učesnici će dobiti jasne smernice kako da:

- sistematizuju IKT resurse, organizacione jedinice i odgovornosti;
- primene CIA metodologiju za procenu poverljivosti, integriteta i raspoloživosti;
- identifikuju pretnje, ranjivosti i postojeće bezbednosne kontrole;
- izračunaju inherentni i rezidualni rizik primenom matrice 5×5;
- sprovedu GAP analizu i identifikuju nedostatke u postojećem sistemu zaštite;
- odrede odgovarajuće mere za tretman rizika i prate njihovu realizaciju;
- povežu registar rizika sa planovima kontinuiteta poslovanja (BCP) i oporavka od katastrofe (DRP);
- pripreme dokumentaciju i dokaze o sprovedenim merama za potrebe provere usklađenosti i inspekcijskog nadzora.

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs

Institut za ekonomsku diplomatiju vas poziva na praktičnu radionicu

---

Obuka je namenjena licima odgovornim za informacionu bezbednost, IT rukovodiocima i administratorima, zaposlenima koji učestvuju u upravljanju IKT rizicima, rukovodiocima organizacionih jedinica, internim kontrolorima i revizorima, kao i svim licima uključenim u pripremu i sprovođenje dokumentacije o informacionoj bezbednosti.

Predavačica: Ekspertkinja za informacionu bezbednost i upravljanje rizicima, master inženjerka. Specijalistkinja je za transformaciju kompleksnih teorijskih i regulatornih zahteva u praktične operativne procedure, sa dugogodišnjim iskustvom u oblasti informacione bezbednosti i upravljanja rizicima. Poseban fokus njenog rada je na primeni mera koje doprinose kontinuitetu poslovanja, razvoju bezbednosne kulture i dokumentacionoj spremnosti organizacije za proveru usklađenosti i inspekcijski nadzor.

NAPOMENA: Polaznicima će biti obezbeđene prezentacije i materijali u elektronskom obliku.

NASTAVNI PROGRAM

UVODNI BLOK – ZAKONODAVNE OBAVEZE I SISTEM INFORMACIONE BEZBEDNOSTI

- Novi Zakon o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025) – obaveze operatora IKT sistema od posebnog i važnog značaja
- Obavezna dokumentacija i međusobna povezanost Akta o proceni rizika, Akta o bezbednosti IKT sistema, Plana kontinuiteta poslovanja (BCP) i Plana oporavka (DRP)
- Definisanje konteksta procene rizika – uloga rukovodstva u utvrđivanju kriterijuma prihvatljivosti rizika i aktiviranja BCP/DRP
- Registracija u nadležnoj evidenciji, rokovi usklađivanja i zaštita poverljivih podataka o IKT infrastrukturi

MODUL 1 – SISTEMATIZACIJA IKT RESURSA I CIA VREDNOVANJE IMOVINE

- Sistematizacija radnih mesta i organizacionih jedinica – definisanje odgovornosti i razgraničenje uloga vlasnika resursa i vlasnika rizika
- Šifarnik i klasifikacija imovine – elektronski resursi, papirna dokumentacija, softverski i fizički resursi, zaposleni, imidž i reputacija
- Registar organizacionih jedinica – pravilno postavljanje i šifriranje sektora unutar informacionog sistema
- CIA metodologija – kriterijumi za vrednovanje poverljivosti, integriteta i raspoloživosti
- Skala vrednovanja od 1 do 5 – kvantifikacija finansijskih i operativnih posledica narušavanja bezbednosti
- Praktična analiza kritičnosti IKT resursa na konkretnim primerima

MODUL 2 – KATALOG PRETNJI, MATRICA RIZIKA 5×5 I GAP ANALIZA

- Izrada kataloga pretnji i ranjivosti – namerni napadi, tehnički kvarovi, ljudske greške i bezbednosne slabosti sistema
- Primena matrice rizika 5×5 – kriterijumi i nivoi rizika

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs

- Proračun inherentnog rizika na osnovu identifikovanih IKT resursa, pretnji i ranjivosti
- Proračun rezidualnog rizika – vrednovanje postojećih bezbednosnih kontrola i utvrđivanje preostalog rizika
- GAP analiza – identifikacija razlika između postojećeg i potrebnog nivoa bezbednosti
- Analiza ključnih pokazatelja – maksimalni rizik sistema, prosečni rizik organizacije i identifikacija kritičnih tačaka

MODUL 3 – TRETMAN RIZIKA, BEZBEDNOSNE MERE I ISO 27001 KONTROLE

- Registar rizika – poređenje dosadašnje prakse i zahteva novog zakonodavnog okvira
- Strategije tretmana rizika – izbor odgovarajućeg načina postupanja sa identifikovanim rizicima
- Primena referentnih bezbednosnih kontrola – izbor mera za otklanjanje utvrđenih nedostataka
- ISO/IEC 27001 – Izjava o primenljivosti (Statement of Applicability) i obrazloženje primene ili izuzimanja kontrola iz skupa od 93 kontrole standarda ISO/IEC 27002:2022
- Definisanje rokova, odgovornosti i statusa sprovođenja bezbednosnih mera
- Povezivanje registra rizika sa Planom kontinuiteta poslovanja (BCP) i Planom oporavka od katastrofe (DRP)

DOKUMENTOVANJE, IZVEŠTAVANJE I PRIPREMA ZA NADZOR

- Izveštaj o proveri mera bezbednosti IKT sistema – struktura i sadržina
- Dokumentovanje sprovedenih mera i obezbeđivanje dokaza o usklađenosti sa propisima
- Najvažniji zaključci i preporuke za praktičnu primenu
- Pitanja učesnika i odgovori

Način realizacije, kotizacija i popusti

Obuka se realizuje isključivo u nastavnoj sali, zbog izrazite interaktivnosti predavanja, u jednom od **najlepših i najreprezentativnijih zdanja starog Beograda – Arhivu Jugoslavije**. Smeštena u monumentalnoj zadužbini kralja Aleksandra I Karađorđevića iz 1933. godine, zgrada je proglašena spomenikom kulture i predstavlja jedno od najznačajnijih ostvarenja beogradske međuratne arhitekture.

Posebnu atmosferu daje i prostrani park koji okružuje kompleks, pa će učesnici tokom pauze imati priliku da uživaju u jednom od najlepših zelenih ambijenata ovog dela grada, a po želji i da obiđu aktuelnu izložbu Arhiva Jugoslavije i deo bogatog kulturno-istorijskog nasleđa koje ova ustanova čuva.

Kotizacija iznosi 25.800,00 (+PDV) i obuhvata nastavu, nastavni materijal, odgovore na pitanja, sertifikat o odslušanoj obuci, kao i posluženje u pauzama

Institut za ekonomsku diplomatiju vas poziva na praktičnu radionicu

Popusti:

- **Za sve prijave** odobravamo popust od 5%
- **Za dva i više učesnika** iz iste organizacije, odobravamo dodatnih 10% popusta.
- Za **učesnike naših prethodnih obuka iz oblasti IKT bezbednosti,** odobravamo dodatnih 5% popusta.

Informacije i prijavljivanje:

Prijavu možete izvršiti klikom na dugme "Prijavite se" gde možete popuniti elektronsku prijavu ili preuzeti obrazac u .doc formatu i poslati ga na bilo koju od naših e-mail adresa

Za dodatne informacije kontaktirajte nas na:
011/3077612, 3077613, 063/509972
prijava@economicdiplomacy.co.rs
ied.bg@mts.rs