Samoprocjena kibernetičke sigurnosti - okvir i smjer prema reviziji

ZSIS – svibanj 2025. godine

Sadržaj

Smjernice

za provedbu samoprocjena kibernetičke sigurnosti

Kalkulator

za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta

Pravila

sigurnosne certifikacije za reviziju kibernetičke sigurnosti

obuhvaćaju:

- organizacijske i stručne zahtjeve
- pravila, tehničke zahtjeve, norme i postupke (u provedbi revizije)
- postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti

Okvir

za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima

Katalog kontrola

Popis svih kontrola razvrstanih u tematske kategorije

Vremenski okvir i standardi

Zakon o kibernetičkoj sigurnosti

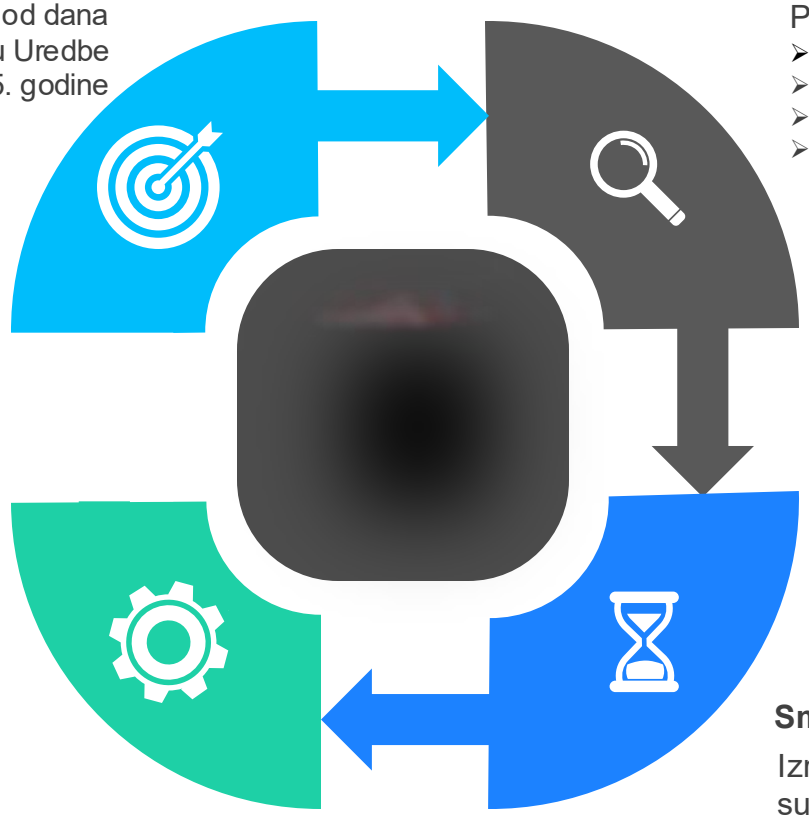
Stupio na snagu 15. veljače 2024.
čl. 31. st. 2. provjera usklađenosti obavlja se u postupku revizije i/ili samoprocjene kibernetičke sigurnosti
čl. 113. st. 5. donijeti pravila u roku od devet mjeseci od dana stupanja na snagu Uredbe
= 30. kolovoz 2025. godine

Uredba o kibernetičkoj sigurnosti

Stupila na snagu 30. studenog 2024.
Prilog II – Mjere upravljanja kibernetičkim sigurnosnim rizicima
čl. 114. st. 6. donijeti smjernice u roku od šest mjeseci od dana stupanja na snagu Uredbe
= 30. svibanj 2025. godine

Daljnji koraci

Smjernice za provedbu samoprocjena kibernetičke sigurnosti su završile javno savjetovanje
Očekujemo do 15. srpnja u javno savjetovanje pustiti Pravila sigurnosne certifikacije



Nacionalni i međunarodni standardi

Uspostava veza između mjera i međunarodnih standarda i normi
Povezivanje mjera na:

- ISO/IEC 27001, 27002, 27005, 27032, 27035,
- NIST Cybersecurity Framework + SP 800 Serija,
- CIS kontrole,
- COBIT

Okvir i kontrole

Izrađen Okvir i katalog kontrola koji je sastavni dio Smjernica za provedbu samoprocjena kibernetičke sigurnosti i Pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti

Smjernice i kalkulator

Izrađene Smjernice i kalkulator za bodovanje sukladno uspostavljenom Okviru

Pravila sigurnosne certifikacije

za reviziju kibernetičke sigurnosti

Uredba o kibernetič

Uredba – Prilog II

- Mjera 5. Osnovne prakse kibernetičke sigurnosti
- Mjere iz podskupa mjere:
  - 5.1. razviti dokumentirati...
  - 5.2. osigurati da se na svim...
  - 5.3. uz provedbu politike korištenja...
  - 5.4. osigurati korištenje osnovnog...
  - 5.5. osigurati pravovremenu i cjelovitu...
  - 5.6. osigurati, ukoliko je tehnički izvedivo...
  - 5.7. definirati i dokumentirati...
  - 5.8. implementirati mehanizme...
  - 5.9. osigurati središnju pohranu...
  - 5.10. osigurati primjenu kontrola...
  - 5.11. smanjiti potencijalnu površinu...

5.1. razviti, dokumentirati, održavati i implementirati pravila osnovne prakse kibernetičke higijene te redovito educirati sve korisnike svojih mrežnih i informacijskih sustava o tim pravilima

5.2. osigurati da se na svim mrežnim i informacijskim sustavima za pristup kojima se koriste lozinke, kao sredstvo autentifikacije koriste politike »najjačih mogućih lozinki« ili ukoliko zbog operativnih razloga to nije moguće, subjekt će definirati i obrazložiti svoju politiku korištenja lozinki koja mora biti u skladu s trenutnim dobrim praksama, kao što je primjerice *»Password Policy Guide of Center for Internet Security (CIS)«*. Ukoliko je subjekt odlučio implementirati svoju politiku korištenja lozinki ona treba uključivati različite smjernice za različite mrežne i informacijske sustave i namjene korištenja lozinki, s obzirom da razina potrebne zaštite često nije ista na svim vrstama mrežnih i informacijskih sustava (primjerice na novijim Windows Server sustavima korištenje lozinke dulje od 14 znakova onemogućava korištenje zastarjele LAN Manager autentifikacije). Općenito na svim mrežnim i informacijskim sustavima koji nemaju mogućnost više-faktorske autentifikacije (MFA) ili za korisničke račune na kojima MFA nije tehnički moguć, minimalna duljina je 14 znakova koji moraju predstavljati kombinaciju velikih i malih slova, znamenki te specijalnih znakova. Lozinka za korisničke račune s privilegiranim pravima pristupa mrežnom i informacijskom sustavu treba biti duga najmanje 16 znakova, a lozinke za servisne račune najmanje 24 znaka, koristeći ranije opisano pravilo o kombinaciji velikih i malih slova, znamenki i specijalnih znakova. Za korisničke račune, uključujući one s privilegiranim pravima pristupa i servisne račune, za koje je uključena provjera drugog faktora, duljina lozinke može biti kraća, ali ne kraća od 8 znakova, ukoliko je to tehnički izvedivo, vodeći pri tome računa o potrebi korištenja ranije opisanog pravila o kombinaciji velikih i malih slova, znamenki i specijalnih znakova. U slučaju da mrežni i informacijski sustav ne može podržati primjenu opisanih pravila određivanja lozinki, subjekt je dužan osigurati druge kompenzacijske mjere zaštite, odnosno ograničavanje pristupa mrežnom i informacijskom sustavu temeljem odgovarajuće kompenzacijske mjere (primjerice obavezno ograničenje fizičkog pristupa ili obavezni udaljeni pristup koji je zaštićen s dva autentifikacijska faktora). Ukoliko se subjekt odlučio za autentifikaciju koja ne uključuje korištenje lozinki, nužno je korištenje dva faktora (biometrija i posjedovanje drugog autentifikacijskog uređaja ili upravljanog pristupnog uređaja). U okviru ovoga podskupa mjere subjekt je dužan:

– osigurati da je snaga provjere autentičnosti prikladna kritičnosti mrežnog i informacijskog sustava te u sladu s procjenom rizika

– provoditi korištenje metoda autentifikacije (lozinke, digitalni certifikati, pametne kartice, biometrija i sl.) koje su u skladu sa stanjem razvoja tehnologije i koristiti jedinstvena autentifikacijska sredstva (nešto što korisnik zna kao lozinka ili pin, nešto što korisnik posjeduje kao pametni telefon ili token, te nešto što korisnik jeste kao otisak prsta, prepoznavanje lica i sl.)

– osigurati sigurnu dodjelu i korištenje autentifikacijskih sredstava (primjerice pohranjivanje i prijenos takvih sredstava u zaštićenom obliku, automatsko generiranje, izrada kriptografskih sažetaka uz »soljenje« i/ili »paprenje« itd.), što uključuje i savjetovanje osoblja o prikladnom postupanju

– zahtijevati inicijalnu promjenu osobnih pristupnih podataka (lozinke i PIN) prilikom prvog korištenja korisničkog računa, kao i u slučaju postojanja sumnje da su osobni pristupni podaci kompromitirani

– ukoliko je tehnički izvedivo, potrebno je zabraniti spremanje lozinki u web-preglednike

– osigurati zaključavanje korisničkih računa nakon prekomjernih neuspjelih pokušaja prijave (account *lockout),* uz mogućnost automatskog otključavanja nakon razumnog vremenskog perioda radi sprječavanja napada uskraćivanjem usluge

– ugasiti neaktivne korisničke sjednice nakon unaprijed određenog perioda neaktivnosti gdje to poslovni proces dopušta i

– zahtijevati posebne vjerodajnice za pristup privilegiranim ili administratorskim korisničkim računima

Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima

Uredba – Prilog II

...

Okvir

- Propisuje:
  - kontrole po mjerama
  - pragove, odnosno težinu, pojedine kontrole
  - pragove, odnosno težinu, pojedine mjere iz podskupa mjera u odnosnu na ostale

$$(O_i \geq P_i, \forall i) \wedge \left(\frac{\sum_{i=0}^{N} O_i}{N} \geq T\right)$$

O_i – ocjena subjekta za *i*-tu kontrolu
P_i – prag za prolaz za *i*-tu kontrolu
T – dodatni prag za prosjek svih ocjena
n – ukupan broj kontrola

5.4. osigurati korištenje osnovnog antivirusnog alata na svim radnim stanicama. Samo korištenje programskih antivirusnog alata za detekciju zlonamjernog softvera i oporavak često nije dovoljno pa je, sukladno procjeni rizika koju provodi subjekt, potrebno primijeniti i dodatne mjere odnosno koristiti alate za otkrivanje i odgovor na kibernetičke prijetnje na krajnjim točkama (EPP/EDR), s prikladnom razinom automatskog odgovora na prijetnje, u svrhu napredne zaštite na svim radnim stanicama i poslužiteljima gdje je to tehnički izvedivo. Subjekt može, zbog tehničke složenosti ili vrlo visoke cijene implementacije, odlučiti mjeru primijeniti samo na odabranom i obrazloženom podskupu programske ili sklopovske imovine sukladno procjeni rizika, primjerice na poslužiteljskoj infrastrukturi, ali onda ista mora biti logički odvojena od nezaštićene programske i sklopovske imovine, kako kompromitacija nezaštićene programske i sklopovske imovine ne bi lako dovela do kompromitacije zaštićenog dijela programske i sklopovske imovine.

tbl 44.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RES-002	≥3	≥4	5
NAD-002	-	≥2	≥4
SKM-001	-	≥3	≥3
SKM-002	≥2	≥3	≥4
RIZ-010	-	≥2	≥3
BODOVNI PRAG	> 2.0	≥ 3.0	> 4.0

Katalog kont

Uredba – Prilog II

Okvir

Katalog kontrola

- Sastoji od 145 kontrola podijeljenih u 14 kategorija:
  - Politike i procedure (POL)
  - Organizacijske odgovornosti (ORG)
  - Podizanje svijesti i edukacija (EDU)
  - Upravljanje resursima (RES)
  - Upravljanje i sudjelovanje (UPR)
  - Praćenje i nadzor (NAD)
  - Upravljanje imovinom (INV)
  - Zaštita podataka (POD)
  - Upravljanje rizicima (RIZ)
  - Digitalni identiteti (DID)
  - Sigurnosne konfiguracije i mehanizmi (SKM)
  - Sigurnost razvoja softvera (SRZ)
  - Kriptografija (KRIP)
  - Fizička sigurnost (FIZ)

5.4. osigurati korištenje osnovnog antivirusnog
korištenje programskih antivirusnog alata za detek
nije dovoljno pa je, sukladno procjeni rizika koj
dodatne mjere odnosno koristiti alate za otkrivar
krajnjim točkama (EPP/EDR), s prikladnom razinc
svrhu napredne zaštite na svim radnim stanicama i
Subjekt može, zbog tehničke složenosti ili vrlo vis
primijeniti samo na odabranom i obrazloženom po
sukladno procjeni rizika, primjerice na poslužitelj
logički odvojena od nezaštićene programske i s
nezaštićene programske i sklopovske imovine ne bi
dijela programske i sklopovske imovine.

tbl.44.

KONTROLA	OSNOVNA	R
RES-002	≥3	
NAD-002	-	
SKM-001	-	
SKM-002	≥2	
RIZ-010	-	
BODOVNI PRAG	> 2.0	

SKM-002: Implementacija osnovnog antivirusnog alata na radnim stanicama i poslužiteljima

Ova kontrola osigurava implementaciju osnovnog antivirusnog alata na svim radnim stanicama i poslužiteljima subjekta kako bi se osigurala osnovna razina zaštite od zlonamjernog softvera. Antivirusni alati moraju uključivati redovito ažuriranje definicija zlonamjernog softvera (ukoliko su temeljeni na definicijama), automatsku detekciju i uklanjanje prijetnji. Subjekt je odgovoran za osiguranje dosljednog upravljanja ovim alatima putem centraliziranog sustava, gdje je to tehnički izvedivo, uključujući redovitu provjeru stanja alata na svim radnim stanicama i poslužiteljima.

Provjera usklađenosti uključuje pregled sustava za upravljanje antivirusnim alatima, dokumentacije ažuriranja definicija zlonamjernog softvera te može uključivati provođenje nasumičnih testova kako bi se osiguralo da alati pravilno funkcioniraju.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Antivirusni alat nije implementiran.
2	Antivirusni alat je sporadično implementiran na podskupa radnih stanica i poslužitelja te povremeno ažuriran.
3	Antivirusni alat je uniformno implementiran uz manje objašnjive iznimke, redovito se ažurira, ali nije centralno upravljan.
4	Antivirusni alat je centralno upravljan, a sve iznimke su jasno vidljive i opravdane.
5	Uspostavljen je sustav koji osigurava da se antivirusni alat uniformno implementira na svakom novom računalu te se sva kasnija odstupanja detektiraju i rješavaju u najkraćem mogućem roku.

Reference:

- ISO/IEC 27001:2022 (A.8.16)
- ISO/IEC 27002:2022 (8.16)
- NIST SP 800-53 Rev. 5 (SI-3, SI-4)
- CIS v8 (10.1)

Revizija VS samoprocjena

Revizija kibernetičke sigurnosti

- tko: Ključni subjekti (važni na zahtjev nadležnog tijela)
- koliko često: najmanje 1x u dvije godine
- rezultat: Izvješće o provedenoj reviziji
  - dostaviti nadležnom tijelu bez odgode (najkasnije 8 dana od dana primitka izvješća
- troškove revizije snose ključni i važni subjekti
- članak 33. Zakona
  - (2) Pravila iz stavka 1. ovoga članka donosi središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, a ona obuhvaćaju:
    - organizacijske i stručne zahtjeve koje moraju ispunjavati pružatelji upravljanih sigurnosnih usluga za provedbu revizije kibernetičke sigurnosti
    - pravila, tehničke zahtjeve, norme i postupke koji se primjenjuju u provedbi revizije kibernetičke sigurnosti, uključujući obvezni sadržaj izvješća o provedenoj reviziji kibernetičke sigurnosti i
    - postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti, prava i obveze pružatelja upravljanih sigurnosnih usluga te pravnu zaštitu u tom postupku.

Samoprocjena kibernetičke sigurnosti

- tko: Važni subjekti
- koliko često: najmanje 1x u dvije godine
- rezultat: Izjava o sukladnosti
  - čuvati 10 godina od sastavljanja
- troškove samoprocjene snose važni subjekti
- cilj:
  - odrediti stupanj usklađenosti uspostavljenih mjera
  - odrediti trend podizanja razine zrelosti kibernetičke sigurnosti subjekta
- članak 52. Uredbe
  - (1) Stupanj usklađenosti uspostavljenih mjera temelji se na procjeni stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima u subjektu.
  - (2) Procjenom stupnja usklađenosti dokumentiranih mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se postoje li dokumentirane sigurnosne politike o provedbi mjera i u kojoj mjeri su u skladu sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima Prilogom II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe koju je subjekt dužan provoditi.
  - (3) Procjenom stupnja usklađenosti implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se u kojoj mjeri su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima usklađene sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima u Prilogu II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe koju je subjekt dužan provoditi.

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

Uvod
Provedba samoprocjene kibernetičke sigurnosti
Izgled kalkulatora samoprocjene kibernetičke sigurnosti
Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima
Trend podizanja razine zrelosti kibernetičke sigurnosti
Postupak nakon provedene samoprocjene

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

- **Uvod**
- **Provedba samoprocjene kibernetičke sigurnosti**

Izgled kalkulatora samoprocjene kibernetičke sigurnosti
Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima
Trend podizanja razine zrelosti kibernetičke sigurnosti
Postupak nakon provedene samoprocjene

Uvod

Zavod za sigurnost informacijskih sustava (u daljnjem tekstu: ZSIS), u skladu s člankom 57. Uredbe o kibernetičkoj sigurnosti („Narodne novine“, broj: 135/2024., u daljnjem tekstu: Uredba) donosi ove Smjernice za provedbu samoprocjene kibernetičke sigurnosti (u daljnjem tekstu: Smjernice).

Ključni i važni subjekti dužni su provjeravati usklađenost uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom o kibernetičkoj sigurnosti („Narodne novine“, broj: 14/2024., u daljnjem tekstu: Zakon) i Uredbom. Provjera usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima obavlja se u postupku revizije kibernetičke sigurnosti ključnih i važnih subjekata te u postupku samoprocjene kibernetičke sigurnosti (u daljnjem tekstu: samoprocjena) važnih subjekata.

Cilj provođenja samoprocjene je utvrditi:

- stupanj usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. Uredbe utvrđenim za razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. Uredbe koju je subjekt dužan provoditi i
- trend podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Smjernice definiraju postupak i sistematiziraju podatke potrebne za utvrđivanje stupnja usklađenosti uspostavljenih mjera temeljenog na procjeni stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima u subjektu te trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Sastavne dijelove Smjernica čine:

- **Prilog A - Kalkulator za samoprocjenu kibernetičke sigurnosti:** služi kao alat za provedbu samoprocjene koji uključuje bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.
- **Prilog B - Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima:** predstavlja upute za evaluacije postupaka, kontrola i mjera koje subjekt provodi radi identifikacije, ublažavanja i upravljanja potencijalnim kibernetičkim prijetnjama i ranjivostima. U dokumentu je pojašnjen sustav ocjenjivanja podskupova mjera i definirani su bodovni pragovi ocjena prema razini mjere koju subjekt prema provedenoj nacionalnoj procjeni rizika mora primjenjivati.

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

- **Uvod**
- **Provedba samoprocjene kibernetičke sigurnosti**
- **Izgled kalkulatora samoprocjene kibernetičke sigurnosti**

Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima
Trend podizanja razine zrelosti kibernetičke sigurnosti
Postupak nakon provedene samoprocjene

Izgled kalkulatora samoprocjene kibernetičke sigurnosti

Kalkulator kao alat za provedbu samoprocjene sadrži tablični prikaz mjera, podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima (u daljnjem tekstu: podskupovi mjera), naziva kontrola mjera i polja za unos ocjena, te polja koja se automatizmom izračunavaju.

Kalkulator se sastoji od sljedećih radnih listova: uvoda, radnih listova za unos ocjena i izračun konačnog rezultata samoprocjene po pripadajućim razinama mjera upravljanja kibernetičkim sigurnosnim rizicima i izjave o sukladnosti.

Slika 1 Prikaz trake kartica radnih listova

Na radnom listu „Uvod" nalaze se kratke značajke Kalkulatora, padajući izbornik s razinom mjera te korisne poveznice. U padajućem izborniku subjekt odabire razinu koja je utvrđena nacionalnom procjenom rizika.


PRILOG A
KALKULATOR ZA SAMOPROCJENU KIBERNETIČKE SIGURNOSTI

Obveznici primjene provedbe samoprocjene kibernetičke sigurnosti, sukladno Zakonu o kibernetičkoj sigurnosti („Narodne novine", broj 14/24.; dalje: Zakon) i Uredbi o kibernetičkoj sigurnosti („Narodne novine", broj 135/24.; dalje: Uredba) prilikom provedbe samoprocjene kibernetičke sigurnosti koriste i popunjavaju ovaj tablični kalkulator koji služi za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Prilikom korištenja kalkulatora obveznici primjene provedbe samoprocjene dužni su pridržavati se Smjernica za provedbu procjene kibernetičke sigurnosti (dalje: Smjernice). Zavod za sigurnost informacijskih sustava (dalje: ZSIS) sukladno isključivoj nadležnosti i ovlasti propisanoj Uredbom donosi navedene Smjernice s pripadajućim prilozima.

Smjernice s pripadajućim prilozima objavljuju se na mrežnim stranicama ZSIS-a te su javno dostupni.

U svrhu prilagodbe važećim izvorima prava te postizanja visoke razine kibernetičke sigurnosti, ZSIS će redovito, a najmanje jednom u dvije (2) godine, provoditi reviziju Smjernica i pripadajućih priloga te, prema potrebi, izvršiti nužne izmjene i dopune. Sve izmjene Smjernica i pripadajućih priloga stupaju na snagu prvog dana nakon njihove službene objave na mrežnim stranicama ZSIS-a.

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA | OSNOVNA

POVEZNICE
Zakon o kibernetičkoj sigurnosti (NN 14/2024)
Uredba o kibernetičkoj sigurnosti (NN 135/2024)
Nacionalni centar za kibernetičku sigurnost
Zavod za sigurnost informacijskih sustava

Verzija kalkulatora: 1.0

UVOD | OSNOVNA | SREDNJA | NAPREDNA | SAŽETAK | TREND | IZJAVA

Slika 2 Radni list „Uvod"

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

- **Uvod**
- **Provedba samoprocjene kibernetičke sigurnosti**
- **Izgled kalkulatora samoprocjene kibernetičke sigurnosti**
- **Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima**

Trend podizanja razine zrelosti kibernetičke sigurnosti

Postupak nakon provedene samoprocjene

Ocjena dokumentacije pojedinog podskupa mjere (DP) određuje se kao aritmetička sredina ocjena dokumentacije pojedinačnih kontrola tog podskupa.

$$DP = \frac{\sum_{i=1}^{n} DKi}{n}, \quad n \in \mathrm{N} \qquad (1.2)$$

DP – ocjena dokumentacije podskupa mjere

DK – ocjena dokumentacije kontrole

Ocjena implementacije pojedinog podskupa mjere (IP) određuje se kao aritmetička sredina ocjena implementacije pojedinačnih kontrola tog podskupa.

$$IP = \frac{\sum_{i=1}^{n} IKi}{n}, \quad n \in \mathrm{N} \qquad (1.3)$$

IP – ocjena implementacije podskupa mjere

IK – ocjena implementacije kontrole

Ocjena pojedinog podskupa mjere (P) određuje se kao aritmetička sredina ocjene dokumentacije podskupa mjere (DP) i ocjene implementacije podskupa mjere (IP).

$$P = \frac{DP + IP}{2} \qquad (1.4)$$

P – ocjena podskupa mjere

DP – ocjena dokumentacije podskupa mjere

IP – ocjena implementacije podskupa mjere

Ocjena pojedine mjere (M) određuje se kao aritmetička sredina ocjena podskupova iz te mjere (P).

$$M = \frac{\sum_{i=1}^{n} Pi}{n}, \quad n \in \mathrm{N} \qquad (1.5)$$

M – ocjena mjere

P – ocjena podskupa mjere

Bodovni pragovi ocjena koji se moraju zadovoljiti definirani su u Prilogu B - Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima (u daljnjem tekstu: Prilog B). Ako je

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

- **Uvod**
- **Provedba samoprocjene kibernetičke sigurnosti**
- **Izgled kalkulatora samoprocjene kibernetičke sigurnosti**
- **Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima**
- **Trend podizanja razine zrelosti kibernetičke sigurnosti**

Postupak nakon provedene samoprocjene

Trend podizanja razine zrelosti kibernetičke sigurnosti

Trend podizanja razine zrelosti kibernetičke sigurnosti (u daljnjem tekstu: trend) utvrđuje se dodatnim bodovanjem podskupova mjera koje subjekt provodi na temelju mjere 3. »Upravljanje rizicima« iz Priloga II. Uredbe, u smislu podizanja razine provedbe pojedinih obvezujućih mjera, kao i u smislu provedbe dobrovoljnih mjera.

Sukladno uvjetima koji su sadržani u Prilogu C, ocjenjuje se usklađenost dokumentiranih i implementiranih kontrola podskupova mjera koje subjekt provodi kao dobrovoljne i kontrola podskupova obvezujućih mjera u slučaju podizanja razine mjera, pri čemu se upisuju ocjene u stupce ocjena dokumentacije kontrole i ocjena implementacije kontrole.

U inicijalnom postupku samoprocjene, dobiveni rezultat u izračunu trenda se ne uzima u obzir. Trend se uključuje u izračun rezultata samoprocjene nakon prve obavljene samoprocjene, odnosno pri idućoj provedbi samoprocjene.

Radi preglednosti i lakšeg snalaženja, polja koja se odnose na dobrovoljne podskupove mjera označena su sivom bojom. Podskupovi mjera koje subjekt provodi kao dobrovoljne, označava u tablici na način da se u padajućem izborniku stupca „podskup mjere se ocjenjuje“ pojedinog podskupa mjere odabere opcija *DA* kako bi se bodovi uključili u izračun trenda. Odabirom opcije *DA* u polju „podskup mjere se ocjenjuje“, polja koja se odnose na dobrovoljni podskup mjere postaju bijela. Dobrovoljne podskupove mjera koje subjekt ne provodi, u navedenom stupcu, u padajućem izborniku odabire opciju *NE*, čime polja koja se odnose na te podskupove mjera ostaju obojana sivom bojom.

#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE
3.7	koristiti napredne softverske alate za procjenu i praćenje rizika. Ovi alati trebaju omogućiti detaljnu analizu i procjenu kibernetičkih prijetnji, identifikaciju ranjivosti, te praćenje incidenata u stvarnom vremenu. Softverski alati moraju biti sposobni za automatizirano prikupljanje i analizu relevantnih podataka, generiranje izvještaja i pružanje preporuka za ublažavanje ili eliminaciju rizika. Subjekt mora osigurati redovitu upotrebu i ažuriranje ovih alata kako bi se osigurala njihova učinkovitost u prepoznavanju i upravljanju rizicima. Rezultati dobiveni korištenjem ovih alata moraju biti integrirani u sveukupni proces upravljanja rizicima unutar subjekta.	DOBROVOLJNO	DA	RIZ-011: Softverski alati za procjenu i praćenje rizika

Slika 9 Prikaz dobrovoljnog podskupa mjere koji je uključen u izračun trenda

#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE
4.9	raziti i provoditi obuku za odgovor na incidente u subjektu za ključne osobe koje sudjeluju u tom procesu. Obuka mora uključivati praktične scenarije i redovite vježbe kako bi se osiguralo da su svi sudionici dobro pripremljeni za učinkovito reagiranje na incidente. Redovitim ažuriranjem obuke, subjekt je dužan prilagoditi obuku novim prijetnjama i najboljim praksama u području kibernetičke sigurnosti. Time se povećava otpornost subjekta na incidente i osigurava brza i adekvatna reakcija u slučaju njihovog pojavljivanja.	DOBROVOLJNO	NE	EDU-006: Program osposobljavanja zaposlenika o specifičnim mjerama kibernetičke sigurnosti EDU-008: Program obuke za odgovor na incidente

Slika 10 Prikaz dobrovoljnog podskupa mjere koji nije uključen u izračun trenda

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

- **Uvod**
- **Provedba samoprocjene kibernetičke sigurnosti**
- **Izgled kalkulatora samoprocjene kibernetičke sigurnosti**
- **Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima**
- **Trend podizanja razine zrelosti kibernetičke sigurnosti**
- **Postupak nakon provedene samoprocjene**

Postupak nakon provedene samoprocjene

Ako nakon provedene samoprocjene ukupni bodovi stupnja usklađenosti mjera pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom, subjekt sastavlja izjavu o sukladnosti.

Na obrascu izjave o sukladnosti koji se nalazi u Prilogu IV. Uredbe upisuju se ukupni bodovi stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt, ukupni bodovi trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta i ostali traženi podaci sadržani u Uredbi.

Obrazac izjave o sukladnosti također je moguće popuniti i u kalkulatoru. Navedeni obrazac nalazi se na radnom listu „Izjava". Ako se obrazac izjave o sukladnosti popunjava u kalkulatoru, tada se automatski popunjavaju sljedeća polja:

- Razina mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom,
- Ukupni bodovi stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima i
- Ukupni bodovi trenda podizanja razine zrelosti.

Ako ukupni bodovi stupnja usklađenosti mjera pokazuju da uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima nisu u skladu s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom, subjekt određuje plan daljnjeg postupanja koji obuhvaća ponovnu samoprocjenu te ispravke utvrđenih nedostataka.

Izjavu o sukladnosti i plan daljnjeg postupanja važni subjekti dužni su dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti bez odgode, a najkasnije u roku od osam dana od dana njihova sastavljanja. Subjekt je dužan čuvati izjavu o sukladnosti i drugu dokumentaciju nastalu u postupku samoprocjene deset godina od sastavljanja izjave.

PRILOG A
KALKULATOR ZA SAMOPROCJENU KIBERNETIČKE SIGURNOSTI

Obveznici primjene provedbe samoprocjene kibernetičke sigurnosti, sukladno Zakonu o kibernetičkoj sigurnosti(„Narodne novine“, broj 14/24.; dalje: Zakon) i Uredbi o kibernetičkoj sigurnosti(„Narodne novine“, broj 135/24.; dalje: Uredba) prilikom provedbe samoprocjene kibernetičke sigurnosti koriste i popunjavaju ovaj tablični kalkulator koji služi za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Prilikom korištenja kalkulatora obveznici primjene provedbe samoprocjene dužni su pridržavati se Smjernica za provedbu procjene kibernetičke sigurnosti (dalje: Smjernice). Zavod za sigurnost informacijskih sustava (dalje: ZSIS) sukladno isključivoj nadležnosti i ovlasti propisanoj Uredbom donosi navedene Smjernice s pripadajućim prilozima.

Smjernice s pripadajućim prilozima objavljuju se na mrežnim stranicama ZSIS-a te su javno dostupni.

U svrhu prilagodbe važećim izvorima prava te postizanja visoke razine kibernetičke sigurnosti, ZSIS će redovito, a najmanje jednom u dvije (2) godine, provoditi reviziju Smjernica i pripadajućih priloga te, prema potrebi, izvršiti nužne izmjene i dopune. Sve izmjene Smjernica i pripadajućih priloga stupaju na snagu prvog dana nakon njihove službene objave na mrežnim stranicama ZSIS-a.

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

POVEZNICE

Verzija kalkulatora: 1.0

Zakon o kibernetičkoj sigurnosti (NN 14/2024)
Uredba o kibernetičkoj sigurnosti (NN 135/2024)
Nacionalni centar za kibernetičku sigurnost
Zavod za sigurnost informacijskih sustava

Prilog A - Kalkulator samoprocjene.xlsx - Excel

Marko Vrančić

File Home Insert Page Layout Formulas Data Review View Developer Help Tell me what you want to do Share

J27 OSNOVNA

PRILOG A
KALKULATOR ZA SAMOPROCJENU KIBERNETIČKE SIGURNOSTI

Obveznici primjene provedbe samoprocjene kibernetičke sigurnosti, sukladno Zakonu o kibernetičkoj sigurnosti(„Narodne novine“, broj 14/24.; dalje: Zakon) i Uredbi o kibernetičkoj sigurnosti(„Narodne novine“, broj 135/24.; dalje: Uredba) prilikom provedbe samoprocjene kibernetičke sigurnosti koriste i popunjavaju ovaj tablični kalkulator koji služi za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Prilikom korištenja kalkulatora obveznici primjene provedbe samoprocjene dužni su pridržavati se Smjernica za provedbu procjene kibernetičke sigurnosti (dalje: Smjernice). Zavod za sigurnost informacijskih sustava (dalje: ZSIS) sukladno isključivoj nadležnosti i ovlasti propisanoj Uredbom donosi navedene Smjernice s pripadajućim prilozima.

Smjernice s pripadajućim prilozima objavljuju se na mrežnim stranicama ZSIS-a te su javno dostupni.

U svrhu prilagodbe važećim izvorima prava te postizanja visoke razine kibernetičke sigurnosti, ZSIS će redovito, a najmanje jednom u dvije (2) godine, provoditi reviziju Smjernica i pripadajućih priloga te, prema potrebi, izvršiti nužne izmjene i dopune. Sve izmjene Smjernica i pripadajućih priloga stupaju na snagu prvog dana nakon njihove službene objave na mrežnim stranicama ZSIS-a.

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

OSNOVNA
SREDNJA
NAPREDNA

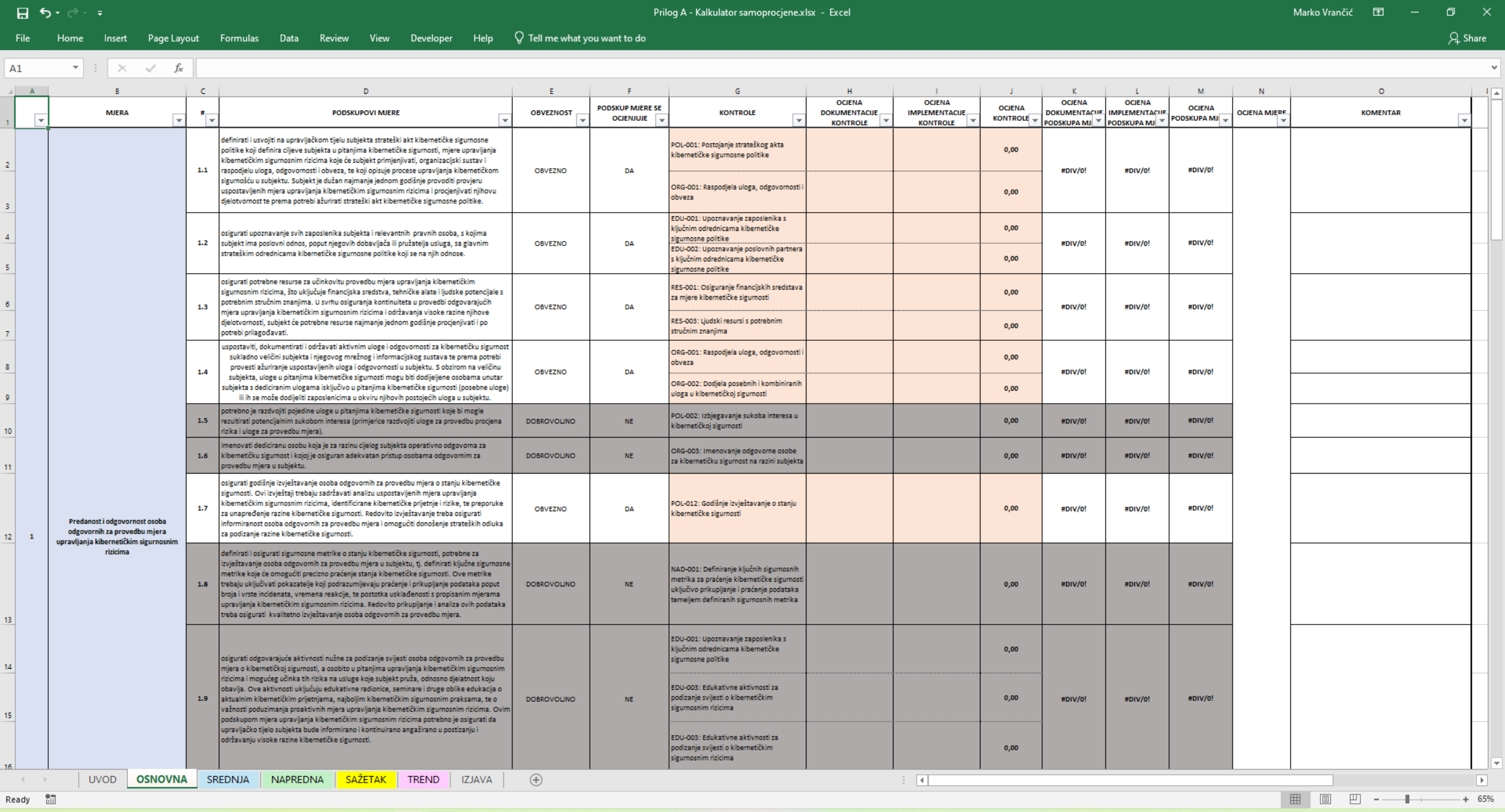
POVEZNICE

Verzija kalkulatora: 1.0

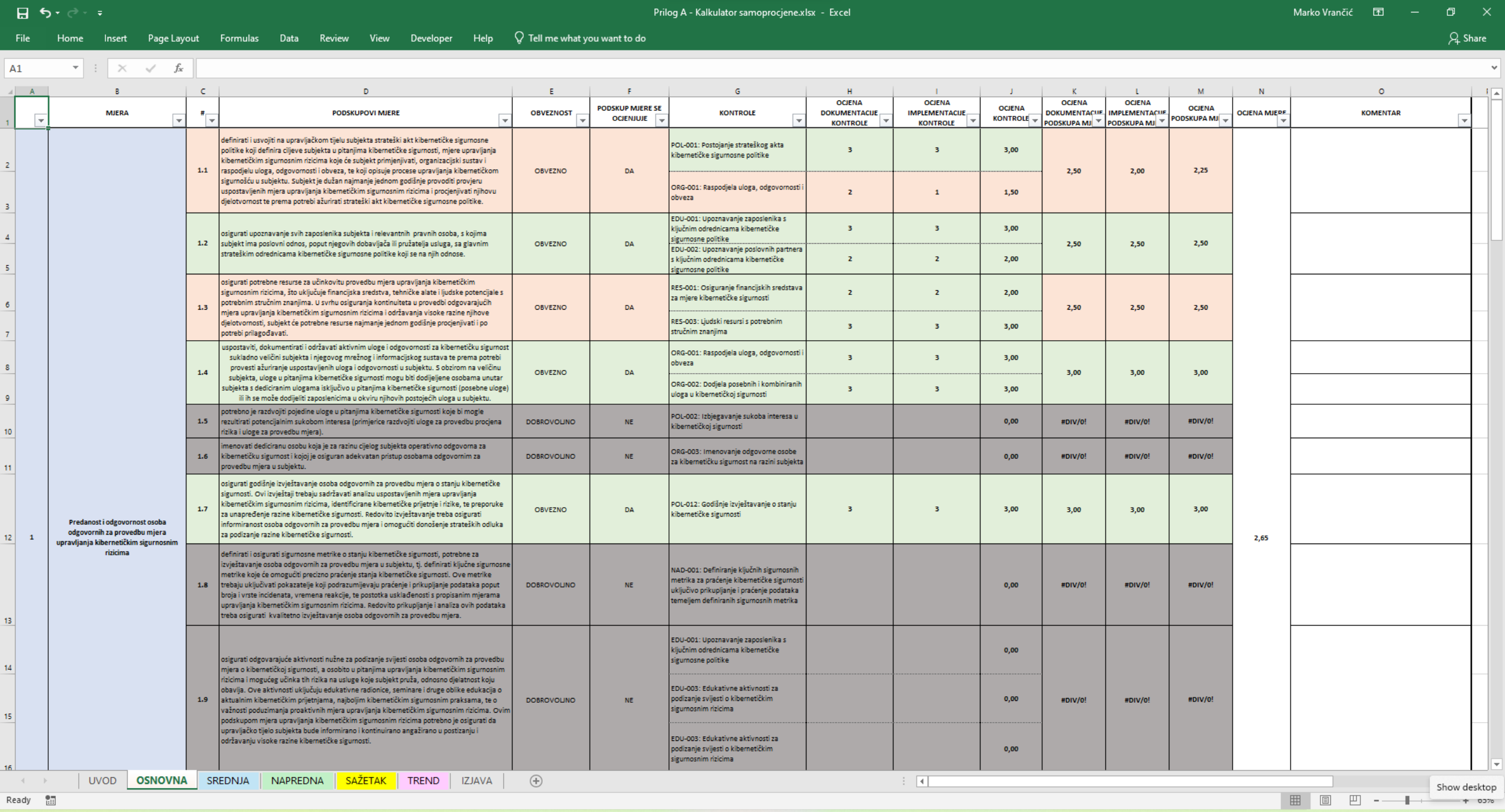
Zakon o kibernetičkoj sigurnosti (NN 14/2024)
Uredba o kibernetičkoj sigurnosti (NN 135/2024)
Nacionalni centar za kibernetičku sigurnost
Zavod za sigurnost informacijskih sustava

UVOD OSNOVNA SREDNJA NAPREDNA SAŽETAK TREND IZJAVA

Ready 100%



	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJ	OCJENA MJERE	KOMENTAR
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.1	definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.	OBVEZNO	DA	POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						ORG-001: Raspodjela uloga, odgovornosti i obveza			0,00					
		1.2	osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, sa glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.	OBVEZNO	DA	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike			0,00					
		1.3	osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati.	OBVEZNO	DA	RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						RES-003: Ljudski resursi s potrebnim stručnim znanjima			0,00					
		1.4	uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovog mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu.	OBVEZNO	DA	ORG-001: Raspodjela uloga, odgovornosti i obveza			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti			0,00					
		1.5	potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera).	DOBROVOLJNO	NE	POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.6	imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu.	DOBROVOLJNO	NE	ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.7	osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti.	OBVEZNO	DA	POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.8	definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera.	DOBROVOLJNO	NE	NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.9	osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti.	DOBROVOLJNO	NE	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					



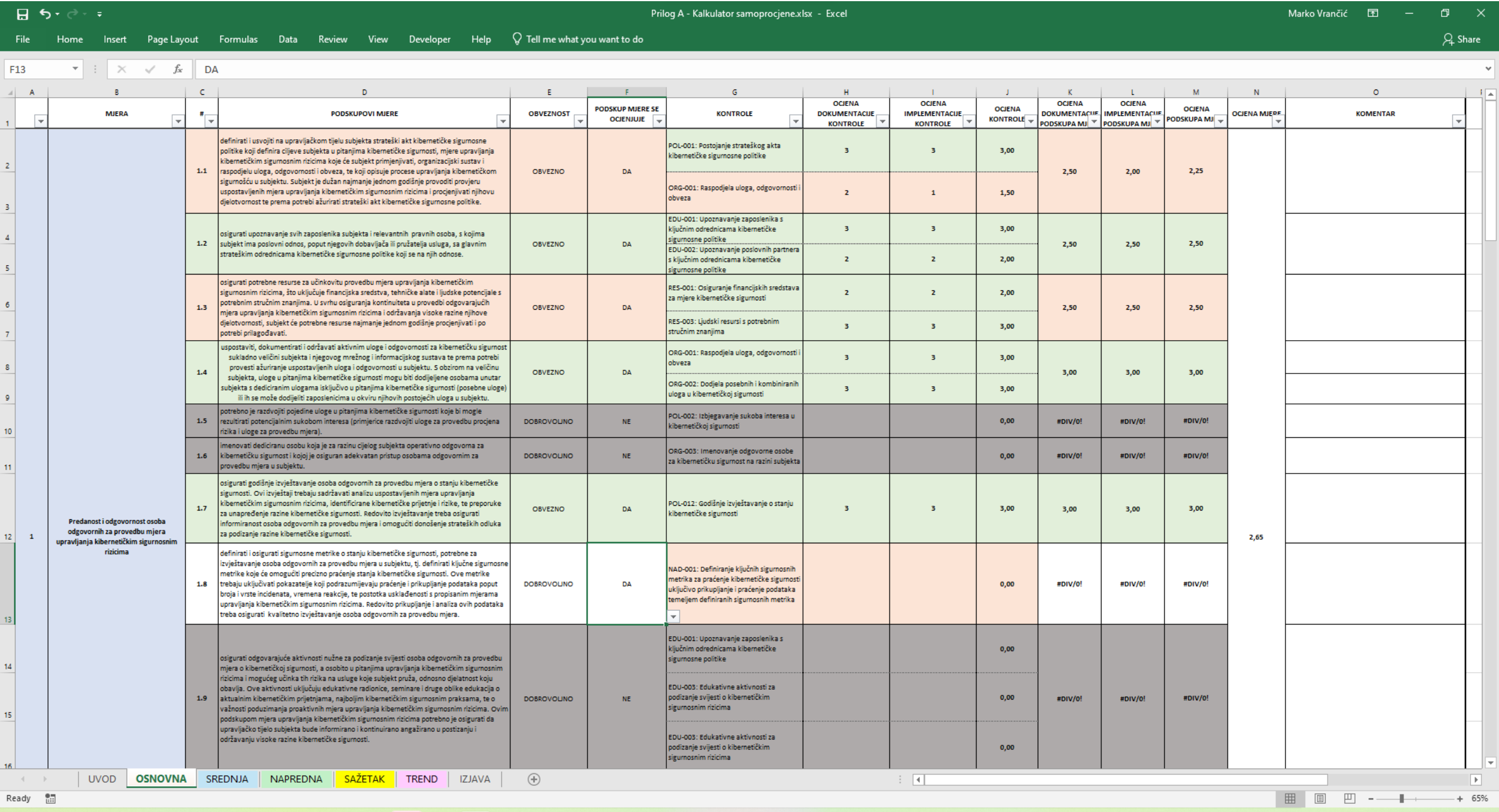
	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJ	OCJENA MJERE	KOMENTAR
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.1	definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.	OBVEZNO	DA	POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike	3	3	3,00	2,50	2,00	2,25	2,65	
						ORG-001: Raspodjela uloga, odgovornosti i obveza	2	1	1,50					
		1.2	osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, sa glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.	OBVEZNO	DA	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike	3	3	3,00	2,50	2,50	2,50		
						EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike	2	2	2,00					
		1.3	osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati.	OBVEZNO	DA	RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti	2	2	2,00	2,50	2,50	2,50		
						RES-003: Ljudski resursi s potrebnim stručnim znanjima	3	3	3,00					
		1.4	uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovog mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu.	OBVEZNO	DA	ORG-001: Raspodjela uloga, odgovornosti i obveza	3	3	3,00	3,00	3,00	3,00		
						ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti	3	3	3,00					
		1.5	potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera).	DOBROVOLJNO	NE	POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.6	imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu.	DOBROVOLJNO	NE	ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.7	osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti.	OBVEZNO	DA	POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti	3	3	3,00	3,00	3,00	3,00		
		1.8	definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera.	DOBROVOLJNO	NE	NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.9	osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti.	DOBROVOLJNO	NE	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					

F13 NE

	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJ	OCJENA MJERE	KOMENTAR
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.1	definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.	OBVEZNO	DA	POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike	3	3	3,00	2,50	2,00	2,25	2,65	
						ORG-001: Raspodjela uloga, odgovornosti i obveza	2	1	1,50					
		1.2	osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, sa glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.	OBVEZNO	DA	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike	3	3	3,00	2,50	2,50	2,50		
						EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike	2	2	2,00					
		1.3	osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati.	OBVEZNO	DA	RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti	2	2	2,00	2,50	2,50	2,50		
						RES-003: Ljudski resursi s potrebnim stručnim znanjima	3	3	3,00					
		1.4	uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovog mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu.	OBVEZNO	DA	ORG-001: Raspodjela uloga, odgovornosti i obveza	3	3	3,00	3,00	3,00	3,00		
						ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti	3	3	3,00					
		1.5	potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera).	DOBROVOLJNO	NE	POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.6	imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu.	DOBROVOLJNO	NE	ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.7	osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti.	OBVEZNO	DA	POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti	3	3	3,00	3,00	3,00	3,00		
		1.8	definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera.	DOBROVOLJNO	NE	NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.9	osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti.	DOBROVOLJNO	NE	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					

UVOD | OSNOVNA | SREDNJA | NAPREDNA | SAŽETAK | TREND | IZJAVA

Ready 65%



	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJ	OCJENA MJERE	KOMENTAR
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.1	definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.	OBVEZNO	DA	POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike	3	3	3,00	2,50	2,00	2,25	2,65	
						ORG-001: Raspodjela uloga, odgovornosti i obveza	2	1	1,50					
		1.2	osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, sa glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.	OBVEZNO	DA	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike	3	3	3,00	2,50	2,50	2,50		
						EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike	2	2	2,00					
		1.3	osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati.	OBVEZNO	DA	RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti	2	2	2,00	2,50	2,50	2,50		
						RES-003: Ljudski resursi s potrebnim stručnim znanjima	3	3	3,00					
		1.4	uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovog mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu.	OBVEZNO	DA	ORG-001: Raspodjela uloga, odgovornosti i obveza	3	3	3,00	3,00	3,00	3,00		
						ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti	3	3	3,00					
		1.5	potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera).	DOBROVOLJNO	NE	POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.6	imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu.	DOBROVOLJNO	NE	ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.7	osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti.	OBVEZNO	DA	POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti	3	3	3,00	3,00	3,00	3,00		
		1.8	definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera.	DOBROVOLJNO	DA	NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.9	osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti.	DOBROVOLJNO	NE	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					

C13 1.8

	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJ	OCJENA MJERE	KOMENTAR
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.1	definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.	OBVEZNO	DA	POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike	3	3	3,00	2,50	2,00	2,25	2,65	
						ORG-001: Raspodjela uloga, odgovornosti i obveza	2	1	1,50					
		1.2	osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, sa glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.	OBVEZNO	DA	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike	3	3	3,00	2,50	2,50	2,50		
						EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike	2	2	2,00					
		1.3	osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati.	OBVEZNO	DA	RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti	2	2	2,00	2,50	2,50	2,50		
						RES-003: Ljudski resursi s potrebnim stručnim znanjima	3	3	3,00					
		1.4	uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovog mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu.	OBVEZNO	DA	ORG-001: Raspodjela uloga, odgovornosti i obveza	3	3	3,00	3,00	3,00	3,00		
						ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti	3	3	3,00					
		1.5	potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera).	DOBROVOLJNO	NE	POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.6	imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu.	DOBROVOLJNO	NE	ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		1.7	osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti.	OBVEZNO	DA	POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti	3	3	3,00	3,00	3,00	3,00		
		1.8	definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera.	DOBROVOLJNO	DA	NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika	4	2	3,00	4,00	2,00	3,00		
		1.9	osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti.	DOBROVOLJNO	NE	EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					
						EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima			0,00					

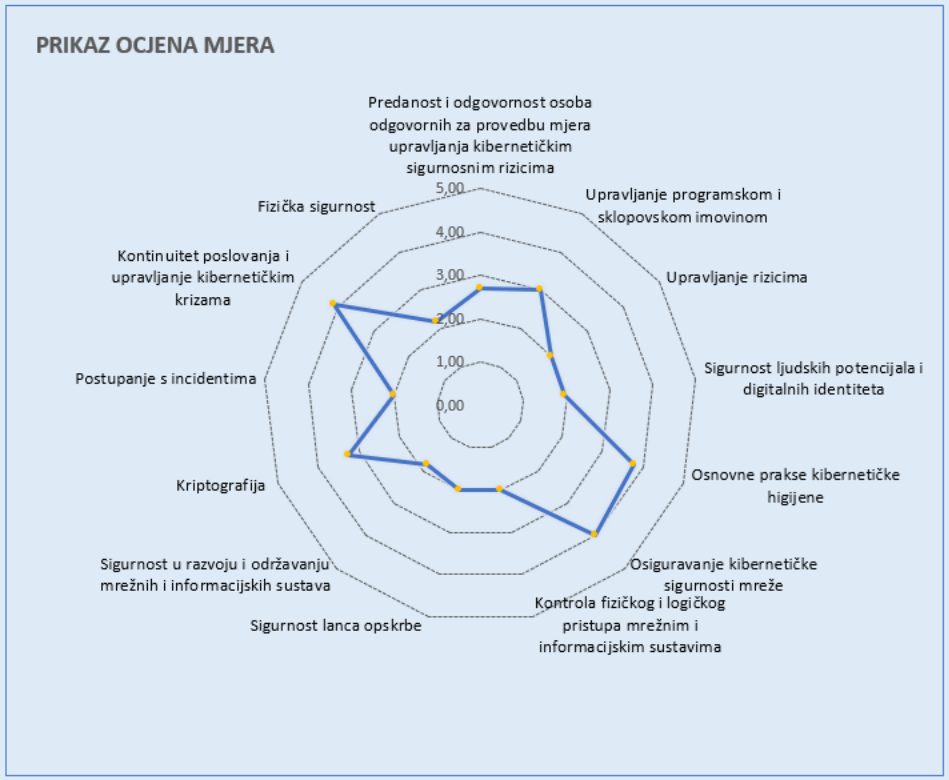
UVOD | OSNOVNA | SREDNJA | NAPREDNA | SAŽETAK | TREND | IZJAVA

D3

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

#	MJERA	OCJENA	RAZINA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	2,70	OSNOVNA
2	Upravljanje programskom i sklopovskom imovinom	3,00	OSNOVNA
3	Upravljanje rizicima	2,00	OSNOVNA
4	Sigurnost ljudskih potencijala i digitalnih identiteta	1,94	OSNOVNA
5	Osnovne prakse kibernetičke higijene	3,79	OSNOVNA
6	Osiguravanje kibernetičke sigurnosti mreže	4,00	OSNOVNA
7	Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima	2,00	OSNOVNA
8	Sigurnost lanca opskrbe	2,00	OSNOVNA
9	Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava	1,83	OSNOVNA
10	Kriptografija	3,25	OSNOVNA
11	Postupanje s incidentima	2,00	OSNOVNA
12	Kontinuitet poslovanja i upravljanje kibernetičkim krizama	4,10	OSNOVNA
13	Fizička sigurnost	2,17	OSNOVNA
#	UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	2,68	

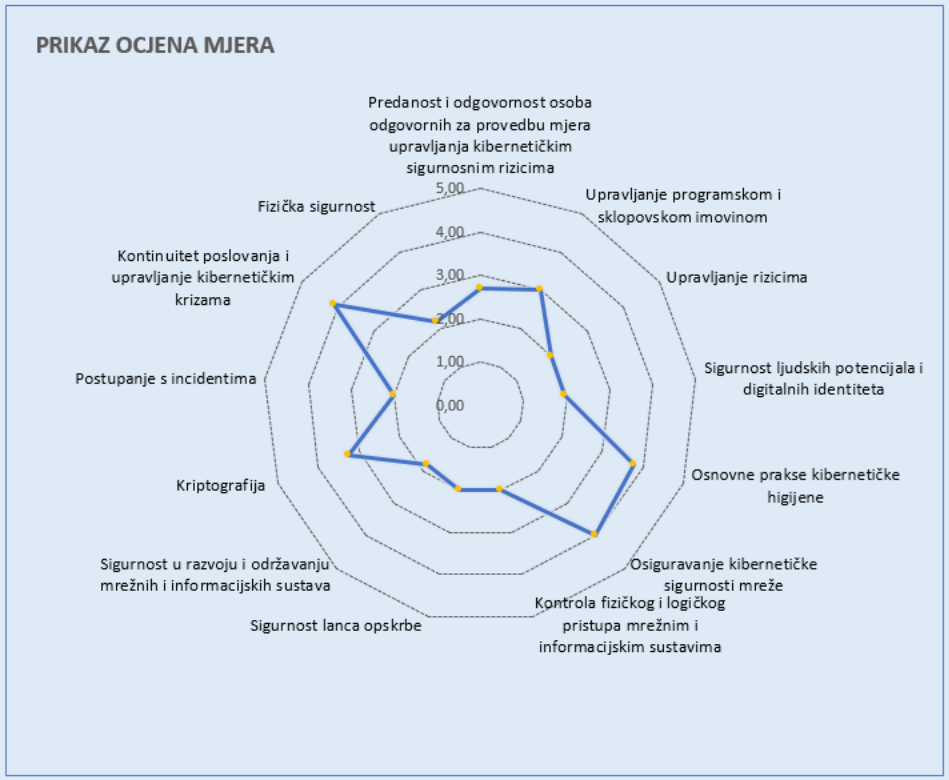


E14 =D3

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

#	MJERA	OCJENA	RAZINA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	2,70	OSNOVNA
2	Upravljanje programskom i sklopovskom imovinom	3,00	OSNOVNA
3	Upravljanje rizicima	2,00	OSNOVNA
4	Sigurnost ljudskih potencijala i digitalnih identiteta	1,94	OSNOVNA
5	Osnovne prakse kibernetičke higijene	3,79	OSNOVNA
6	Osiguravanje kibernetičke sigurnosti mreže	4,00	OSNOVNA
7	Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima	2,00	OSNOVNA / SREDNJA / NAPREDNA
8	Sigurnost lanca opskrbe	2,00	
9	Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava	1,83	OSNOVNA
10	Kriptografija	3,25	OSNOVNA
11	Postupanje s incidentima	2,00	OSNOVNA
12	Kontinuitet poslovanja i upravljanje kibernetičkim krizama	4,10	OSNOVNA
13	Fizička sigurnost	2,17	OSNOVNA
#	UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	2,68	



UVOD | OSNOVNA | SREDNJA | NAPREDNA | SAŽETAK | TREND | IZJAVA

Ready

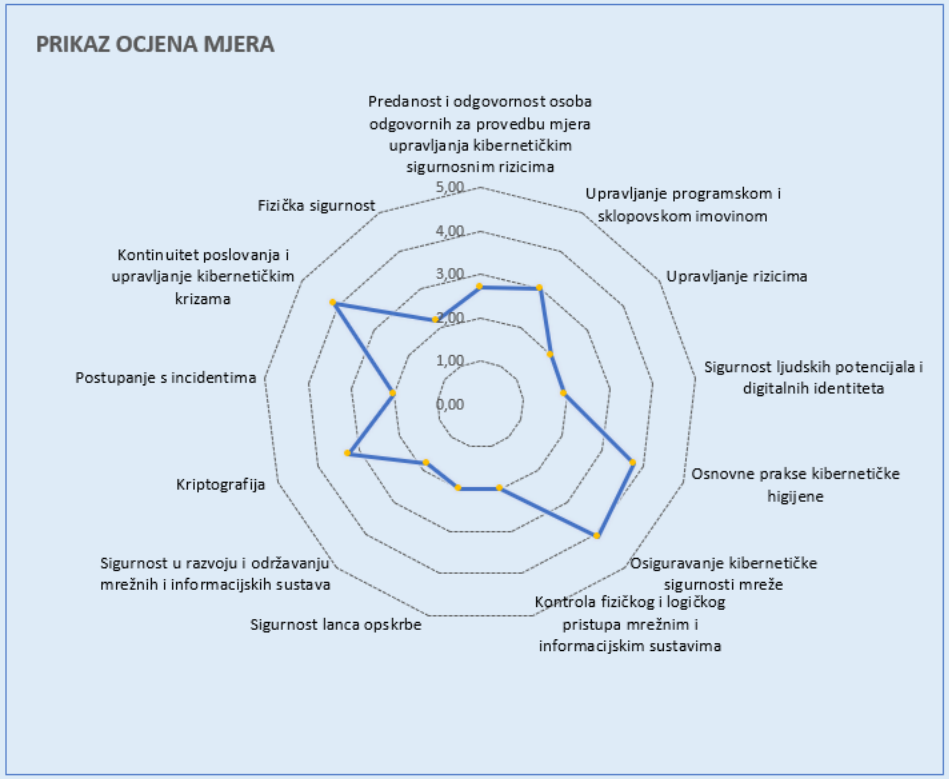
	MJERA	#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJE	OCJENA IMPLEMENTACIJE PODSKUPA MJE	OCJENA PODSKUPA MJERE	OCJENA MJERE	KOME
			planiranim intervalima provjeravati bilježe li se dnevnički zapisi ispravno kroz provođenje ili simulaciju radnje koja bi trebala rezultirati bilježenjem odgovarajućeg dnevničkog zapisa. Subjekt mora voditi brigu da se praćenje implementira i na način kojim bi se minimaliziralo postojanje lažno pozitivnih i lažno negativnih događaja.			DID-006: Nadzor i revizija aktivnosti korisnika sustava			0,00					
		5.10	osigurati primjenu kontrola koje sprječavaju ili otkrivaju korištenje poznatih ili sumnjivih zlonamjernih web stranica. Filter je moguće ostvariti primjenom liste zabranjenih kategorija ili imena domena, ili primjenom liste dozvoljenih kategorija ili imena domena, ovisno o apetitu subjekta za rizik te poslovnim potrebama.	OBVEZNO	DA	NAD-005: Filtriranje pristupa zlonamjernim web stranicama			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
		5.11	smanjiti potencijalnu površinu izloženosti subjekta kibernetičkim napadima: -identifikacijom i ograničavanjem servisa koji su javno izloženi/dostupni putem Interneta (primjerice web stranice, e-pošta, VPN ulazne točke, nadzorne konzole, RDP ili SSH servisi za udaljenu administraciju, SFTP, SMB i sličnih servisa za razmjenu datoteka, i dr.) -smanjenjem broja administratorskih i visoko privilegiranih korisničkih računa -blokiranjem pristupa javno dostupnim servisima s TOR mreže i poznatih anonimizacijskih VPN servisa -ograničavanjem izravnog pristupa Internet poslužiteljima, ukoliko je moguće.	OBVEZNO	DA	NAD-006: Ograničavanje javno izloženih servisa			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						SKM-008: Blokiranje pristupa iz anonimizacijskih mreža			0,00					
						DID-010: Upravljanje i politike korištenja privilegiranih računa			0,00					
6	Osiguravanje kibernetičke sigurnosti mreže	6.1	definirati i uspostaviti, sukladno svojoj mrežnoj arhitekturi i izloženosti javnim mrežama, obavezne mjere zaštite mreže te pritom razmotriti adekvatne mjere poput korištenje vatrozida, virtualne privatne mreže (VPN), mrežnog pristupa uz stalnu primjenu principa nultog povjerenja (zero trust – „svi su nepouzdani"), sigurnih mrežnih protokola za bežičnu mrežu, odvajanje mreža različitih namjena, sukladno kritičnosti podataka ili prioritetu pojedinih mrežnih segmenata (primjerice uredska mreža, nadzorna mreža, produkcija, proizvodnja, gosti itd.)	OBVEZNO	DA	POL-007: Uspostava obaveznih mjera zaštite mreže	4	4	4,00	4,00	4,00	4,00	4,06	
		6.2	osigurati da obavezne mjere zaštite mreže osiguravaju zaštićeni prijenos kritičnih podataka te autorizaciju i kontrolu korištenja mreža i mrežno dostupnih resursa. Primjerice, subjekt će osigurati korištenje sigurnih inačica protokola kao što su HTTPS i sFTP, pristup mreži samo za ovlaštene pojedince ili uređaje (autorizacija može biti utemeljena na provjerenom digitalnom identitetu pojedinca, provjerenom digitalnom identitetu uređaja, oboje ili gdje drugačije nije moguće lokacijom spajanja ukoliko se provodi autorizacija pristupa lokaciji, primjerice čuvani uredski prostor ili podatkovni centar).	OBVEZNO	DA	NAD-008: Sigurni mrežni protokoli za prijenos podataka	5	4	4,50	4,50	3,00	3,75		
						DID-008: Autorizacija korištenja mrežnih resursa	4	2	3,00					
		6.3	svake godine provesti sveobuhvatan pregled svih definiranih mjera zaštite mreže kako bi se osiguralo da su one i dalje učinkovite i relevantne. Ovaj pregled uključuje procjenu trenutnih kibernetičkih prijetnji, ranjivosti i promjena u poslovnom okruženju koje bi mogle utjecati na uspostavljene mjere zaštite. Na temelju rezultata pregleda, provodi se ažuriranje tehničkih mjera zaštite kako bi se odgovorilo na nove izazove i rizike, osiguravajući stalnu usklađenost s najboljim praksama i zahtjevima. Svi rezultati i promjene koje se predlažu moraju se dokumentirati i odobriti od strane osoba odgovornih za provedbu mjera.	OBVEZNO	DA	NAD-014: Godišnji pregled i ažuriranje mjera zaštite mreže	5	3	4,00	5,00	3,00	4,00		
		6.4	implementirati mehanizme praćenja odlaznog i dolaznog mrežnog prometa u svrhu smanjenja rizika od kibernetičkog napada te definirati metode filtriranja nepoželjnog mrežnog prometa u smislu prepoznavanja potencijalnih indikatora kompromitacije. Ovo uključuje postavljanje odgovarajućih alata za praćenje i analizu mrežnog prometa koji omogućuju identifikaciju i automatsko blokiranje potencijalno opasnih aktivnosti. Također, subjekt mora definirati i primijeniti metode filtriranja nepoželjnog mrežnog prometa, poput upotrebe sustava za otkrivanje i sprječavanje napada (IDS/IPS) i drugih sigurnosnih rješenja. Svi implementirani mehanizmi i metode filtriranja moraju biti redovito revidirani i ažurirani kako bi se održala visoka razina sigurnosti mreže.	OBVEZNO	DA	NAD-009: Filtriranje nepoželjnog mrežnog prometa	5	4	4,50	5,00	4,00	4,50		
		6.5	implementirati tehničke mehanizme detekcije anomalija u mreži temeljene ili na odstupanju od tipičnog mrežnog prometa ili na odstupanju od interno definiranih pravila.	DOBROVOLJNO	NE	NAD-002: Implementacija sustava za nadzor aktivnosti na informacijskim sustavima u stvarnom vremenu			0,00	#DIV/0!	#DIV/0!	#DIV/0!		
						NAD-003: Postavljanje automatskih alarma za detekciju prijetnji			0,00					
						NAD-009: Filtriranje nepoželjnog mrežnog prometa			0,00					
						DID-001: Uspostava i upravljanje jedinstvenim			0,00					

E14 SREDNJA

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

#	MJERA	OCJENA	RAZINA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	2,70	OSNOVNA
2	Upravljanje programskom i sklopovskom imovinom	3,00	OSNOVNA
3	Upravljanje rizicima	2,00	OSNOVNA
4	Sigurnost ljudskih potencijala i digitalnih identiteta	1,94	OSNOVNA
5	Osnovne prakse kibernetičke higijene	3,79	OSNOVNA
6	Osiguravanje kibernetičke sigurnosti mreže	4,06	SREDNJA
7	Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima	2,00	OSNOVNA
8	Sigurnost lanca opskrbe	2,00	OSNOVNA
9	Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava	1,83	OSNOVNA
10	Kriptografija	3,25	OSNOVNA
11	Postupanje s incidentima	2,00	OSNOVNA
12	Kontinuitet poslovanja i upravljanje kibernetičkim krizama	4,10	OSNOVNA
13	Fizička sigurnost	2,17	OSNOVNA
#	UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	2,68	



UVOD | OSNOVNA | SREDNJA | NAPREDNA | SAŽETAK | TREND | IZJAVA

Ready

E41

RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	OSNOVNA

NAPOMENA: Prilikom prve samoprocjene kalkulator će izračunati trend podizanja razine zrelosti kibernetičke sigurnosti, ali se ne uzima u obzir.

RAZINA MJERE	PRAG ZA UTVRĐIVANJE TRENDA
Osnovna	≥ 109
Srednja	≥ 58
Napredna	≥ 15

TREND PODIZANJA RAZINE ZRELOSTI KIBERNETIČKE SIGURNOSTI	
Bodovi ostvareni ispunjavanjem mjera iz više razine	24,36
Bodovi ostvareni ispunjavanjem dobrovoljnih podskupova mjera	3
UKUPNI BODOVI TRENDA PODIZANJA RAZINE ZRELOSTI	**13,68**

MJERE IZ VIŠE RAZINE			
#	MJERA	SREDNJA	NAPREDNA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima		
2	Upravljanje programskom i sklopovskom imovinom		
3	Upravljanje rizicima		
4	Sigurnost ljudskih potencijala i digitalnih identiteta		
5	Osnovne prakse kibernetičke higijene		
6	Osiguravanje kibernetičke sigurnosti mreže	16,24	
7	Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima		
8	Sigurnost lanca opskrbe		
9	Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava		
10	Kriptografija		
11	Postupanje s incidentima		
12	Kontinuitet poslovanja i upravljanje kibernetičkim krizama		
13	Fizička sigurnost		
#	TEŽINSKI FAKTOR	1,5	2
#	UKUPNO	24,36	0,00
#	BODOVI OSTVARENI ISPUNJAVANJEM MJERA IZ VIŠE RAZINE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	24,36	

OSNOVNA RAZINA - DOBROVOLJNI PODSKUPOVI MJERA			
#	MJERA	DOBROVOLJNI PODSKUPOVI MJERE	OCJENA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.5	/
		1.6	/
		1.8	3,00
		1.9	/
		1.10	/
		1.11	/
2	Upravljanje programskom i sklopovskom imovinom	2.6	/
		2.7	/
		2.8	/
		2.9	/

SREDNJA RAZINA - DOBROVOLJNI PODSKUPOVI MJERA			
#	MJERA	DOBROVOLJNI PODSKUPOVI MJERE	OCJENA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	1.10	/
		1.11	/
2	Upravljanje programskom i sklopovskom imovinom	2.8	/
		2.9	/

NAPREDNA RAZINA - DOBROV	
#	MJERA
1	Predanost i odgovornost osoba odgovornih za pr upravljanja kibernetičkim sigurnosnim rizicima
3	Upravljanje rizicima

UVOD OSNOVNA SREDNJA NAPREDNA SAŽETAK TREND IZJAVA

Ready 80%

B7

IZJAVA O SUKLADNOSTI
SPOSTAVLJENIH MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIM

PODACI O SUBJEKTU	
NAZIV	
ADRESA	
SEKTOR PODSEKTOR VRSTA SUBJEKTA	
SEKTOR GLAVNA POSLOVNA DJELATNOST	

SAMOPROCJENA KIBERNETIČKE SIGURNOSTI	
UTVRĐENA RAZINA KIBERNETIČKIH SIGURNOSNIH RIZIKA	
RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA KOJA JE UTVRĐENA OBVEZUJUĆOM	OSNOVNA
UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	2,68
UKUPNI BODOVI TRENDA PODIZANJA RAZINE ZRELOSTI	13,68
POPIS DOKUMENTACIJE	
IME, PREZIME I POTPIS OSOBE KOJA JE PROVELA POSTUPAK SAMOPROCJENE	

IZJAVA O SUKLADNOSTI
Rezultati provedene samoprocjene kibernetičke sigurnosti za subjekt pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti.

Hvala na pažnji