ZAVOD ZA SIGURNOST
INFORMACIJSKIH SUSTAVA

Smjernice za provedbu samoprocjene kibernetičke sigurnosti

Verzija: 1.0

Sadržaj

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.

- **Prilog C - Katalog kontrola:** sadrži kontrole za mjere i podskupove mjera upravljanja kibernetičkim sigurnosnim rizicima propisanih Uredbom, podjelu kontrola po kategorijama te postupak ocjenjivanja kontrola.

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

Obveznici primjene provedbe samoprocjene, sukladno Zakonu i Uredbi, prilikom provedbe samoprocjene dužni su se pridržavati pravila sadržanih u ovim Smjernicama.

U svrhu prilagodbe važećim izvorima prava te postizanja visoke razine kibernetičke sigurnosti, ZSIS će redovito, a najmanje jednom u dvije godine provoditi reviziju Smjernica te, prema potrebi, izvršiti nužne izmjene i dopune. Sve izmjene i dopune Smjernica stupaju na snagu prvoga dana nakon njihove službene objave na mrežnim stranicama ZSIS-a (www.zsis.hr), osim u iznimnim slučajevima kada je zbog opsega izmjena Smjernica i njihove svrhe potrebno omogućiti duži rok za implementaciju.

Provedba samoprocjene kibernetičke sigurnosti

Samoprocjenom se određuje stupanj usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima (u daljnjem tekstu: mjera) koji se nalaze u Prilogu II. Uredbe, kao i trend podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Važni subjekti i subjekti iz članka 47. Uredbe samoprocjenu provode najmanje jednom u dvije godine.

Ključni subjekti mogu provoditi samoprocjenu kao pripremu za provedbu revizije kibernetičke sigurnosti ili stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti iz članka 75. stavka 1. Zakona.

Stupanj usklađenosti uspostavljenih mjera temelji se na procjeni stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima u subjektu, a utvrđuje su temeljem bodovanja podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 44. stavka 1. i 2. Uredbe, koje subjekt provodi:

- kao obvezujuće (označene oznakom »A« u Prilogu II. Uredbe) ili
- obvezujuće pod uvjetima (označene oznakom »B« u Prilogu II. Uredbe).

Trend podizanja razine zrelosti kibernetičke sigurnosti utvrđuje se dodatnim bodovanjem podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 44. stavka 1. i 2. Uredbe, koje subjekt provodi na temelju mjere 3. „Upravljanje rizicima“ iz Priloga II. Uredbe, u smislu podizanja razine provedbe pojedinih:

- obvezujućih mjera (označene oznakom »A« u Prilogu II. Uredbe)
- obvezujućih pod uvjetima (označene oznakom »B« u Prilogu II. Uredbe),

kao i u smislu provedbe dobrovoljnih mjera iz članka 44. stavka 3. Uredbe (označene oznakom »C« u Prilogu II. Uredbe).

U svrhu provođenja postupka bodovanja uvodi se Kalkulator za samoprocjenu kibernetičke sigurnosti (u daljnjem tekstu: Kalkulator).

Pomoću Kalkulatora izračunava se konačni rezultat samoprocjene, odnosno ukupni bodovi stupnja usklađenosti mjera i ukupni bodovi trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta. Ispunjeni Kalkulator pohranjuje se na infrastrukturi koja je pod kontrolom subjekta koji vrši samoprocjenu. Pristup osjetljivim podacima iz Kalkulatora trebao bi biti dopušten samo ovlaštenim osobama. Razmjena podataka iz Kalkulatora treba biti kontrolirana i autorizirana, osiguravajući pristup samo nadležnima za proces samoprocjene i nadzora.

Za provedbu samoprocjene subjekt je prema članku 56. Uredbe dužan odrediti svoje zaposlenike ili vanjske suradnike koji posjeduju najmanje:

- relevantna znanja iz implementacije međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti,
- potvrdu o završenoj vanjskoj ili internoj edukaciji za internog revizora po nekoj od relevantnih međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti i
- jednu godinu radnog iskustva u okviru provođenja sličnih vrsta interne revizije u području mrežnih i informacijskih sustava odnosno kibernetičke sigurnosti.

Provođenjem samoprocjene subjekti stječu uvid u stanje svoje kibernetičke sigurnosti, omogućuju proaktivno upravljanje rizicima te unapređuju sposobnost obrane od potencijalnih kibernetičkih prijetnji.

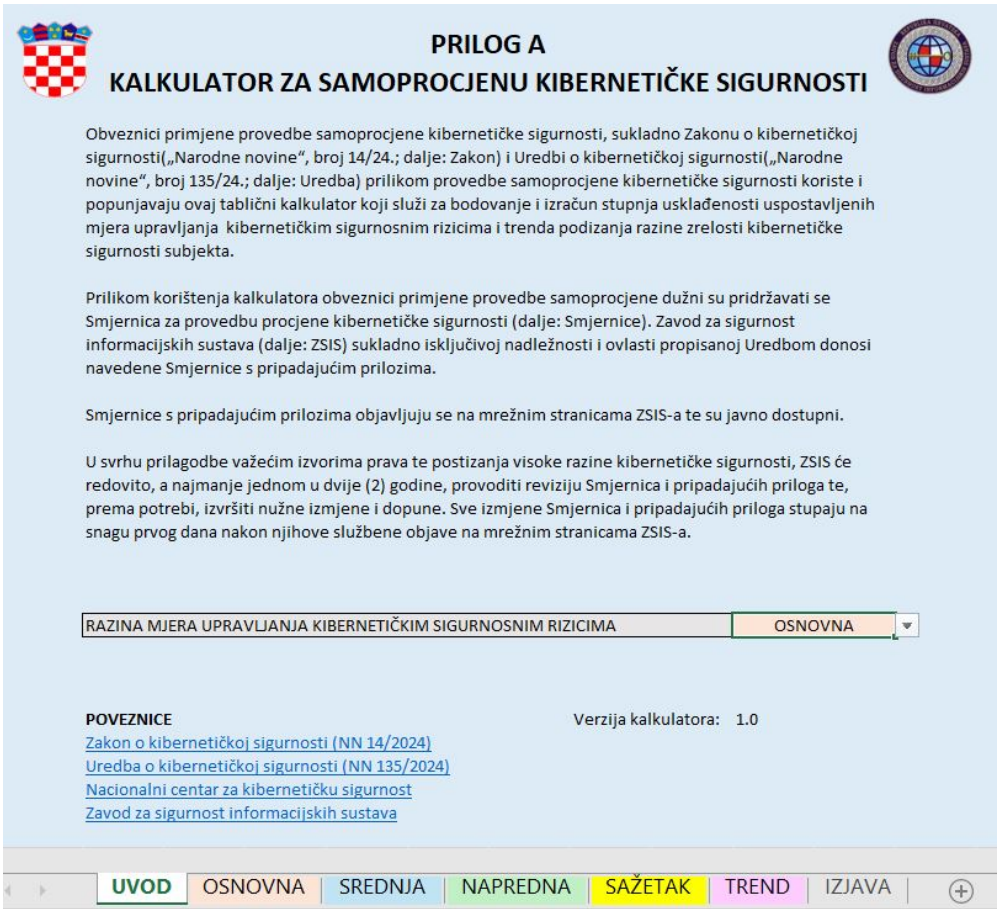
Izgled kalkulatora samoprocjene kibernetičke sigurnosti

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.

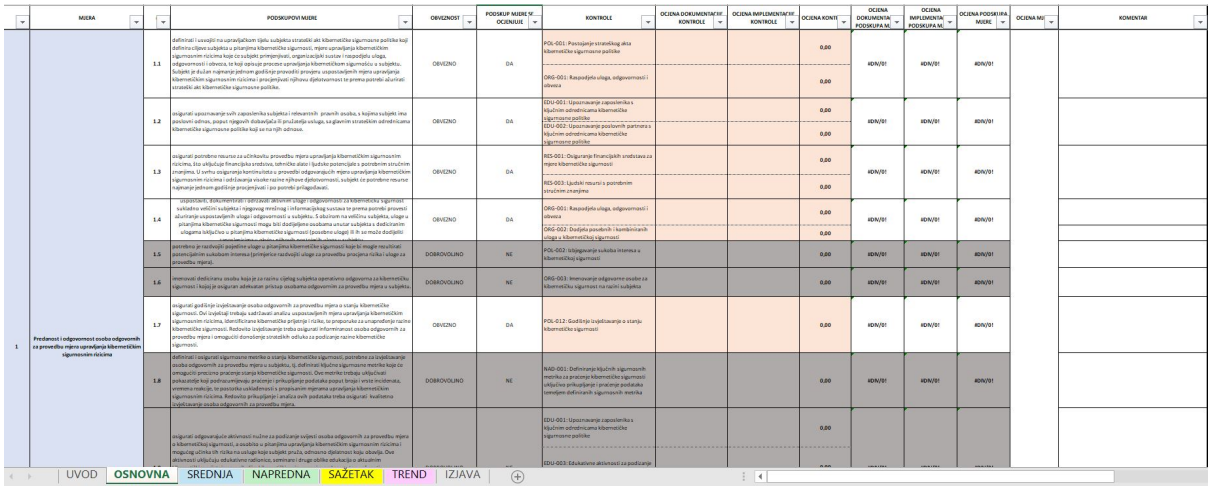
Slika 1 Prikaz trake kartica radnih listova

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.



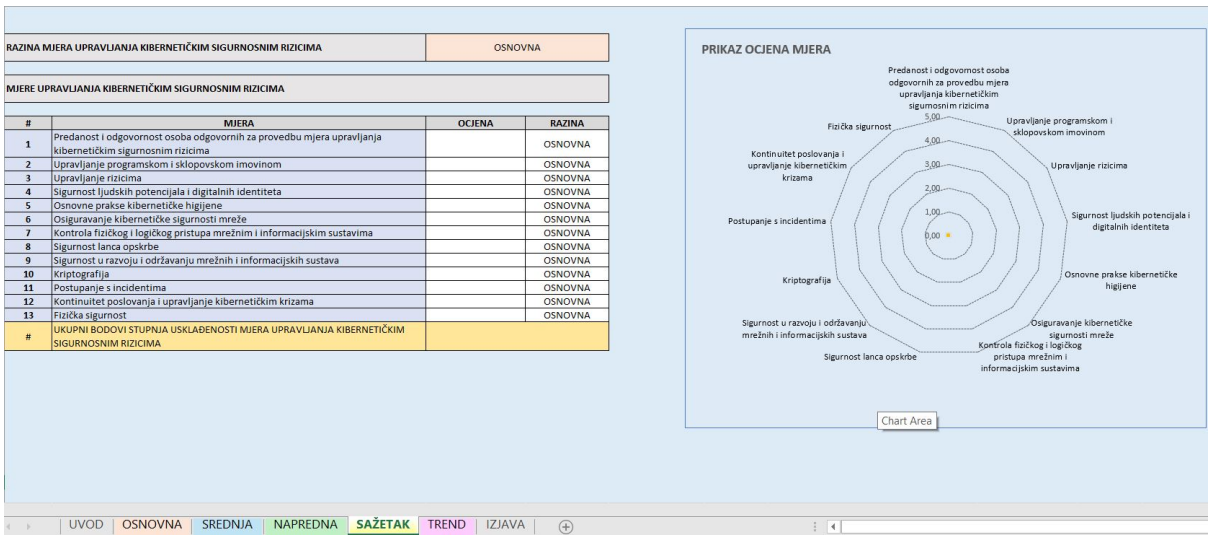
Slika 2 Radni list „Uvod“

Svaka razina mjera ima svoj radni list u kalkulatoru naziva: osnovna, srednja i napredna. Svaki radni list koji se odnosi na pojedinu razinu mjere obuhvaća mjere koje sadrže obvezne, obvezne pod uvjetom i dobrovoljne podskupove mjera s pripadajućim kontrolama za ocjenjivanje. Ostali elementi koji se nalaze na navedenim radnim listovima se odnose na ocjene; ocjena dokumentacije i implementacije kontrola, te ocjena pojedine kontrole, ocjene dokumentacije i implementacije podskupa mjere, ukupna ocjena podskupa mjere i ocjena mjere. Uz ocjene, u stupcu „KOMENTAR“, osobi koja provodi samoprocjenu dana je mogućnost bilježenja zapažanja tijekom postupka samoprocjene.



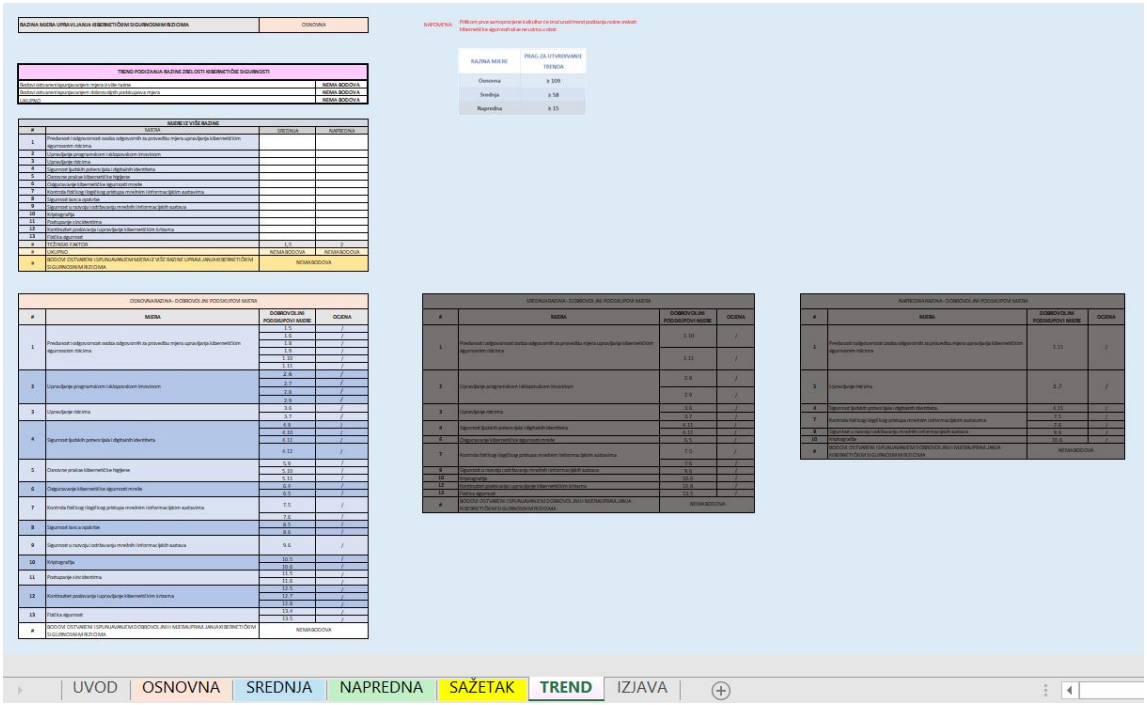
Slika 3 Prikaz dijela radnog lista „Osnovna“

Na radnom listu „Sažetak“ prikazana je razina mjere koja je odabrana u padajućem izborniku na radnom listu „Uvod“. Ispod padajućeg izbornika nalazi se tablica sa svim ocjenama mjera po razinama mjere te ukupni bodovi stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima. Pored tablice s ukupnom ocjenom je smješten radar graf koji vizualno prikazuje ostvarene ocjene subjekta po svim mjerama.



Slika 4 Radni list „Sažetak“

Radni list „Trend“ sadrži tablicu s ukupnim zbrojem bodova trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta. Radni list sadrži i tablicu u kojoj su prikazane mjere koje su ocjenjivane iz više razine mjera s njihovim postignutim bodovima i njihov zbroj bodova, kao i tri tablice koje se odnose na dobrovoljne podskupove mjera. Svaka razina mjere koja je utvrđena nacionalnom procjenom rizika ima zasebnu tablicu u kojoj su navedene mjere s pripadajućim dobrovoljnim podskupovima mjera i njihovim ocjenama koje je subjekt odlučio primjeniti.



Slika 5 Radni list "Trend"

Na radnom listu „Izjava“ nalazi se izjava o sukladnosti koja je ujedno Prilog IV. Uredbe. Izjavu o sukladnosti važni subjekti ispunjavaju nakon provedene samoprocjene, ako rezultati pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom i Uredbom.

IZJAVA O SUKLADNOSTI
USPOSTAVLJENIH MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

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	3,40
UKUPNI BODOVI TRENDA PODIZANJA RAZINE ZRELOSTI	NEMA BODOVA
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.	
IME, PREZIME I POTPIS OSOBE ODGOVORNE ZA UPRAVLJANJE MJERAMA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	

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

Slika 6 Radni list „Izjava“ s izjavom o sukladnosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima

Izračun stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima

Stupanj usklađenosti uspostavljenih dokumentiranih i implementiranih mjera propisanih Uredbom utvrđuje se temeljem bodovanja podskupova mjera koje subjekt provodi kao obvezujuće u okviru jedne od tri razine mjera (osnovna, srednja, napredna) kojoj subjekt pripada.

Na radnom listu „Uvod“, potrebno je na padajućem izborniku odabrati razinu mjere koja je dodijeljena subjektu, te nakon odabira otvoriti radni list odabrane razine mjere (osnovna, srednja, napredna). Ako je subjekt lokalnom procjenom rizika utvrdio višu razinu mjera od one koja je utvrđena nacionalnom procjenom rizika (za jednu ili više mjera), tada se pojedine mjere, te shodno tome podskupovi mjera, ocjenjuju u radnom listu za razinu koju je subjekt utvrdio.

Podskupove mjera koje je subjekt dužan provoditi u okviru određene razine mjere kao obvezujuće pod uvjetima opisanim u razradi mjere iz članka 43. Uredbe, uključuje u izračun na način da u padajućem izborniku stupca „podskup mjere se ocjenjuje“ odabere opciju *DA*.

#	PODSKUPOVI MJERE	OBVEZNOST	PODSKUP MJERE SE OCJENJUJE	KONTROLE
3.8	upravljanje rizicima integrirati kao dio upravljanja rizicima na razini poslovanja subjekta (ERM). UVJET: Mjera 3.8. je obvezujuća za subjekt koji ima uspostavljene procese upravljanja rizicima na razini poslovanja subjekta te se u tom slučaju upravljanje rizikom, opisano u okviru podskupova mjere 3. (3.1. do. 3.7.), provodi integrirano, kao dio uspostavljenog procesa upravljanja rizicima poslovanja subjekta. Ako subjekt nema uspostavljene procedure upravljanja rizicima na razini poslovanja subjekta, uspostavlja mjeru 3. (3.1. do 3.7.) kao novi poslovni proces	OBVEZUJUĆE POD UVJETOM	DA	RIZ-012: Integracija upravljanja kibernetičkim rizicima u upravljanje rizicima poslovanja (ERM)

Slika 7 Prikaz podskupa mjere koji je obvezujući pod uvjetom

Sukladno uvjetima koji su sadržani u prilogu Katalog kontrola (u daljnjem tekstu: Prilog C), ocjenjuje se usklađenost dokumentiranih i implementiranih kontrola i pritom se upisuju ocjene u stupce ocjena dokumentacije kontrole i ocjena implementacije kontrole. Vrijednosti u ostalim stupcima automatski izračunava Kalkulator.

Izračun se vrši temeljem elemenata koji su prikazani u tablici na radnom listu („Osnovna“, „Srednja“ ili „Napredna“) kako slijedi.

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

$$K = \frac{DK + IK}{2} \#(1.1)$$

K – ocjena kontrole

DK – ocjena dokumentacije kontrole

IK – ocjena implementacije kontrole

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

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

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.

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

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).

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

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).

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

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 subjekt ocjenjivao mjere po višoj razini koja je utvrđena lokalnom procjenom rizika, onda se moraju zadovoljiti bodovni pragovi ocjena koji su definirani tom razinom mjere.

U slučaju da je ocjena kontrole zadovoljila definirani bodovni prag, pozadinska boja polja s ocjenom u kalkulatoru će se promijeniti u zelenu boju. Ako ocjena nije ostvarila zadani bodovni prag, pozadinska boja polja s ocjenom će se promijeniti u crvenu boju, što ukazuje da kontrola nije zadovoljena.

Model ocjenjivanja podskupova mjera bazira se na ispunjavanju uvjeta pojedinačnih kontrola te uvjeta ukupne ocjene.

Primjeri slučajeva neispunjavanja uvjeta :

Primjer 1: bodovni prag jedne ili više kontrola nije zadovoljen te iz tog razloga mjera iz podskupa mjere nije zadovoljena, bez obzira što je bodovni prag za prolaz mjere iz podskupa mjere zadovoljen.

KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJE	OCJENA IMPLEMENTACIJE PODSKUPA MJE	OCJENA PODSKUPA MJERE
ORG-001: Raspodjela uloga, odgovornosti i obveza	5	5	5,00	3,33	3,33	3,33
ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti	3	3	3,00			
ORG-005: Implementacija prava pristupa prema načelima poslovne potrebe i minimalnih ovlaštenja	2	2	2,00			

Primjer 2: pojedinačne kontrole su zadovoljene, međutim prosječna ocjena svih kontrola ne ostvaruje zadani ukupni bodovni prag pa uvjet za prolaz na razini podskupa mjere nije zadovoljen.

KONTROLE	OCJENA DOKUMENTACIJE KONTROLE	OCJENA IMPLEMENTACIJE KONTROLE	OCJENA KONTROLE	OCJENA DOKUMENTACIJE PODSKUPA MJ	OCJENA IMPLEMENTACIJE PODSKUPA MJ	OCJENA PODSKUPA MJERE
INV-004: Dokumentacija, revizija i ažuriranje inventara kritične imovine	3	3	3,00	3,00	2,50	2,75
RIZ-001: Procjena rizika za kritičnu imovinu temeljem fizičkih prijetnji	3	2	2,50			
RIZ-002: Procjena rizika za kritičnu imovinu temeljem kibernetičkih prijetnji	3	2	2,50			
RIZ-003: Procjena rizika od trećih strana za kritičnu imovinu subjekta	3	3	3,00			

Na radnom listu naziva „Sažetak“ nalazi se izbornik u kojem subjekt odabire razinu mjere koju je ispunio sukladno nacionalnoj procjeni rizika. Preostale elemente automatski unosi Kalkulator na temelju unosa potrebnih vrijednosti na ispunjenom radnom listu razine mjere. U slučaju da su neke mjere ocjenjivane po višoj razini koja je utvrđena lokalnom procjenom

rizika, subjekt u stupcu „RAZINA“ u padajućem izborniku označava razinu po kojoj je mjera ocjenjivana.

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

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

Slika 8 Prikaz padajućeg izbornika u stupcu „RAZINA“ s odabirom razine na mjeri 1

Ukupni bodovi stupnja usklađenosti mjera upravljanja kibernetičkim rizicima (U) određuju se kao aritmetička sredina ocjena svih mjera (M).

$$U = \frac{\sum_{i=1}^{n} Mi}{n},\ n \in \mathrm{N\#}(1.6)$$

U - stupanj usklađenosti mjera upravljanja kibernetičkim rizicima

M - ocjena mjere

Nakon izračuna ukupnih bodova stupnja usklađenosti mjera upravljanja kibernetičkim rizicima, uz tablicu će biti prikazan radar graf. U središnjim točkama grafa prikazane su dobivene ocjene, dok su na osima sve ocjenjivane mjere. Ovaj grafički prikaz omogućava intuitivnu vizualnu analizu rezultata, olakšavajući usporedbu različitih vrijednosti mjera. Također omogućava i brzo prepoznavanje područja u kojima je kibernetička sigurnost subjekta snažnija, kao i onih koja zahtijevaju poboljšanja.

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	razviti 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

Ocjene se unose u tablici (ocjena dokumentacije kontrole i ocjena implementacije kontrole) na radnom listu koji označava razinu mjere koja je utvrđena nacionalnom procjenom rizika. Nakon unosa, idući elementi u stupcima se izračunavaju automatski, kao i za obvezne podskupove mjera. Te vrijednosti će biti prikazane na radnom listu „Trend“ u tablici s dobrovoljnim podskupovima mjera određene razine. U tablici se prikazuju ocjene dobrovoljnih podskupova mjera koji su ocjenjivani te ukupni bodovi koji predstavljaju zbroj ocjena dobrovoljnih podskupova mjera. Navedena tablica koja je prikazana ovisi o odabranoj razini mjera na radnome listu „Uvod“, a ostale sive tablice s dobrovoljnim podskupovima mjera ne ulaze u izračun.

Ako odabrani dobrovoljni podskup mjere ne zadovoljava bodovni prag koji je definiran u Prilogu B, taj dobrovoljni podskup mjere subjekt će isključiti iz ocjenjivanja kako ne bi utjecao na izračun trenda.

U slučaju da je subjekt odlučio podignuti razinu provedbe pojedinih obvezujućih mjera, mjere se ocjenjuju na radnom listu koji je namijenjen izračunu za višu razinu (radni list naziva „Srednja“ ili „Napredna“). Izračun se provodi na isti način kao i izračun stupnja usklađenosti mjera po razini koja je utvrđena nacionalnom procjenom rizika. Ovaj postupak se ne uzima u obzir, ako je subjekt dužan zadovoljiti naprednu razinu mjera. Vrijednosti unesene na radnom listu više razine prilikom unosa se automatski preslikavaju u tablicu „MJERE IZ VIŠE RAZINE“ na radnom listu „Trend“. Ocjene koje su ostvarene u višoj razini se zbrajaju, pri čemu se njihov zbroj množi s odgovarajućim težinskim faktorom čija vrijednost ovisi o razini koja je utvrđena nacionalnom procjenom rizika i razini na koju se podiže provedba pojedinih obvezujućih mjera. Tim postupkom se dobiva ukupna ocjena za ocjenjivane mjere iz više razine.

Primjeri vrijednosti težinskih faktora :

Primjer 1: <u>Subjekt provodi mjere po osnovnoj razini</u>

U ovom slučaju subjekt može podići razinu provedbe pojedinih obvezujućih mjera na srednju i/ili naprednu razinu. Zbroj ocjena mjera koje su ocjenjivane prema uvjetima za srednju razinu množi se s težinskim faktorom u vrijednosti 1,5, a zbroj onih koje su ocjenjivane sukladno zahtjevima za naprednu razinu množi se s 2,0.

Primjer 2: <u>Subjekt provodi mjere po srednjoj razini</u>

U ovom slučaju subjekt može podići razinu provedbe pojedinih obvezujućih mjera na naprednu razinu. Stupac „SREDNJA“ u tablici „MJERE IZ VIŠE RAZINE“ je zatamnjen, s obzirom da u izračun ulaze ocjene samo iz napredne razine. Zbroj ocjena mjera koje su ocjenjivane prema uvjetima za naprednu razinu množi se s težinskim faktorom 1,5.

Trend podizanja razine zrelosti kibernetičke sigurnosti subjekta (T) određuje se na temelju bodova ostvarenih kroz primjenu dobrovoljnih podskupova mjera i bodova ostvarenih primjenom mjera iz više razine.

Ukupna ocjena u trendu dobiva se kao zbroj dvaju elemenata:

- Ocjene dobrovoljnih podskupova mjera – ukupan zbroj ocjena svih primijenjenih dobrovoljnih podskupova mjera i
- Ocjene unaprijeđenih mjera koje obuhvaćaju podskupove mjera - ukupan zbroj ocjena mjera koje su unaprijeđene na višu razinu, pri čemu se njihov doprinos množi odgovarajućim težinskim faktorom ovisno o razini unapređenja.

$$T = \sum_{j=1}^{m} D_j + \sum_{k=1}^{K} \left(\sum_{i=1}^{n_k} V_{k,i} \right) * F_k \#(2.1)$$

T – trend podizanja razine zrelosti kibernetičke sigurnosti

D – ocjena j-tog dobrovoljnog podskupa mjere

m – ukupni broj dobrovoljnih podskupova mjere

Vk,i – ocjena i-te mjere iz podskupa mjere unutar k-te mjere koja je unaprijeđena na višu razinu

nk – broj ocjena unutar k-tog podskupa unaprijeđenih mjera

K – broj mjera koje su unaprijeđene

Fk – težinski faktor povećanja razine mjere

Ukupan rezultat trenda prikazuje se u tablici „TREND PODIZANJA RAZINE ZRELOSTI“ na radnom listu „Trend“.

U svrhu provedbe bodovanja, za sve tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima definira se broj bodova potreban za utvrđivanje trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta. Broj bodova za utvrđivanje trenda podrazumijeva ukupnu ocjenu u trendu koja obuhvaća zbroj ukupnog zbroja ocjena svih primijenjenih dobrovoljnih podskupova mjera i ukupnog zbroja ocjena mjera koje su unaprijeđene na višu razinu. Za svaku razinu mjere određen je broj bodova koji subjekt treba postići kako bi se utvrdio trend.

Za utvrđivanje trenda za određenu razinu sigurnosti potrebno je ispuniti uvjete kako je prikazano u sljedećoj tablici:

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

Sukladno gornjoj tablici, da bi subjektu koji provodi osnovnu razinu mjera bio utvrđen trend, potrebno je ostvariti minimalno 109 bodova u ukupnom rezultatu trenda. Subjekt koji provodi srednju razinu mjera, treba postići minimalno 58 bodova u trendu za utvrđivanje trenda, dok subjektu koji provodi naprednu razinu mjera, trend se utvrđuje ako ostvari minimalno 15 bodova u trendu.

Ako ukupni rezultat trenda (zbroj ukupnog zbroja ocjena svih primijenjenih dobrovoljnih podskupova mjera i ukupnog zbroja ocjena podignutih mjera na višu razinu) pokaže da je subjekt za određenu razinu mjere ostvario manje bodova od potrebnog zbroja bodova, smatra se da trend nije utvrđen.

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.

Popis referentnih dokumenata

Zakon o kibernetičkoj sigurnosti (NN 14/2024)
Uredba o kibernetičkoj sigurnosti (NN 135/2024)
Prilog A – Kalkulator za samoprocjenu kibernetičke sigurnosti
Prilog B – Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima
Prilog C – Katalog kontrola

RAVNATELJ

Predrag Božinović
Ovaj dokument je elektronički ovjeren.

KLASA: 005-13/25-02/01
URBROJ: 509-30-02/40-25-19
U Zagrebu, 23. svibnja 2025.