



HRVATSKA
REVIZORSKA
KOMORA

Stručno savjetovanje ovlaštenih revizora u organizaciji Hrvatske revizorske komore

za 2024. godinu



HRVATSKA
REVIZORSKA
KOMORA

Primjena nove regulative u provedbi IT revizije (DORA i NIS 2)

Vedran Benić

Senior Information Security Consultant

Span d.d.

Napomena

Sadržaj ovog prezentacijskog materijala je informativnog karaktera. Upotreba prezentacijskog materijala ne oslobađa korisnika od poduzimanja potrebnih mjera predostrožnosti prije njegove uporabe, odnosno ne oslobađa korisnika od obveze primjene izvornih zakonskih odredbi i pravila struke, s toga se Hrvatska revizorska komora i autor prezentacijskog materijala ne mogu smatrati odgovornima prilikom uporabe ili u vezi s uporabom sadržaja koji se nalazi u prezentacijskom materijalu.

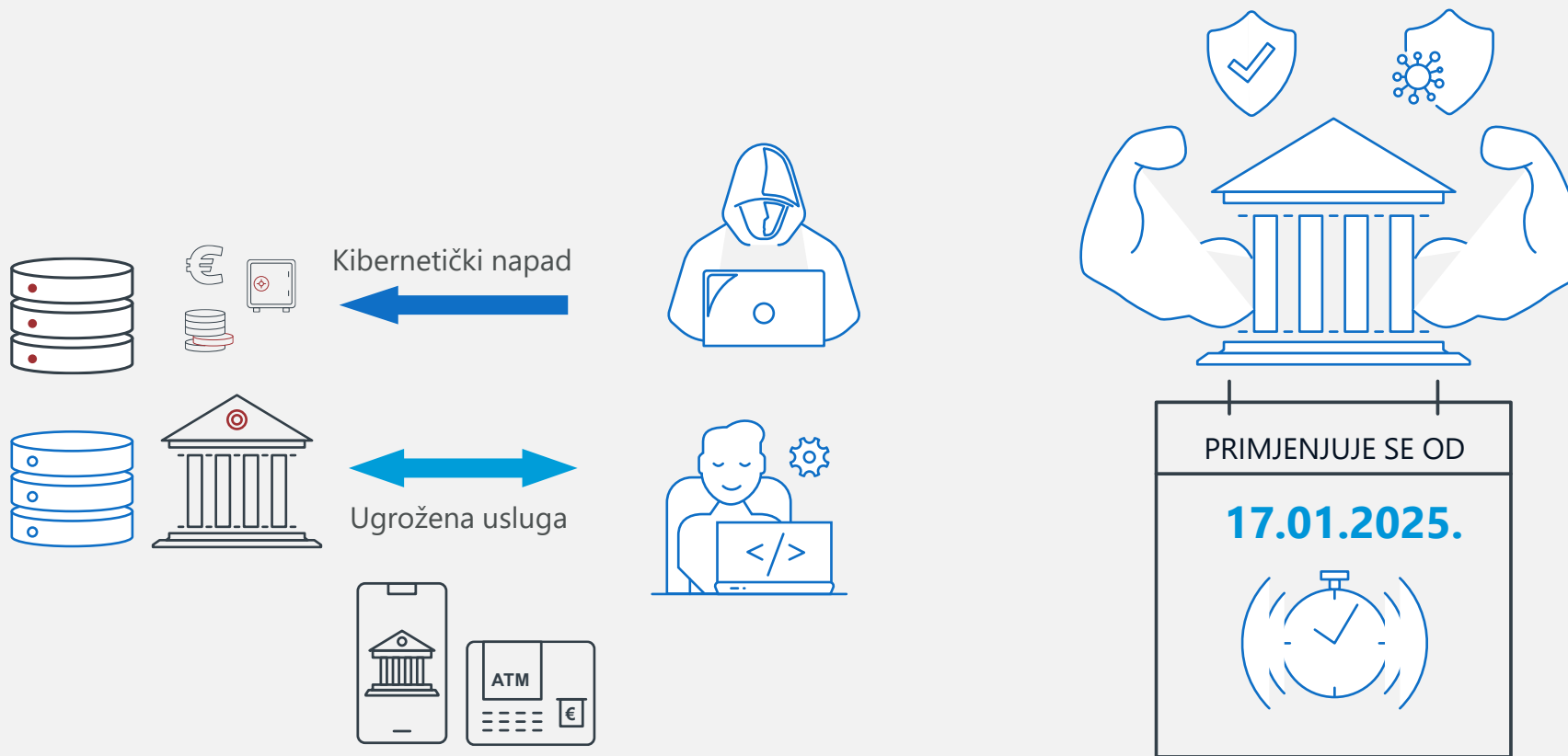
Uporaba sadržaja i podataka iz ovog prezentacijskog materijala dopuštena je pod uvjetom navođenja izvora podataka, osim u slučajevima kada je naznačeno drugačije.

Sadržaj

1. Zašto DORA?
2. NIS 2 – Zakon o kibernetičkoj sigurnosti (ZKS)
3. Zašto NIS 2?
4. DORA vs NIS 2
5. DORA - Polje primjene
6. NIS 2 – Ključni i važni subjekti
7. Mjere kibernetičke sigurnosti
8. DORA i NIS 2 – Upravljanje incidentima
9. DORA - Pružatelji ICT usluga
10. DORA i NIS 2 - Nadzor i kazne
11. NIS 2 (ZKS) – Vremenski okvir
12. DORA i NIS 2 - revizija



Zašto DORA?



NIS 2 – Zakon o kibernetičkoj sigurnosti (ZKS)



NIS 2 Direktiva



Izravna
primjena u
RH



Implementacija
kroz nacionalni
zakon



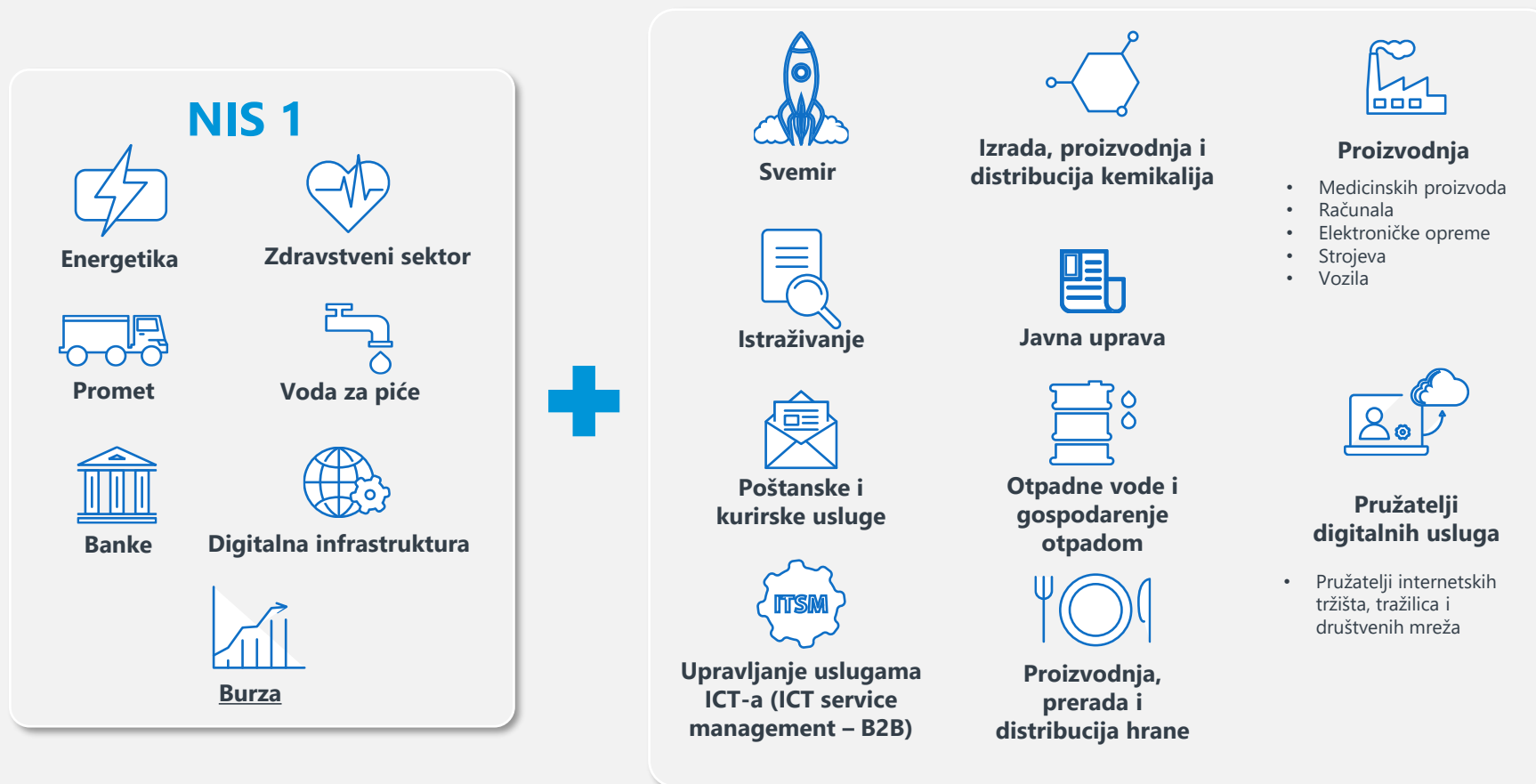
**Zakon o kibernetičkoj
sigurnosti (NN br.
14/24)**



**Stupio na snagu
15.02.2024.**



Zašto NIS 2?



DORA vs NIS 2

DORA	NIS 2
Uredba (Regulation)	Direktiva (Directive)
Financijski subjekti i njihovi pružatelji ICT usluga	Ključni i važni subjekti (energetika, promet, bankarstvo , infrastruktura financijskog tržišta , zdravstvo, javni sektor, gospodarenje otpadom, poštanske usluge itd.)
Lex specialis	Lex generalis



DORA – polje primjene

1) kreditne institucije (HNB – lista);	2) institucije za platni promet (HNB – registar);	3) pružatelji usluga pružanja informacija o računu (HNB – registar);	4) institucije za elektronički novac (HNB – registar);	5) investicijska društva (HANFA – registar);	6) pružatelji usluga povezanih s kriptovalutama i izdavatelje tokena vezanih uz imovinu (HANFA – registar);
7) središnji depozitoriji vrijednosnih papira (SKDD - HANFA);	8) središnje druge ugovorne strane (SKDD- CCP Smart Clear d.d. - HANFA);	9) mjesta trgovanja (HANFA);	10) trgovinski repozitoriji (ESMA – lista);	11) upravitelji alternativnih investicijskih fondova (HANFA – lista);	12) društva za upravljanje (HANFA - lista);
13) pružatelji usluga dostave podataka (ESMA);	14) društva za osiguranje i društva za reosiguranje (HANFA - lista);	15) posrednici u osiguranju, posrednici u reosiguranju i sporedni posrednici u osiguranju (HANFA - lista);	16) institucije za strukovno mirovinsko osiguranje (EIOPA – registar);	17) agencije za kreditni rejting (ESMA - lista);	18) administratori ključnih referentnih vrijednosti (ESMA - registar);
19) pružatelji usluga skupnog financiranja (ESMA - registar);		20) sekuritizacijski repozitoriji (ESMA);		21) treće strane pružatelje IKT usluga.	



NIS 2 – KLJUČNI SUBJEKTI



1) Energetika



4) Burza



7) Otpadne vode



2) Promet



5) Zdravlje



8) Javna uprava



3) Banke



6) Voda za piće



9) Svemir

10) Digitalna infrastruktura

- Pružatelji središta za razmjenu internetskog prometa
- Pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva
- Registri naziva vršnih domena
- Pružatelji usluga podatkovnog centra
- Pružatelji mreže za isporuku sadržaja
- Pružatelji usluga povjerenja
- Pružatelji javnih elektroničkih komunikacijskih mreža
- Pružatelji javno dostupnih elektroničkih komunikacijskih usluga

11) Upravljanje uslugama ICT-a (B2B)

- Pružatelji upravljivih usluga
- Pružatelji upravljanih sigurnosnih usluga



+ 250 zaposlenika;

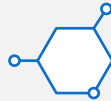
+ godišnji promet preko 50 milijuna EUR
ili ukupna godišnja bilanca preko 43 milijuna EUR)



NIS 2 – VAŽNI SUBJEKTI



1) Poštanske i kurirske usluge



3) Izrada, proizvodnja i distribucija kemikalija



2) Gospodarenje otpadom



4) Proizvodnja, prerada i distribucija hrane



5) Proizvodnja

- Medicinskih proizvoda
- Računala
- Elektroničke opreme
- Strojeva
- Vozila



6) Pružatelji digitalnih usluga

- Pružatelji internetskih tržišta, tražilica i društvenih mreža



7) Istraživanje

+ 50 zaposlenika;

+ godišnji promet preko **10 milijuna EUR** ili ukupna godišnja bilanca preko **10 milijuna EUR**



MJERE KIBERNETIČKE SIGURNOSTI



Upravljanje rizicima
(Risk management)



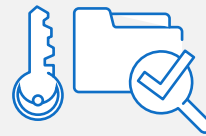
Sigurnost ICT operacija
(ICT operations security)



Mrežna sigurnost
(Network security)



Upravljanje ICT imovinom
(ICT asset management)



Enkripcija i kriptografija
(Encryption and cryptography)



Upravljanje ICT projektima i promjenama
(ICT Project and change management)



MJERE KIBERNETIČKE SIGURNOSTI



ICT kontinuitet poslovanja
(ICT business continuity)



Upravljanje identitetima
(Identity management)



Revizija i izvještavanje
(Review and reporting)



Kontrola pristupa
(Access control)



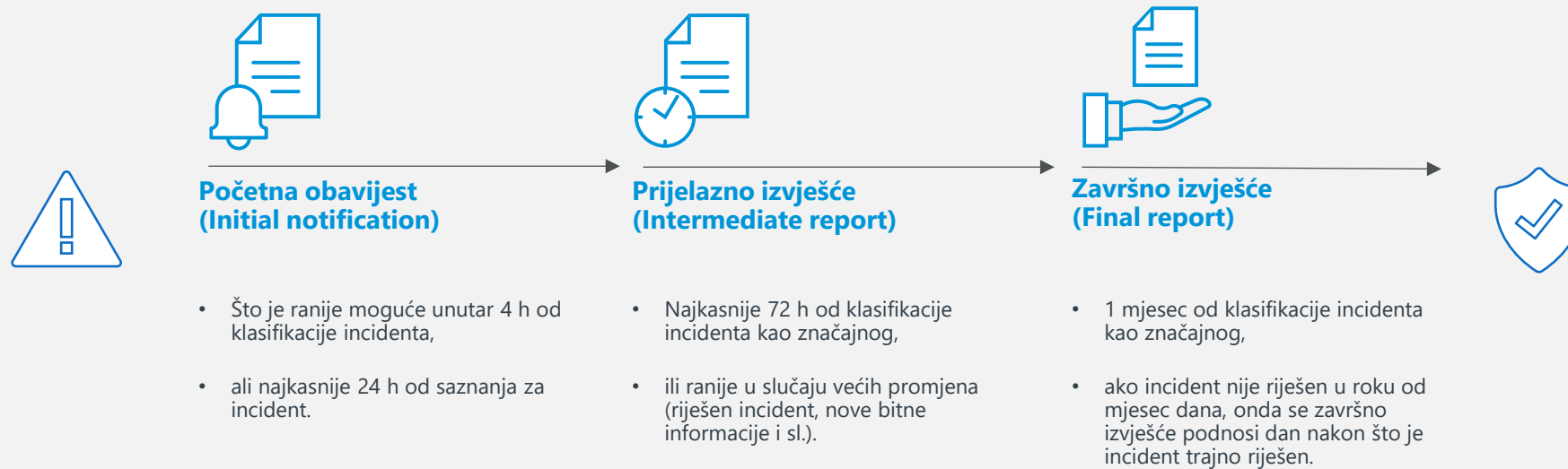
Politika ljudskih resursa
(Human resource policy)



Fizička sigurnost i sigurnost okruženja
(Physical and environmental security)



DORA – UPRAVLJANJE ICT INCIDENTIMA



NIS 2 - IZVJEŠĆIVANJE O (ZNAČAJNIM) INCIDENTIMA



DORA – PRUŽATELJI ICT USLUGA



DORA – NADZOR I KAZNE

Za ključne pružatelje ICT usluga

Visina penala?

1% prosječnog dnevnog svjetskog prometa.

Koliko često se određuje penal?

Svaki dan...

...ali **najviše 6 mjeseci** od obavijesti ključnom pružatelju ICT usluga o kršenju.

A što je sa financijskim subjektima?



NIS 2 – NADZOR I KAZNE

NADZOR

Ključni subjekti nasumične provjere, ne treba poseban razlog.

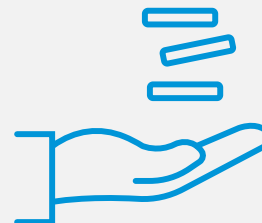
Važni subjekti dolazak u inspekciju tek nakon što postoji dokaz ili informacija o kršenju NIS 2 odredbi.



NOVČANE KAZNE

Ključni subjekti 10 000 000 EUR ili 2% ukupnog godišnjeg prometa

Važni subjekti 7 000 000 EUR ili 1,4% ukupnog godišnjeg prometa



NIS 2 – NADLEŽNA TIJELA

Autonomni sektori

- bankarstvo (Hrvatska narodna banka - **HNB**)
- infrastrukture financijskog tržišta (Hrvatska agencija za nadzor financijskih usluga - **HANFA**)
- zračni promet (Hrvatska agencija za civilno zrakoplovstvo – **HACZ**)

Polu-autonomni sektori

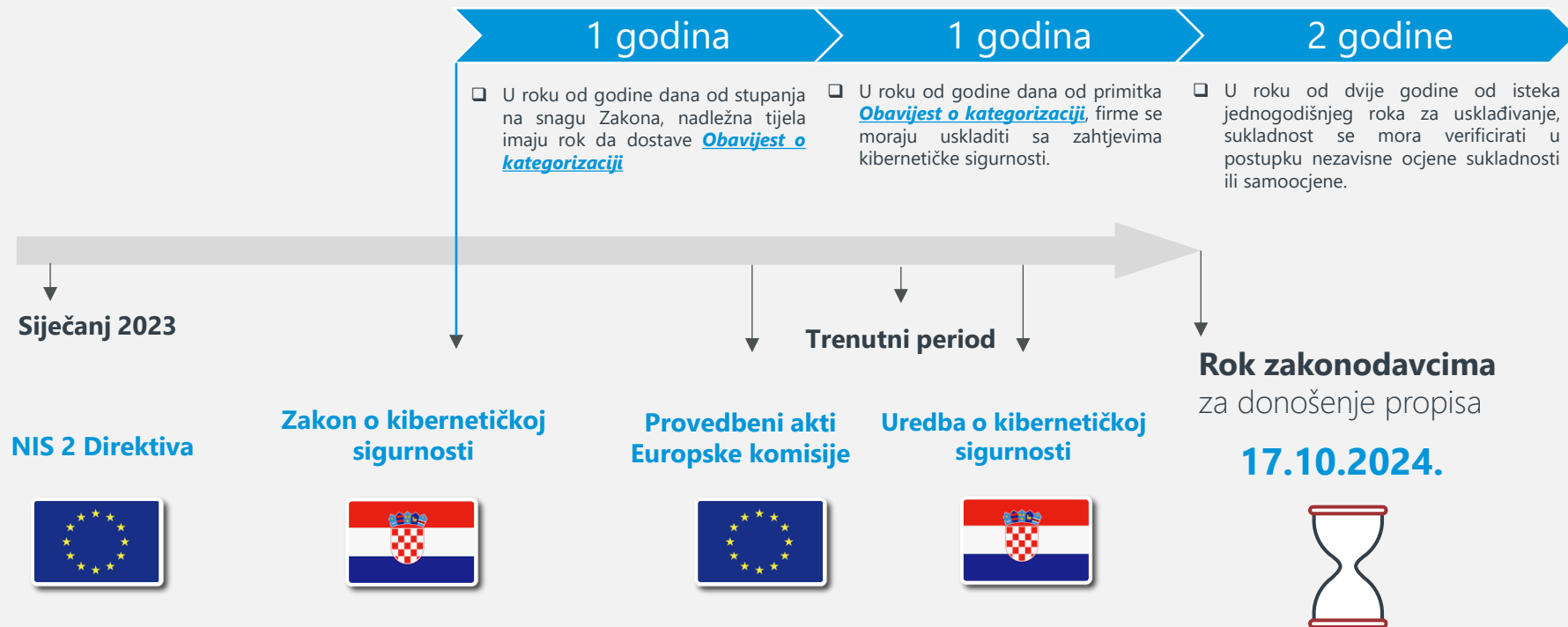
- javni sektor (Ured Vijeća za nacionalnu sigurnost - **UVNS**)
- elektroničke komunikacije (Hrvatska regulatorna agencija za mrežne djelatnosti - **HAKOM**)
- pružatelji usluga povjerenja (Središnji državni ured za razvoj digitalnog društva - **SDURDD**)

Ostali sektori

- Istraživanje, sustav obrazovanja, registar naziva vršne nacionalne domene (Ministarstvo znanosti i obrazovanja - **MZO**)
- Ostali – (Nacionalni centar za kibernetičku sigurnost koji je dio Sigurnosno obavještajne agencije – **NCSC dio SOA-e**)



ZKS (NIS 2) – VREMENSKI OKVIR



DORA – revizija

- Upravljačka tijela financijskih subjekata odobravaju i periodički preispituju planove za **unutarnju reviziju** u području ICT-a. **(članak 5. stavak 3. (f) DORA-e)**
- Financijski subjekti osiguravaju odgovarajuće razdvajanje i neovisnost funkcija upravljanja IKT rizicima, kontrolnih funkcija i funkcija **unutarnje revizije**, u skladu s modelom „triju crta obrane“ ili internim modelom upravljanja rizicima i kontrole nad njima. **(članak 6. stavak 4. DORA-e)**
- Okvir za upravljanje IKT rizicima financijskih subjekata koji nisu mikropoduzeća podliježe redovitoj **unutarnjoj reviziji**, koju revizori provode u skladu s planom revizije financijskog subjekta. Ti revizori moraju imati dostatno znanje, vještine i stručno znanje u području IKT rizika, kao i odgovarajuću neovisnost. Učestalost i težište revizija u području IKT-a moraju biti razmjerni IKT riziku financijskog subjekta. **(članak 6. stavak 6. DORA-e)**
- Financijski subjekti na temelju zaključaka **unutarnjeg revizijskog pregleda** uspostavljaju formalni proces daljnjeg postupanja, uključujući pravila za pravodobnu provjeru i ispravljanje ključnih nalaza revizije u području IKT-a. **(članak 6. stavak 7. DORA-e)**

ZKS (NIS 2) – revizija

Revizori kibernetičke sigurnosti (članak 32. ZKS-a)

Reviziju kibernetičke sigurnosti ključnih i važnih subjekata provode revizori kibernetičke sigurnosti.

Revizori kibernetičke sigurnosti su pružatelji upravljanih sigurnosnih usluga kojima je izdan:

- nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti ili
- odgovarajući kibernetički sigurnosni certifikat na temelju mjerodavne europske sheme kibernetičke sigurnosne certifikacije.

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti (članak 33. ZKS-a)

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti izdaje središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti na temelju pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti.

Provedba revizije kibernetičke sigurnosti (članak 34. ZKS-a)

Reviziju kibernetičke sigurnosti ključni subjekti dužni su provoditi najmanje jednom u dvije godine.

Izvori i literatura:

- Direktiva (EU) 2022/2555 (NIS 2 Direktiva)
- Uredba (EU) 2022/2554 (DORA Uredba)
- Zakon o kibernetičkoj sigurnosti (NN br. 14/24)

Hvala na pozornosti!

Vedran Benić

E-mail: vedran.benic@span.eu

