Regulativni okvir Zakona o kibernetičkoj sigurnosti

dr. sc. Aleksandar Klaić, dipl. ing.

Nacionalni centar za kibernetičku sigurnost

Svibanj 2025.

Mrežna stranica NCSC-HR - www.ncsc.hr

NCSC HR Nacionalni centar za kibernetičku sigurnost

Republika Hrvatska
Sigurnosno-obavještajna agencija

Naslovnica | Novosti | Sigurnosna upozorenja | SK@UT | Dokumenti | Česta pitanja | O nama | Kontakt | EN

Nacionalni centar za kibernetičku sigurnost

Nacionalni centar za kibernetičku sigurnost (NCSC-HR) ustrojen je u okviru Sigurnosno-obavještajne agencije (SOA) s ciljem zaštite nacionalnog kibernetičkog prostora te obavljanje zadaća središnjeg državnog tijela za kibernetičku sigurnost, nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, CSIRT-a, tijela odgovornog za upravljanje kibernetičkim krizama i jedinstvene kontaktne točke prema Zakonu o kibernetičkoj sigurnosti.

Saznajte više

Temeljni zahtjevi NIS2D i Zakona o kibernetičkoj sigurnosti (ZKS)

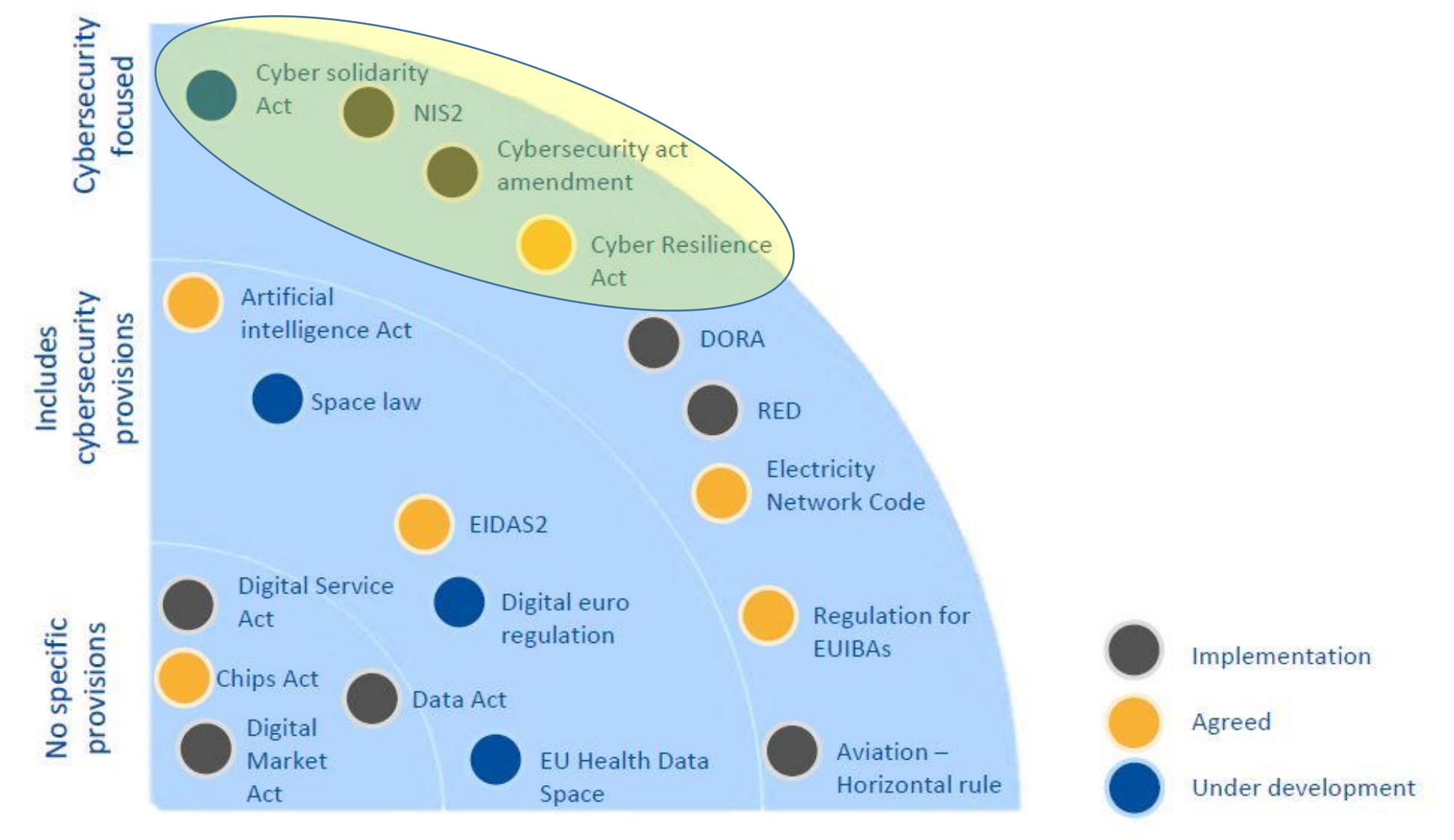
- **Odgovor** na visoku razinu **ovisnosti** suvremenog društva o digitalnoj tehnologiji i temelj za daljnji **gospodarski razvoj** EU

- **Organizacijski način** kako upravljati kibernetičkom sigurnošću i biti spreman za daljnji i sve brži razvoj digitalne tehnologije

- Razvoj **kulture upravljanja rizikom** kibernetičke sigurnosti

➢ **<u>Mjere kibernetičke sigurnosti (politike)</u>**

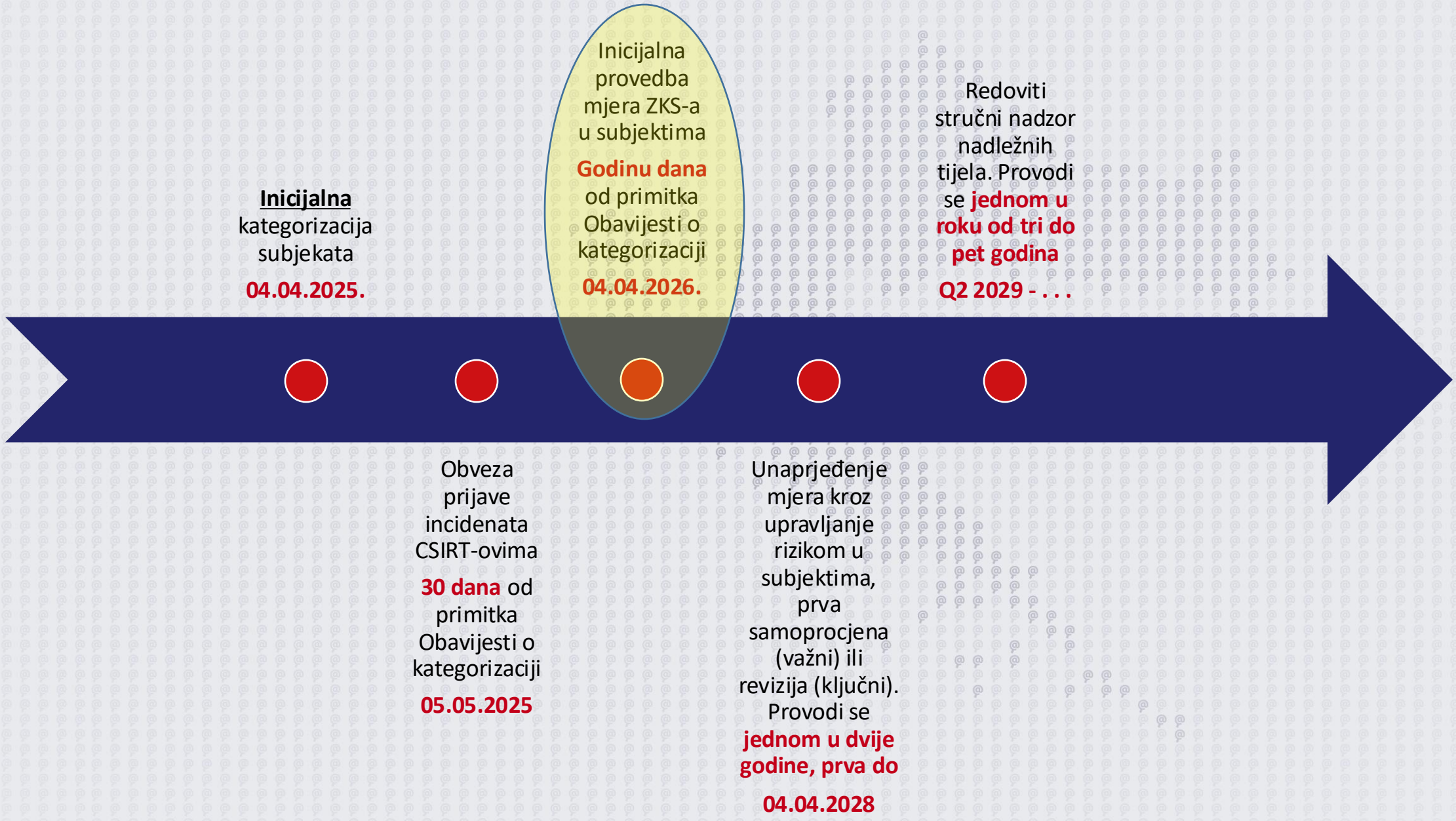
EU regulativa – kibernetička sigurnost i povezana područja



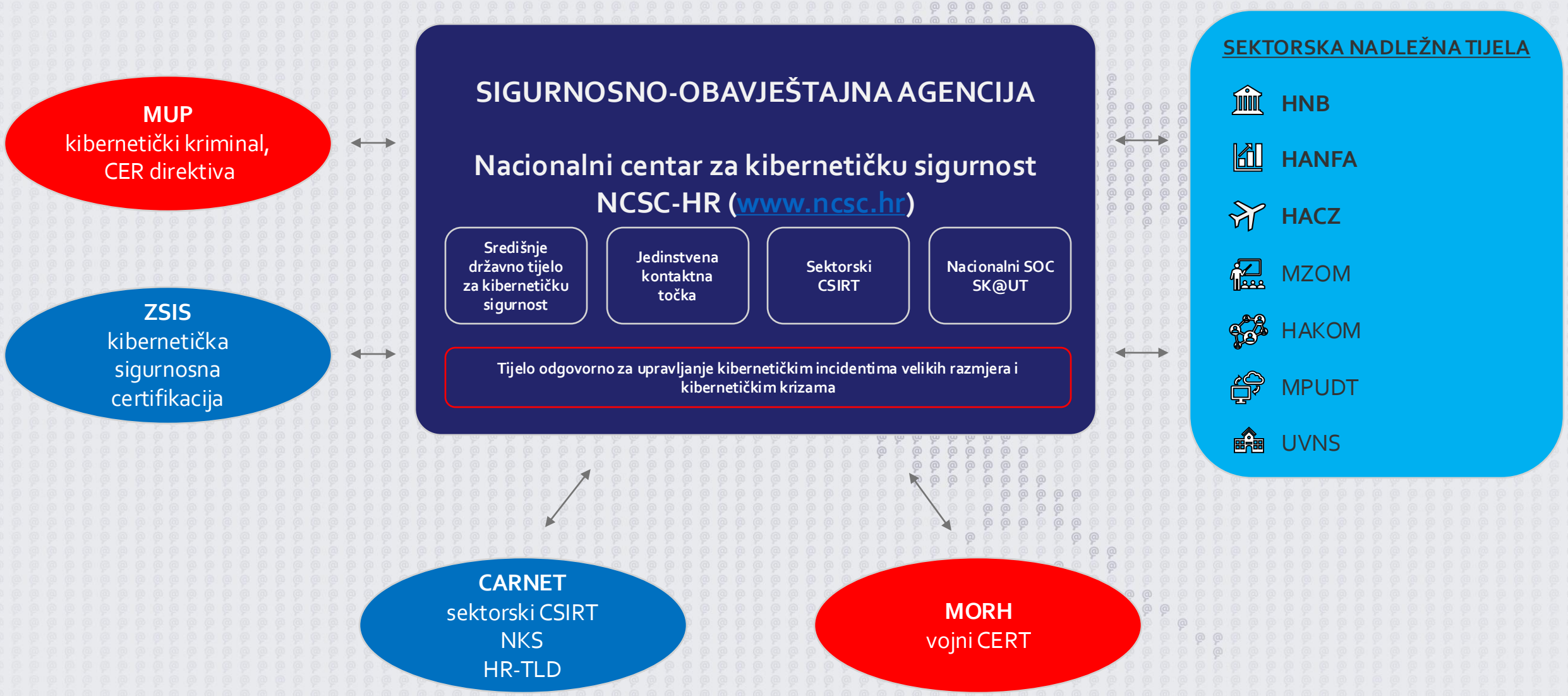
* ENISA: WK 10244/2024 INIT, 17 July 2024

Regulativni okvir Zakona o kibernetičkoj sigurnosti (ZKS):

Rokovi provedbe obveza subjekata kategoriziranih po ZKS-u



Organizacija upravljanja kibernetičkom sigurnošću u RH



Zakon i Uredba o kibernetičkoj sigurnosti – funkcionalna područja

1. **Kategorizacija subjekata**
   - Nadležna tijela
   - Ključni, važni i dobrovoljni subjekti
   - Opći i posebni kriteriji kategorizacije
2. **Provedba obvezujuće razine mjera kibernetičke sigurnosti**
   - Prilog II. Uredbe
   - Nacionalna procjena rizika (veličina subjekta, sektor)
   - Dodatne mjere fizičke sigurnosti, prilog III. Uredbe (CER)
   - Provedbena uredba Komisije
3. **Značajni incidenti**
   - Kriteriji za značajne incidente
   - Obavještavanje o značajnim incidentima
   - Nacionalna platforma PiXi
4. **Lokalna procjena rizika kategoriziranih subjekata**
   - Unaprjeđene i proširenje obvezujućih mjera
   - All-Hazards-Approach
   - Razina zrelosti
5. **Revizija za ključne i samoprocjena za važne i dobrovoljne subjekte**
   - Pravila samoprocjene
   - Pravila revizije
6. **Stručni nadzor**
   - Nadležna tijela za provedbu zahtjeva
   - Redovni i izvanredni nadzori
   - Provedba stručnog nadzora
7. **Dobrovoljno postupanje**
   - Obavještavanje o ostalim incidentima, kibernetičkim prijetnjama te izbjegnutim incidentima
   - Dobrovoljni subjekti
   - Nacionalni sustav SK@UT
8. **Kibernetičko sigurnosno certificiranje**
   - Nacionalne i EU certifikacijske sheme
   - Zakon o provedbi kibernetičke sigurnosne certifikacije (NN 63/22)
   - CSA+, CRA, CSoA

Sektori obuhvaćeni Zakonom o kibernetičkoj sigurnosti

SEKTORI – Prilog I.	NADLEŽNO TIJELO	CSIRT
ENERGETIKA	NCSC-HR	**NCSC-HR**
PROMET	NCSC-HR HACZ	**NCSC-HR**
BANKARSTVO	HNB	**NCERT**
FINANCIJE	HANFA	**NCERT**
ZDRAVSTVO	NCSC-HR	**NCSC-HR**
VODA ZA LJUDSKU POTROŠNJU	NCSC-HR	**NCSC-HR**
OTPADNE VODE	NCSC-HR	**NCSC-HR**
DIGITALNA INFRASTRUKTURA	NCSC-HR MZOM MPUDT HAKOM	**NCSC-HR** **NCERT**
UPRAVLJANJE USLUGAMA IKT-A (B2B)	NCSC-HR	**NCSC-HR**
JAVNI SEKTOR	UVNS	**NCSC-HR**
SVEMIR	NCSC-HR	**NCSC-HR**

SEKTORI – Prilog II.	NADLEŽNO TIJELO	CSIRT
POŠTANSKE I KURIRSKE USLUGE	NCSC-HR	**NCSC-HR**
GOSPODARENJE OTPADOM	NCSC-HR	**NCSC-HR**
IZRADA, PROIZVODNJA i DISTRIBUCIJA KEMIKALIJA	NCSC-HR	**NCSC-HR**
PROIZVODNJA, PRERADA I DISTRIBUCIJA HRANE	NCSC-HR	**NCSC-HR**
PROIZVODNJA	NCSC-HR	**NCSC-HR**
PRUŽATELJI DIGITALNIH USLUGA	NCSC-HR	**NCSC-HR**
ISTRAŽIVANJE	MZOM	**NCERT**
SUSTAV OBRAZOVANJA	MZOM	**NCERT**

Kategorizacija i obveznici Zakona o kibernetičkoj sigurnosti

- subjekti koji posluju u sektorima i podsektorima Priloga I. I II. Zakona
  - veliki ili srednji subjekti prema općim kriterijima
    - neovisno o veličini samo u nekim sektorima (npr. pružatelji usluga povjerenja)
  - posebni kriteriji – neovisni o veličini - tržišni udio, jedini davatelj usluge, davatelji usluga upravljanja IKT-om drugim subjektima ZKS-a, ...

KLJUČNI SUBJEKTI

- predstavljaju veliki subjekt i posluju u sektorima i podsektorima Priloga I. Zakona
- prema posebnim kriterijima

- dužni su provoditi reviziju kibernetičke sigurnosti najmanje jednom u dvije godine

VAŽNI SUBJEKTI

- predstavljaju srednji subjekt iz Priloga I. Zakona
- predstavljaju veliki ili srednji subjekt i posluju u sektorima i podsektorima Priloga II. Zakona
- prema posebnim kriterijima

- dužni su provoditi samoprocjenu kibernetičke sigurnosti najmanje jednom u dvije godine

- **VELIKI SUBJEKTI:**
  > 250 zaposlenika
  > 50/43 mil. EUR
- **SREDNJI SUBJEKTI:**
  > 50 zaposlenika
  > 10 mil. EUR

Statistika inicijalne kategorizacije u RH

- **41** sektor, podsektor i vrsta subjekta
- **702** kategorizirana subjekta
  - **140** ključnih subjekata
  - **562** važna subjekta
- **28** registrara HR domena - ovlašteni od CARNET TLD-a
  - Dostavljaju podatke u registar posebnih subjekata, nisu subjekti ZKS-a
- Promjene registra kategoriziranih subjekata koje se očekuju:
  - **Trajno** - mali broj novih kategorizacija ili dekategorizacija
    - Nove pravne osobe i/ili djelatnosti, spajanja, preuzimanja, …
  - **Jednokratno** do kraja H1/2025 - veći broj novih kategorizacija
    - **mali** subjekti u okviru **sektora upravljanja uslugama IKT-a** - **posebni kriterij** davanja usluga subjektima ZKS-a

Uredba o kibernetičkoj sigurnosti – prilog II.

ZKS, članak 30.

– korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi.

Mjere kibernetičke sigurnosti

PRILOG II

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

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

5.3. uz provedbu politike korištenja lozinki, implementirati višefaktorsku autentifikaciju (MFA) za kritične mrežne i informacijske sustave koji su više izloženi potencijalnim kibernetičkim napadima. Primjena MFA je potrebna na VPN pristupu, SaaS alatima dostupnim s Interneta itd. Potrebno je osigurati da se korisnička imena i lozinke korištene na servisima s dvofaktorskom autentifikacijom ne koriste na drugim servisima bez dvofaktorske autentifikacije. Snaga provjere autentičnosti mora biti usklađena s procjenom rizika i izloženosti mrežnog i informacijskog sustava. Potrebno je uzeti u obzir višefaktorsku provjeru autentičnosti prilikom pristupanja kritičnim mrežnim i informacijskim sustavima s udaljene lokacije, sustavima za administriranje korisnika i mrežnih i informacijskih sustava, kritičnim podacima subjekta itd. Višefaktorska provjera autentičnosti se može kombinirati s drugim tehnikama kako bi se zahtijevali dodatni faktori u specifičnim okolnostima, temeljeno na unaprijed definiranim pravilima i obrascima, poput pristupa s neuobičajene lokacije, s neuobičajenog uređaja ili u neuobičajeno vrijeme.

macijskim sustavima

skih sustava

izama

Smjernice s mapiranjem normi i najboljih praksi na mjere iz Uredbe, www.ncsc.hr - lipanj 2025.

ISO/CIS/ETSI/NIST . . .

Korišteno ili odabrano tehničko rješenje

Informacijska i kibernetička sigurnost

SUBJEKT ZKS-a

INFORMACIJSKA SIGURNOST

Zaštita podataka u fizičkom i elektroničkom obliku

IT SIGURNOST

Zaštita mrežnih i informacijskih sustava

KIBERNETIČKA SIGURNOST

Zaštita IT imovine i korisnika od kibernetičkih ugroza

Government Security Policy

Ljudi, procesi, tehnologija

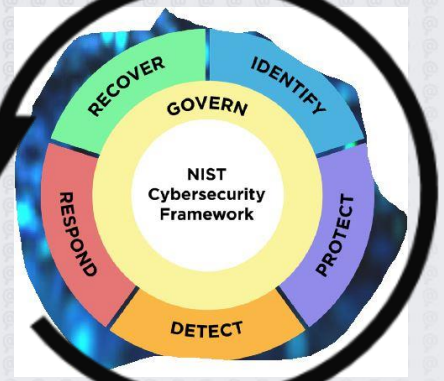
Plan, Do, Check , Act

ISO/IEC 27001:2022 + 27110, ...

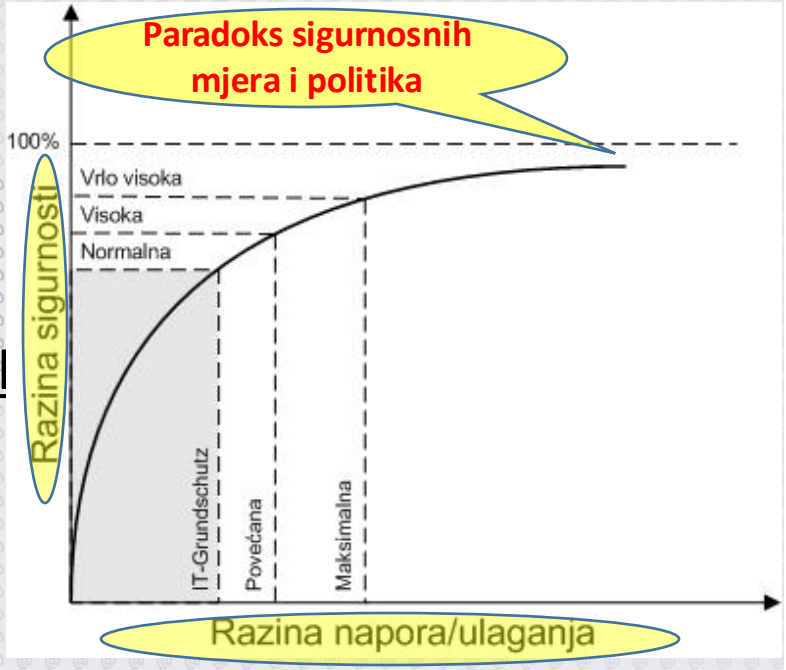
- People (8 controls),
- Organizational (37 controls),
- Technological (34 controls),
- Physical (14 controls).

- ETSI TR 103 305-1 Critical Security Controls for Cyber Defence (09/2018)
- CIS Controls
- ISA/IEC 62443 / NIST SP 800-82 Rev. 3

US NIST CSF 2.0



Provedba obvezujuće razine mjera kibernetičke sigurnosti



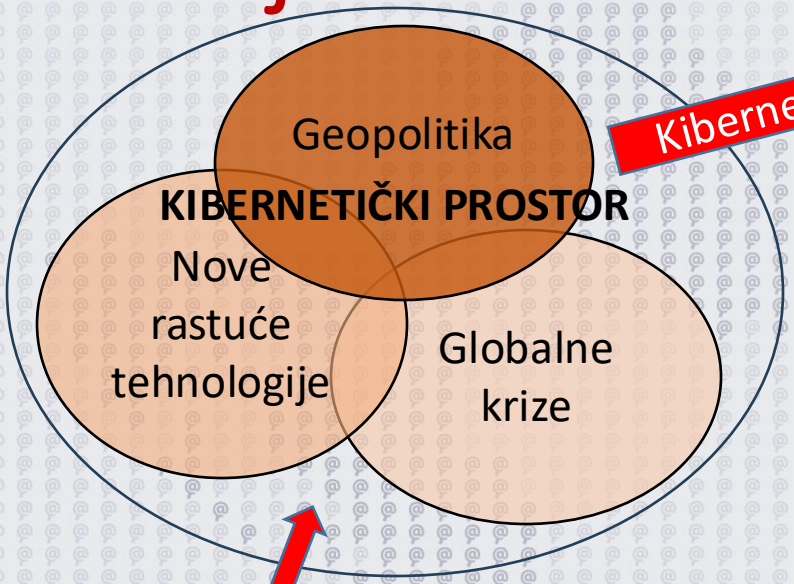
- Utvrđuje se kroz postupak kategorizacije
  - Sektor, podsektor, vrsta subjekta
  - Veličina subjekta
  - Rezultat nacionalne procjene rizika (veličina subjekta i sektor posl
- Nacionalna procjena kibernetičkih sigurnosnih rizika
  - **Osnovna** razina mjera
    - Niska razina rizika
    - Opći skup mjera, oportunistički kibernetički napadi, napadači prosječnih kibernetičkih vještina
  - **Srednja** razina mjera
    - Srednja razina rizika
    - Dopunjeni skup mjera, ciljani kibernetički napadi, napadači prosječnih kibernetičkih vještina
  - **Napredna** razina mjera
    - Visoka razina rizika
    - Napredni skup mjera, ciljani kibernetički napadi, napadači s naprednim vještinama i resursima

Uredba o kibernetičkoj sigurnosti i procjena rizika na nacionalnoj razini:

Smjernice i kalkulator na www.ncsc.hr

Kibernetički napadači

- Državno sponzorirane APT grupe
- Teroristi
- Kibernetički kriminalne grupe
- Haktivističke grupe
- Poslovni konkurenti



Kibernetički ciljevi

Obilježja kibernetičkih ciljeva

Vrste entiteta:
- Državna tijela
- Kritična infrastruktura
- Pravne osobe
- Građanstvo

Obilježja entiteta:
- Veličina
- Sektor
- Utjecaj poremećaja

Razina	Podskupovi mjere								
	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.
osnovna	A	A	A	A	A	C	C	C	C
srednja	A	A	A	A	A	A	A	C	C
napredna	A	A	A	A	A	A	A	A	A

Tri razine mjera kibernetičke sigurnosti:

1. Osnovna
2. Srednja
3. Napredna

Kibernetički napadi

- Poremećaj poslovanja/Sabotaža
- Krađa podataka/špijuniranje
- Kibernetički kriminal (RW, financijske prijevare)
- Vandalizam sadržaja i dostupnosti na Internetu
- Politički utjecaj i dezinformacije

Nacionalna procjena kibernetičkih sigurnosnih rizika

Prepoznavanje različitih:
- Profila rizika (sektori)
- Utjecaja (napadi)
- Razina rizika (subjekti)

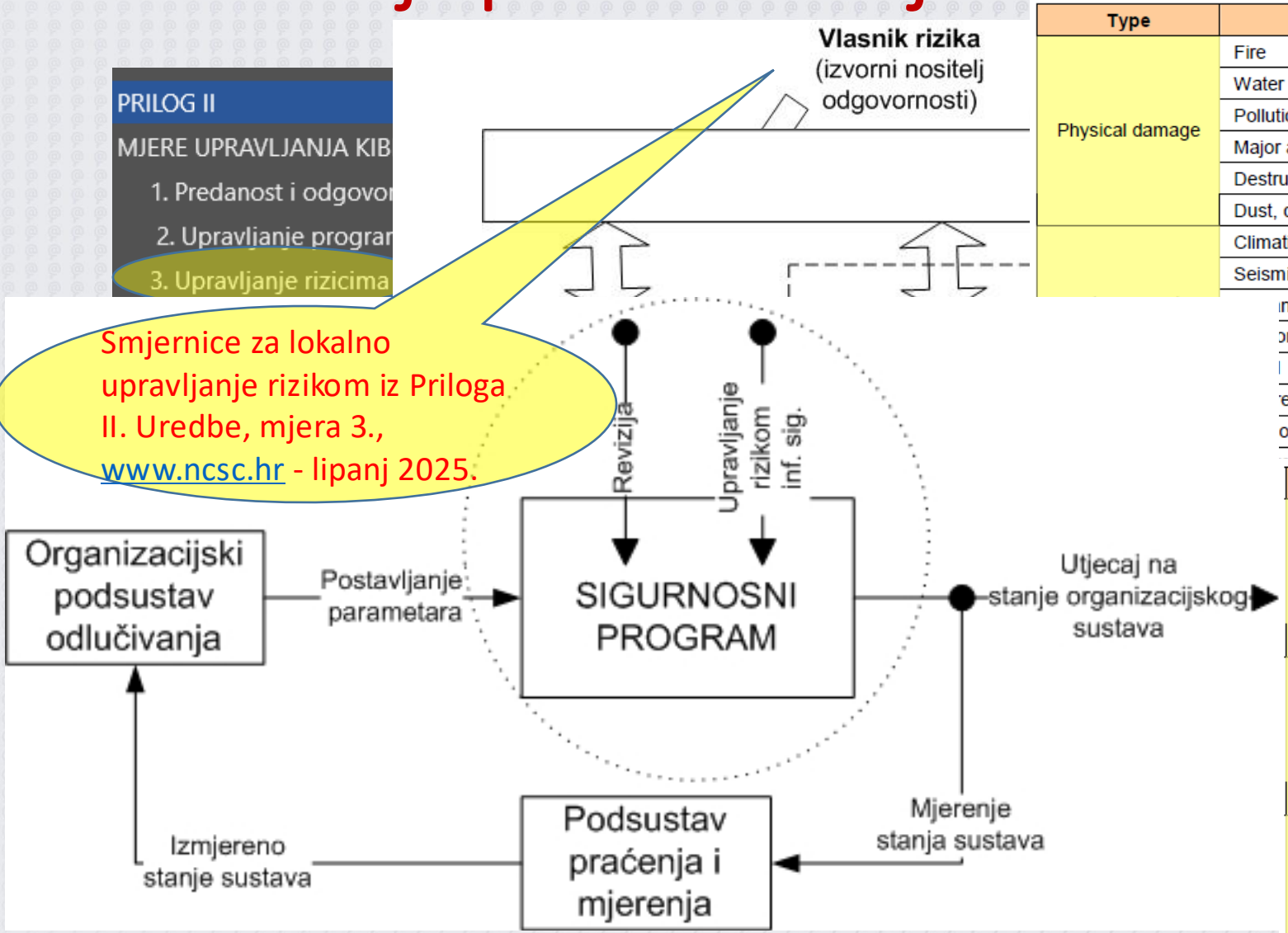
Uredba o kibernetičkoj sigurnosti i lokalno upravljanje rizicima koje provode subjekti (All-Hazards-Approach):

PRILOG II

MJERE UPRAVLJANJA KIB

1. Predanost i odgovor
2. Upravljanje prograr
3. Upravljanje rizicima

Smjernice za lokalno upravljanje rizikom iz Priloga II. Uredbe, mjera 3., www.ncsc.hr - lipanj 2025.



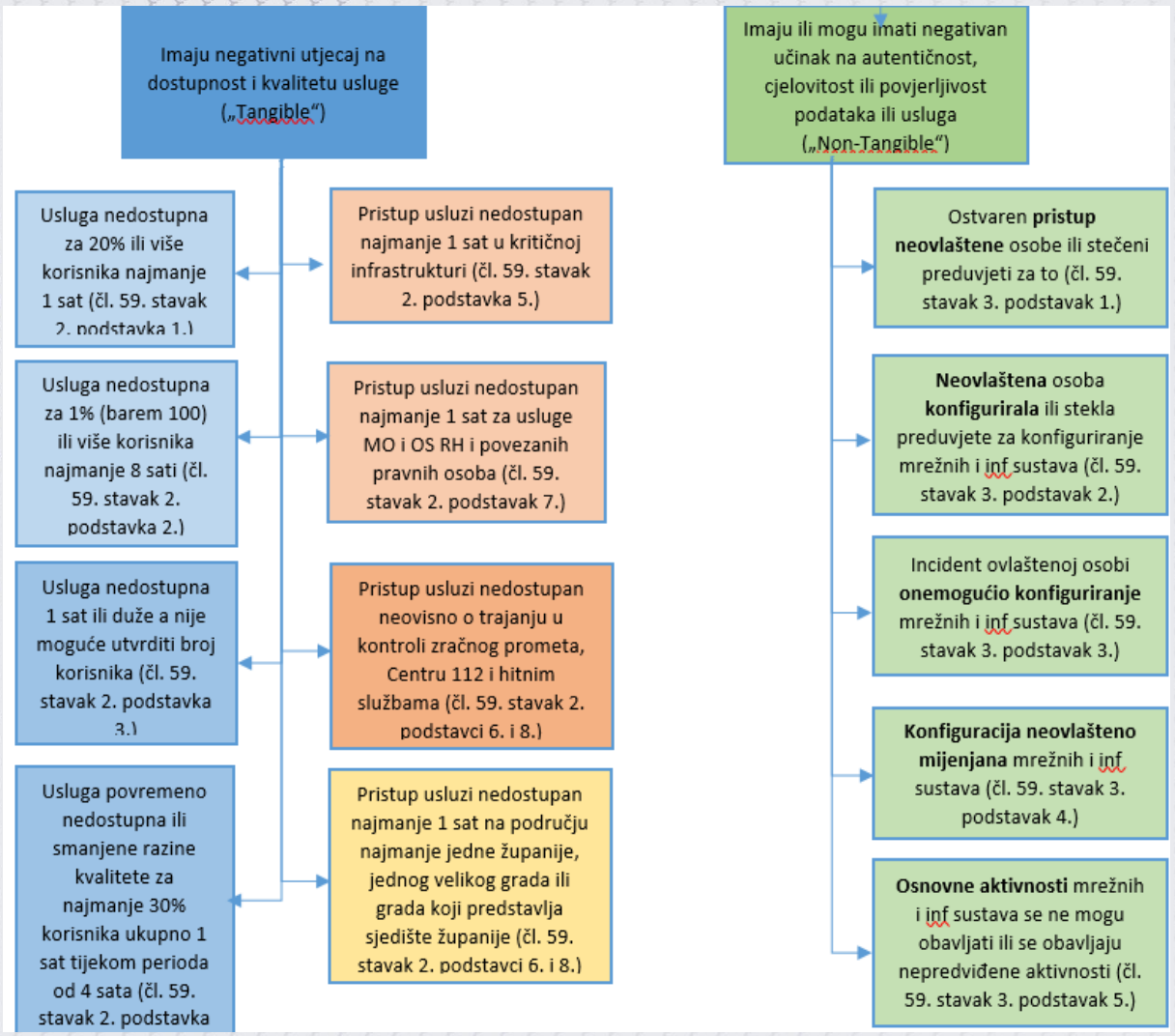
Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
	Climatic phenomenon	E
	Seismic phenomenon	E
	nic phenomenon	E
	orological phenomenon	E
		E
	e of air-conditioning or water supply system	A, D
	of power supply	A, D, E

Obrada rizika

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

Značajni incidenti – kriteriji (1/3)

- Opći kriteriji iz ZKS-a u čl. 37.
- „All Hazards Approach”
  - Mrežni i informacijski sustavi
    - Failure/Accident/Attack
- Razrada općih kriterija iz ZKS-a u Uredbi od čl. 58. do čl. 63.
  - Značajan incident ima znatan učinak na dostupnost, cjelovitost, povjerljivost i/ili autentičnost, a pogađa podatke od značaja za poslovanje subjekta i/ili kontinuitet usluga koje subjekt pruža ili djelatnosti koje obavlja
  - Članak 59. Uredbe

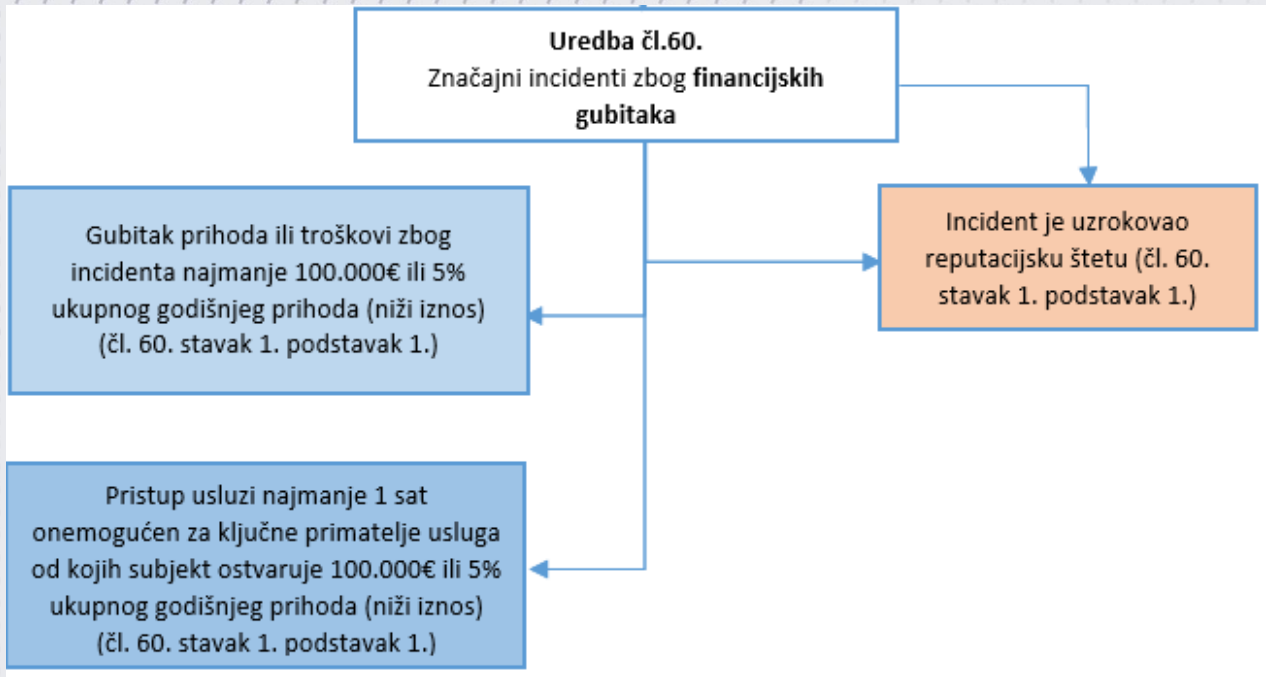


Značajni incidenti – kriteriji (2/3)

- Uredba čl.60.
- Značajni incidenti zbog financijskih gubitaka

Šteta uzrokovana incidentom > 100 000 EUR

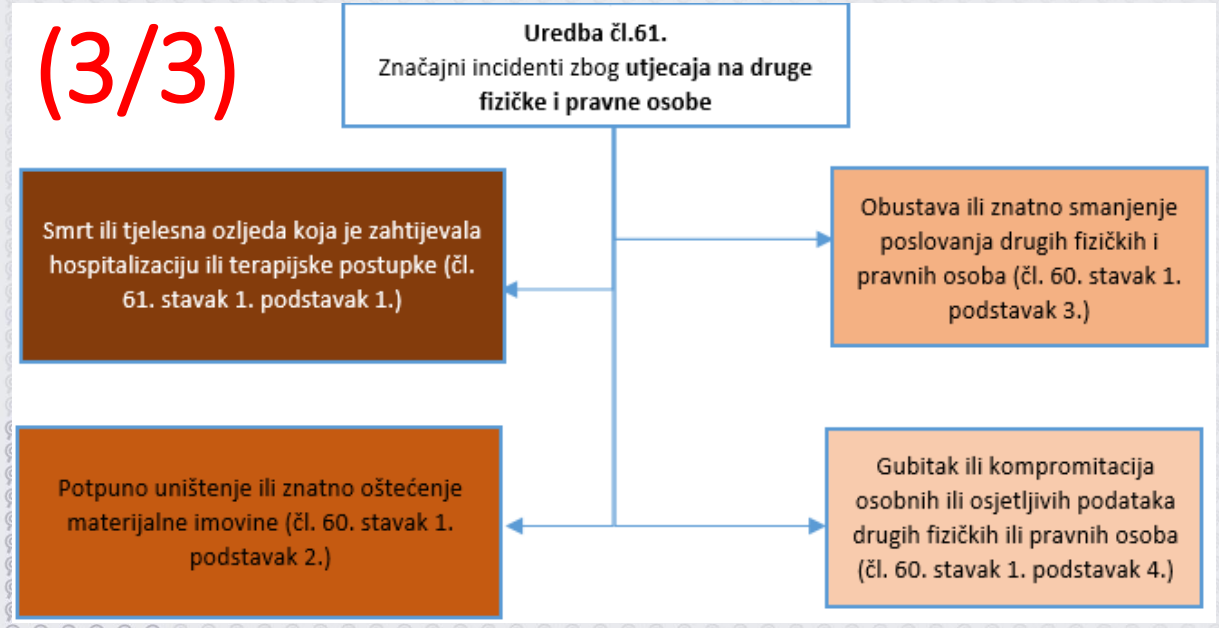
Računa se suma ukupnog broja direktnih i indirektnih troškova i gubitaka koji se javljaju zbog pojave samog incidenta koji mogu uključivati sljedeće:

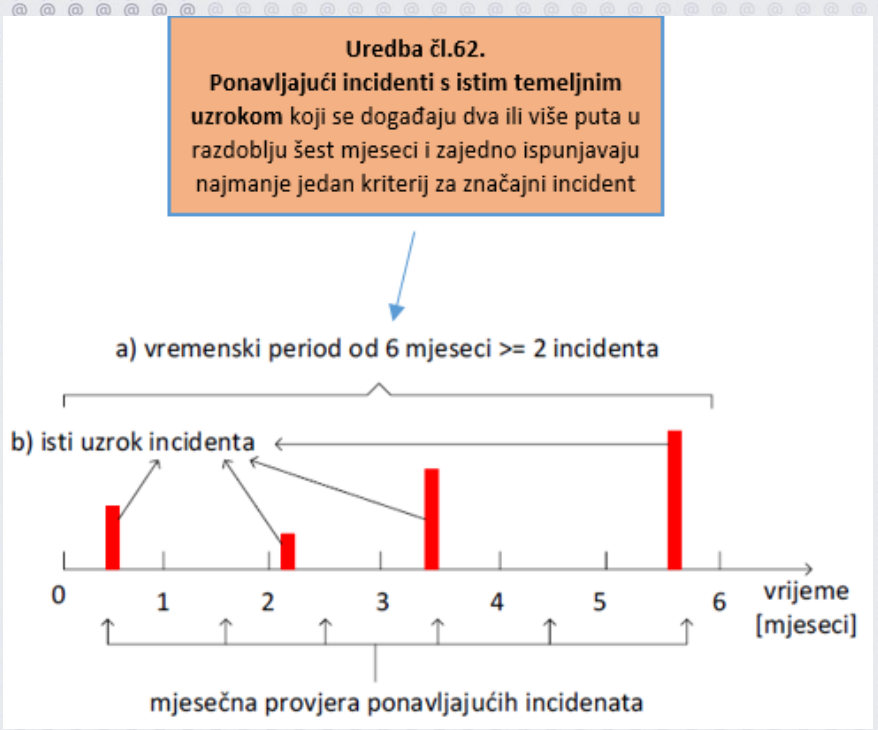


Značajni incidenti – kriteriji (3/3)

- Uredba čl.61.
- Značajni incidenti zbog utjecaja na druge fizičke i pravne osobe

- Uredba čl.62.
- Ponavljajući incidenti s istim temeljnim uzrokom koji se događaju dva ili više puta u razdoblju od šest mjeseci i zajedno ispunjavaju najmanje jedan kriterij za značajni incident





Obvezujuća razina mjera i kriteriji značajnih incidenata – dodatni zahtjevi (CER direktiva, EK)

- Uključuje **dodatne mjere fizičke sigurnosti iz priloga III. Uredbe**
  - **Primjena na subjekte iz sektora digitalne infrastrukture**
  - Mrežni i informacijski sustavi su temelj poslovanja
  - Mjere samo kroz NIS2 transpoziciju, a ne kombinirano NIS2 + CER direktiva
- **Provedbena Uredba Komisije (EU) 2024/2690 od 17.10.2024.** pokriva izabrane subjekte iz više sektora s različitim **digitalnim uslugama koje imaju prekogranični EU značaj**
  - Digitalna infrastruktura (prilog I.)
  - Upravljanje uslugama IKT-a (B2B) (prilog I.)
  - Pružatelji digitalnih usluga (prilog II.)

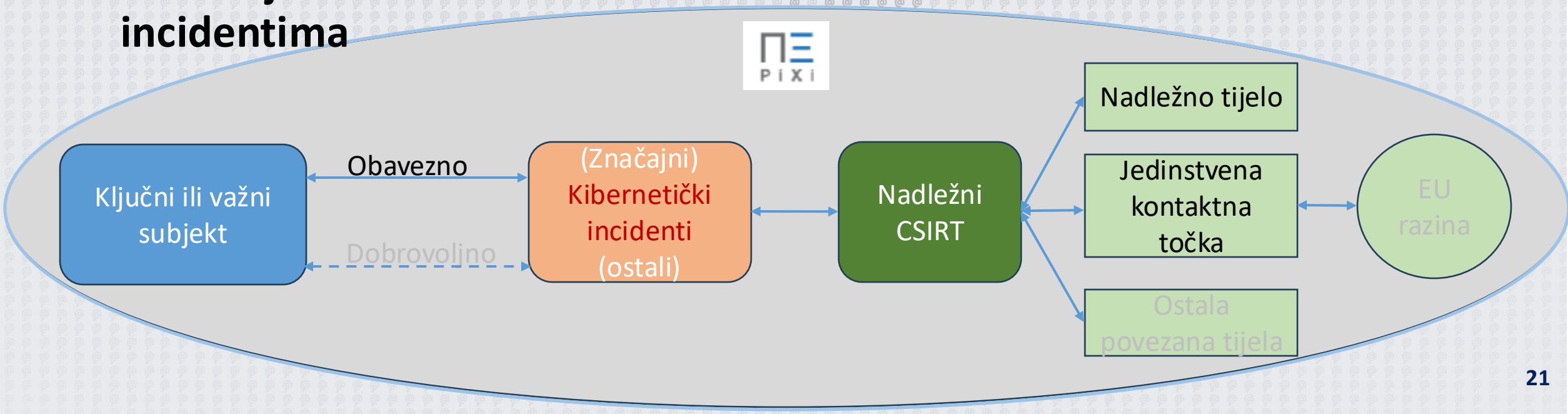
o utvrđivanju pravila za primjenu Direktive (EU) 2022/2555 u **pogledu tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkim sigurnosnim rizicima te dodatnih kriterija u kojima se incident smatra značajnim za**:
- pružatelje usluga DNS-a
- registre naziva vršnih domena
- pružatelje usluga računalstva u oblaku
- pružatelje usluga podatkovnog centra
- pružatelje mreža za isporuku sadržaja
- pružatelje upravljanih usluga
- pružatelje upravljanih sigurnosnih usluga
- pružatelje internetskih tržišta
- internetskih tražilica
- platformi za usluge društvenih mreža te
- pružatelje usluga povjerenja.

Izuzeti od Komisijinog akta:
- pružatelji javnih elektroničkih komunikacijskih mreža
- pružatelji javno dostupnih elektroničkih komunikacijskih usluga
- pružatelji središta za razmjenu internetskog prometa (CIX)

Značajni incidenti – obavještavanje i rokovi

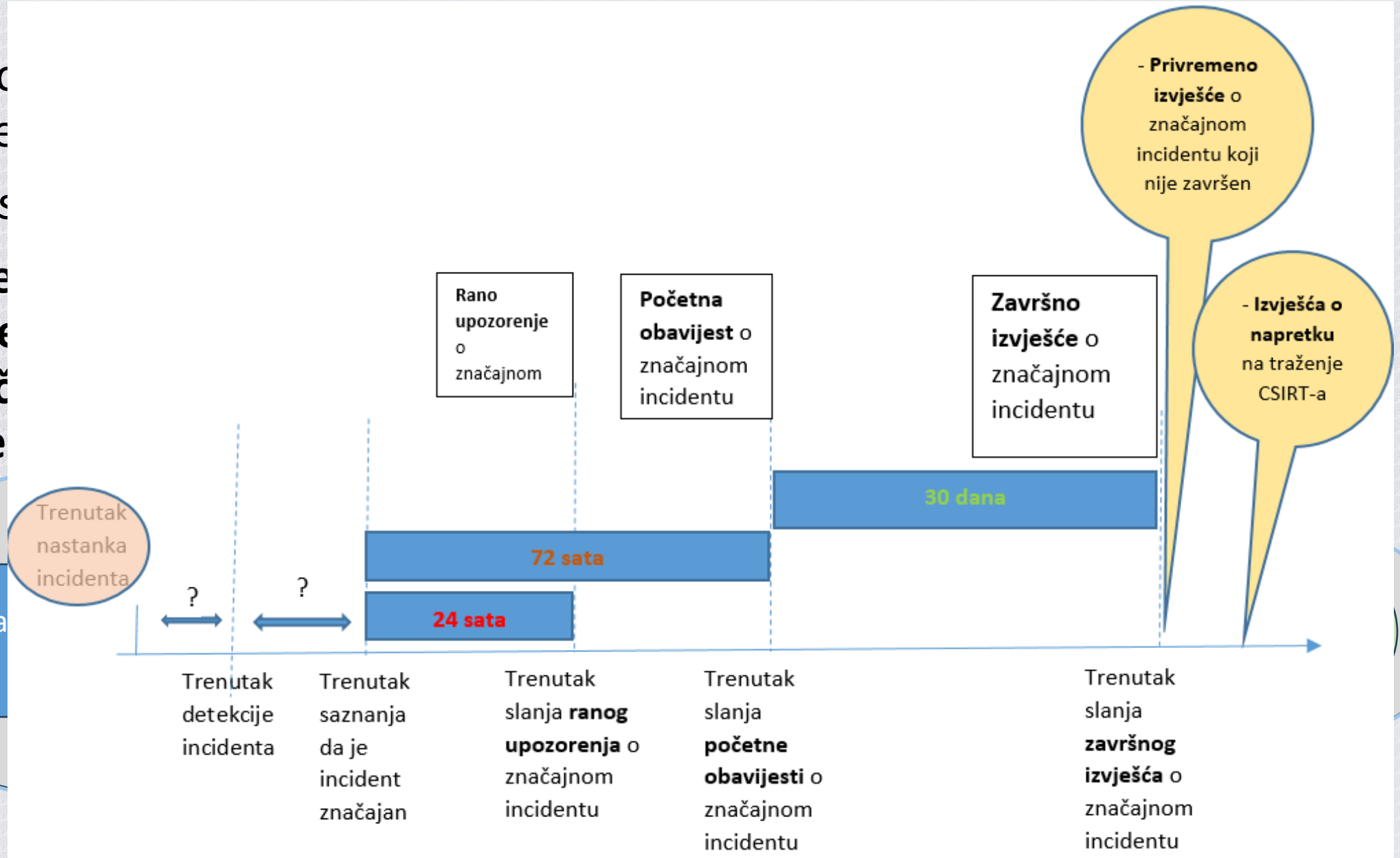
- Kategorije obavještavanja
- Vrste subjekata
- **Obavezno obavještavanje o značajnim incidentima**

	Značajni incidenti	Ostali incidenti	Kibernetičke prijetnje	Izbjegnuti incidenti
Ključni subjekti	Obavezno	Dobrovoljno	Dobrovoljno	Dobrovoljno
Važni subjekti	Obavezno	Dobrovoljno	Dobrovoljno	Dobrovoljno
Dobrovoljni subjekti	Dobrovoljno	Dobrovoljno	Dobrovoljno	Dobrovoljno



Značajni incidenti – obavještavanje i rokovi

- Kategc
  obavje
- Vrste s
- **Obave**
  obavje
  o znač
  incide



Ključni ili va
subjekt

Značajni incidenti – obavještavanje

- **Nacionalna platforma PiXi**
- **Ilustracija** obrazaca:

Smjernice travanj 2025.:
- **Nacionalna taksonomija incidenata (CSIRT-ovi)**
- **Obavijesti o incidentima (CSIRT-ovi)**
- **Nacionalna platforma PiXi (CARNET)**

RANO UPOZORENJE (24 sata)	
	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.
	11.
	12.
	13.
	14.
	15.
	16.
	17.

POČETNA OBAVIJEST (72 sata)	
	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.
	11.
	12.
	13.
	14.
	15.
	16.
	17.
	18.
	19.
	20.
	21.
	22.
	23.
	24.
	25.
	26.

ZAVRŠNO IZVJEŠĆE (30 dana)		
	1.	Datum i vrijeme izvješća
	2.	Kontakt osoba
	3.	Referentni broj incidenta
	4.	Prekogranični incident
	5.	Utjecaj incidenta
	6.	Broj zahvaćenih korisnika usluga po subjektu i/ili sektoru
	7.	Postotak zahvaćenih korisnika u odnosu na ukupan broj korisnika
	8.	Trajanje neraspoloživosti usluga u satima i po zahvaćenim sektorima
	9.	Opis reputacijske štete (zakonska ili regulatorna odstupanja, žalbe, …)
	10.	Ponavljajući incident
	11.	Povezani incidenti ako ih ima
	12.	Dodatne informacije o incidentu
	13.	Kategorija uzroka incidenta prema nacionalnoj taksonomiji
	14.	Sažetak opisa incidenta
	15.	Datum i vrijeme kada je incident razvrstan kao značajan
	16.	Sažetak vremenskog toka događaja u okviru incidenta
	17.	Datum i vrijeme ponovne uspostave usluga, procesa i aktivnosti
	18.	Poduzete mjere za oporavak
	19.	Planirane mjere za nastavak oporavka
	20.	Naučene lekcije
	21.	Način otkrivanja i obavješćivanja o incidentu (tijela, korisnici, javnost)
	22.	Poslovni procesi subjekta koji su bili zahvaćeni incidentom
	23.	Tehnički indikatori kompromitacije (IoC)
	24.	Saznanja o taktikama, tehnikama i procedurama napadača (TTP)
	25.	Opis u slučaju *Ransomware* napada (eksfiltracija, otkupnina, …)
	26.	Iskorištena ranjivost
	27.	Opis tehničke informacijske imovine na koju je incident utjecao
	28.	Opis kriterija i pragova kojima je potvrđen značajni incident
	29.	Opis podataka na koje je incident utjecao (prema kriterijima)
	30.	Utjecaj incidenta prema taksonomiji kibernetičkog kriznog stanja
	31.	Prijava kaznenog djela provedena
	32.	Prijava kompromitacije osobnih podataka provedena

OSTALI INCIDENTI (dobrovoljno, 30 dana)		
	1.	Datum i vrijeme izvješća
	2.	Kontakt osoba
	3.	Referentni broj ostalih incidenta
	4.	Utjecaj incidenta
	5.	Utjecaj na reputaciju
	6.	Trajanje i stanje incidenta u trenutku izvještavanja
	7.	Ponavljajući incident
	8.	Povezani incidenti ako ih ima
	9.	Dodatne informacije o incidentu
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	
	16.	
	17.	
	18.	

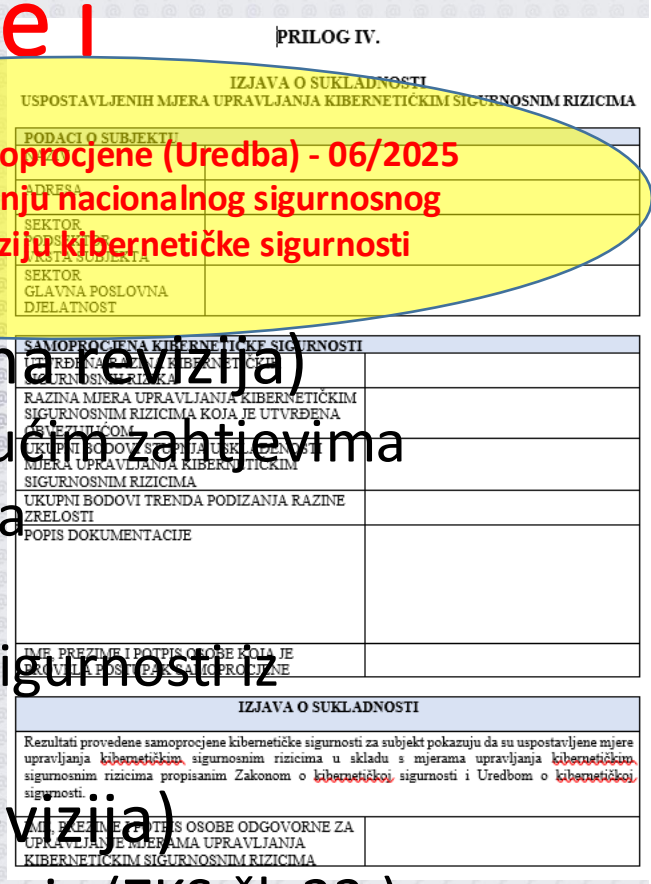
KIBERNETIČKE PRIJETNJE (dobrovoljno, 30 dana)	
	1. Datum i vrijeme izvješća
	2. Kontakt osoba
	3. Referentni broj kibernetičke prijetnje
	4. Sažetak opisa kibernetičke prijetnje
	5.
	6.
	7.
	8.
	9.

IZBJEGNUTI INCIDENT (dobrovoljno, 30 dana)	
	1. Datum i vrijeme izvješća
	2. Kontakt osoba
	3. Referentni broj izbjegnutog incidenta
	4. Sažetak opisa izbjegnutog incidenta
	5. Dodatne informacije o izbjegnutom incidentu

Revizija za ključne i samoprocjena za važne i dobrovoljne subjekte

- ZKS čl. 31. do 36. i Uredba čl. 51. do 57.9
- **Samoprocjena** – najmanje jednom u dvije godine (interna revizija)
  - Stupanj usklađenosti uspostavljenih mjera subjekta s obvezujućim zahtjevima
  - Trend podizanja razine zrelosti kibernetičke sigurnosti subjekta
  - Izjava o sukladnosti (Uredba, prilog IV.) i plan postupanja
  - Dostava nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti iz priloga III. ZKS-a, čuvanje povezane dokumentacije
- **Revizija** – najmanje jednom u dvije godine (nezavisna revizija)
  - Pravne osobe certificirane prema nacionalnoj shemi certificiranja (ZKS čl. 33.)
  - Sadržajno slično samoprocjeni uz dodatne uvjete za pravne osobe – revizore
  - Primjena do donošenja EU sheme
    - donošenje CSA+ amandmana (15.01.2025.)
    - usklađivanje Zakona o provedbi kibernetičke sigurnosne certifikacije (NN 63/2022)

ZSIS donosi:
- **Smjernice za samoprocjene (Uredba) - 06/2025**
- **Pravilnik o izdavanju nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti (ZKS) - 09/2025**



PRILOG IV.

IZJAVA O SUKLADNOSTI
USPOSTAVLJENIH MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

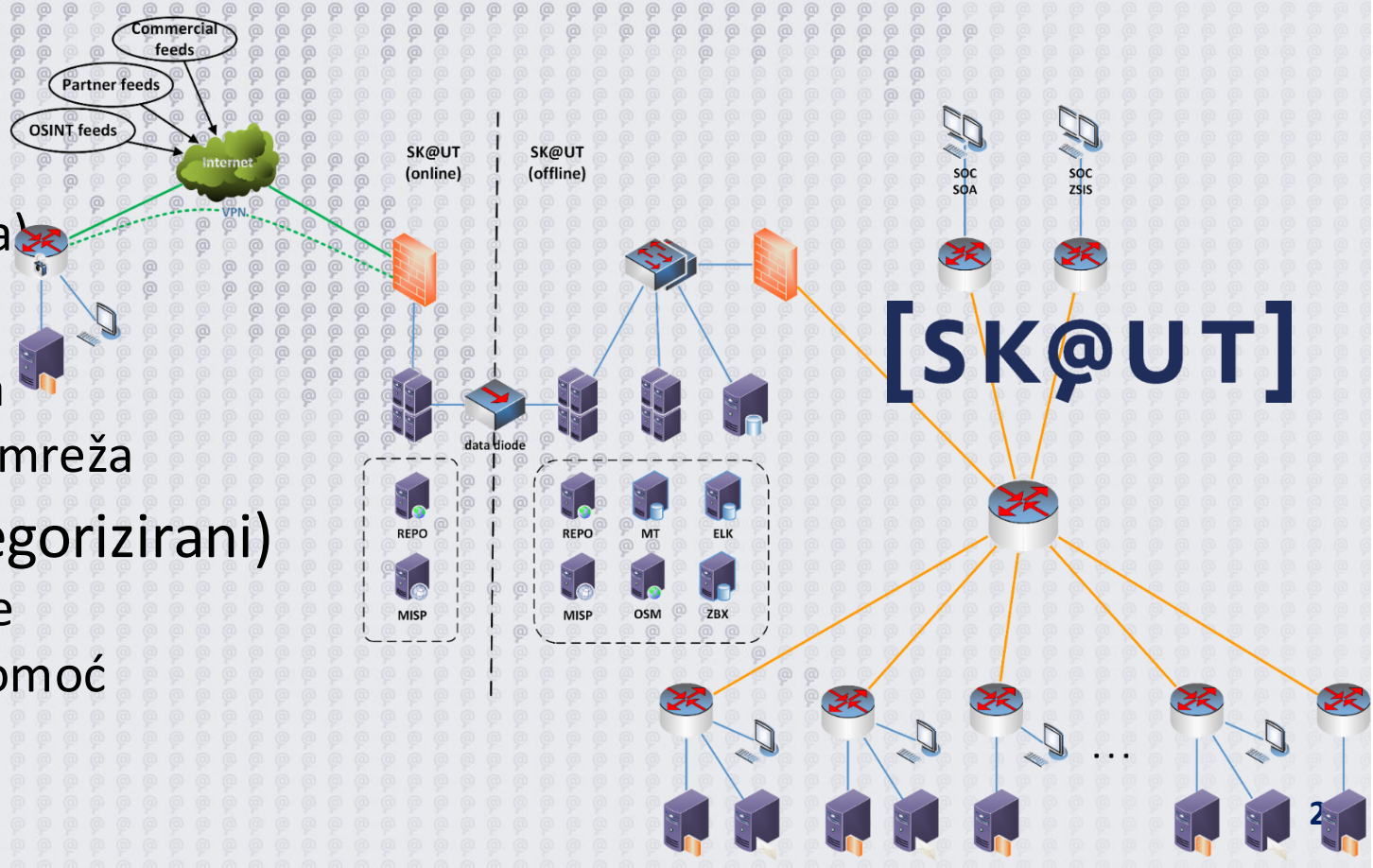
PODACI O SUBJEKTU	
NAZIV	
ADRESA	
SEKTOR	
PODSEKTOR	
VRSTA SUBJEKTA	
SEKTOR GLAVNA POSLOVNA DJELATNOST	

SAMOPROCJENA KIBERNETIČKE SIGURNOSTI	
UTVRĐENA RAZINA KIBERNETIČKE SIGURNOSNE ZRELOSTI	
RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA KOJA JE UTVRĐENA SAMOPROCJENOM	
UKUPNI BODOVI ZRELOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	
UKUPNI BODOVI TRENDA PODIZANJA RAZINE ZRELOSTI	
POPIS DOKUMENTACIJE	
IME, PREZIME I POTPIS OSOBE KOJA JE PROVELA POSTUPAK SAMOPROCJENE	

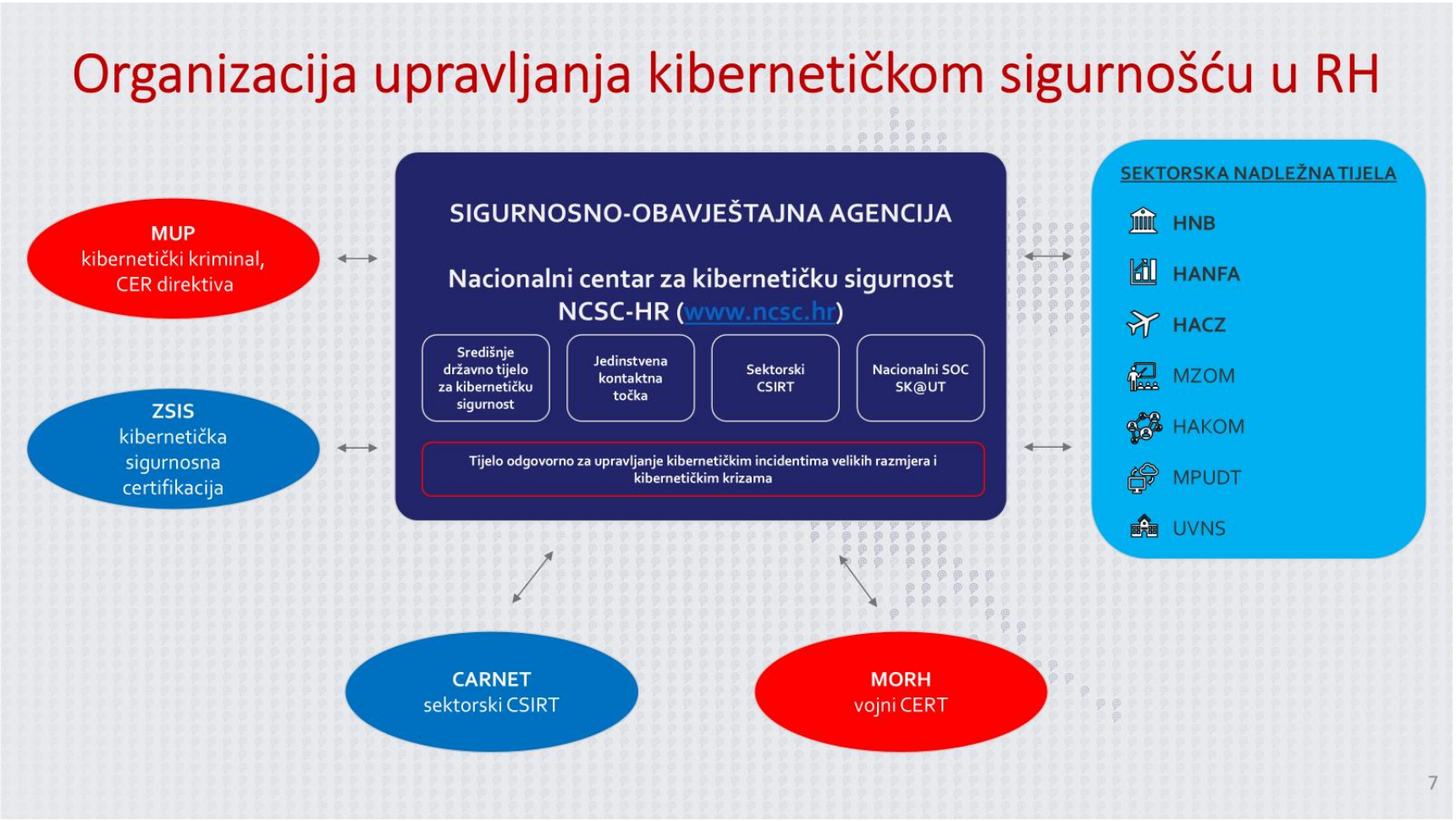
IZJAVA O SUKLADNOSTI	
Rezultati provedene samoprocjene kibernetičke sigurnosti za subjekt pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti.	
IME, PREZIME I POTPIS OSOBE ODGOVORNE ZA UPRAVLJANJE MJERAMA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	

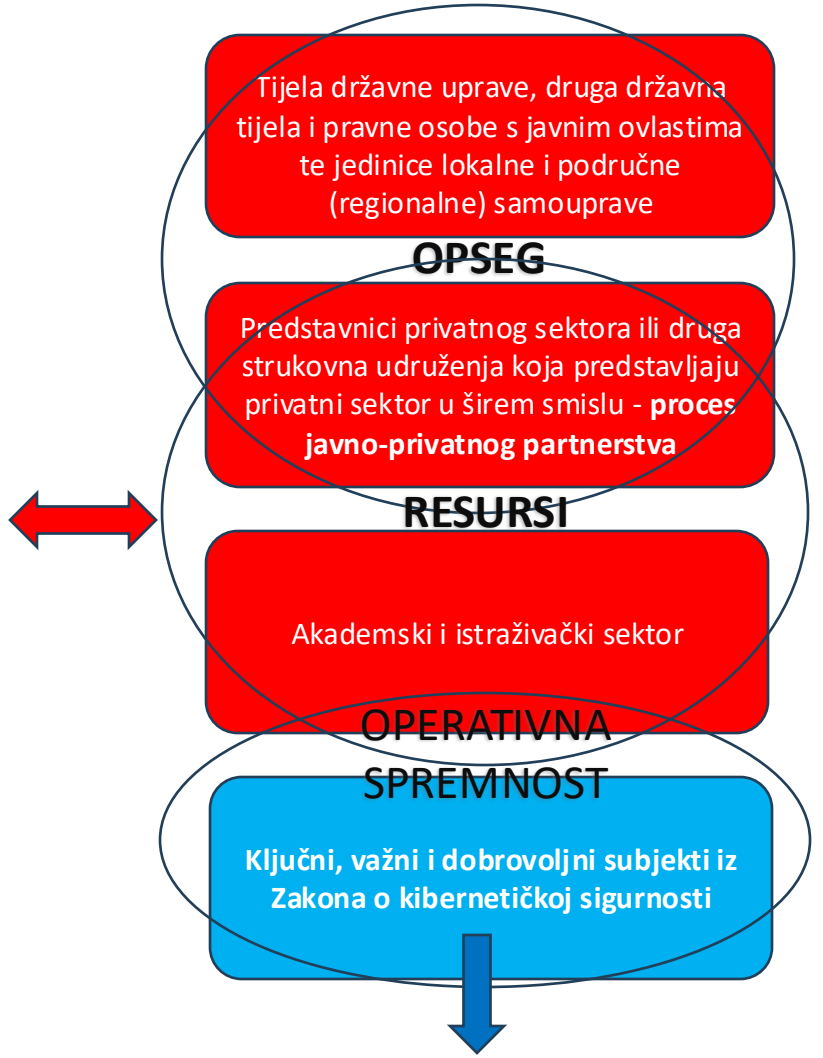
Dobrovoljno postupanje

- **Sustav SK@UT** – nacionalni sigurnosno operativni centar (SOC) i mreža senzora
  - Ministarstva, ključna državna tijela i infrastruktura (2019.-2020.)
  - Gospodarski sektori: energetika, transport, zdravstvo … (2021. -)
  - Druge pravne osobe (2022. -)
- ZKS – sustav SK@UT
  - dobrovoljna i dodatna mjera
  - SK@UT zajednica (preko 100 entiteta)
- EU Cyber Solidarity Act
  - Poticaj izgradnje državnih SOC mreža
  - Poticaj međudržavnog spajanja SOC mreža
- **Dobrovoljni subjekt ZKS-a** (nekategorizirani)
  - Osnovna razina mjera, samoprocjene
  - Izvještavanje o incidentima, CSIRT pomoć



HORIZONTALNA koordinacija u Nacionalnom programu upravljanja kibernetičkim krizama (01/2025)





Mjere kibernetičke sigurnosti iz **Uredbe o kibernetičkoj sigurnosti**

VERTIKALNA koordinacija u Nacionalnom programu upravljanja kibernetičkim krizama (01/2025)

Strateška i politička razina

Vijeće za nacionalnu sigurnost

- Koordinacija za sustav domovinske sigurnosti

Proces eskalacije:

1. **UPOZORAVAJUĆI** način rada – Odgovornost operativne razine koja izvještava stratešku i političku razinu
2. **KRIZNI** način rada – Operativna razina sukladno planu, a strateška i politička razina prema potrebi

Operativna razina

Tijelo odgovorno za upravljanje kibernetičkim krizama (SOA)

- Koordinacija za upravljanje kibernetičkim krizama
  - SOA, MUP, MORH, MZO, UVNS, ZSIS, MPUDT, HAKOM, CARNET, HNB, HANFA, HACZ

Institucije koje sudjeluju koriste interne SOP dokumente

Životni ciklus upravljanja:
- **Redoviti način rada**
- **Upozoravajući način rada**
- **Krizni način rada**

Sektorske i funkcionalne nadležnosti tijela

- CERT/CSIRT/SOC nacionalna tijela sa svojim nadležnostima
- Funkcionalna područja kibernetičkog kriminala, kibernetičke špijunaže, …
- Resorno nadležna ministarstva, regulatorna tijela, gospodarski sektori, …

VERTIKALNA koordinacija u upravljanja kibernetičk

Strateška i politička razina

Vijeće za

- Koordinacija za sustav domovinske sigurnc

Operativna razina

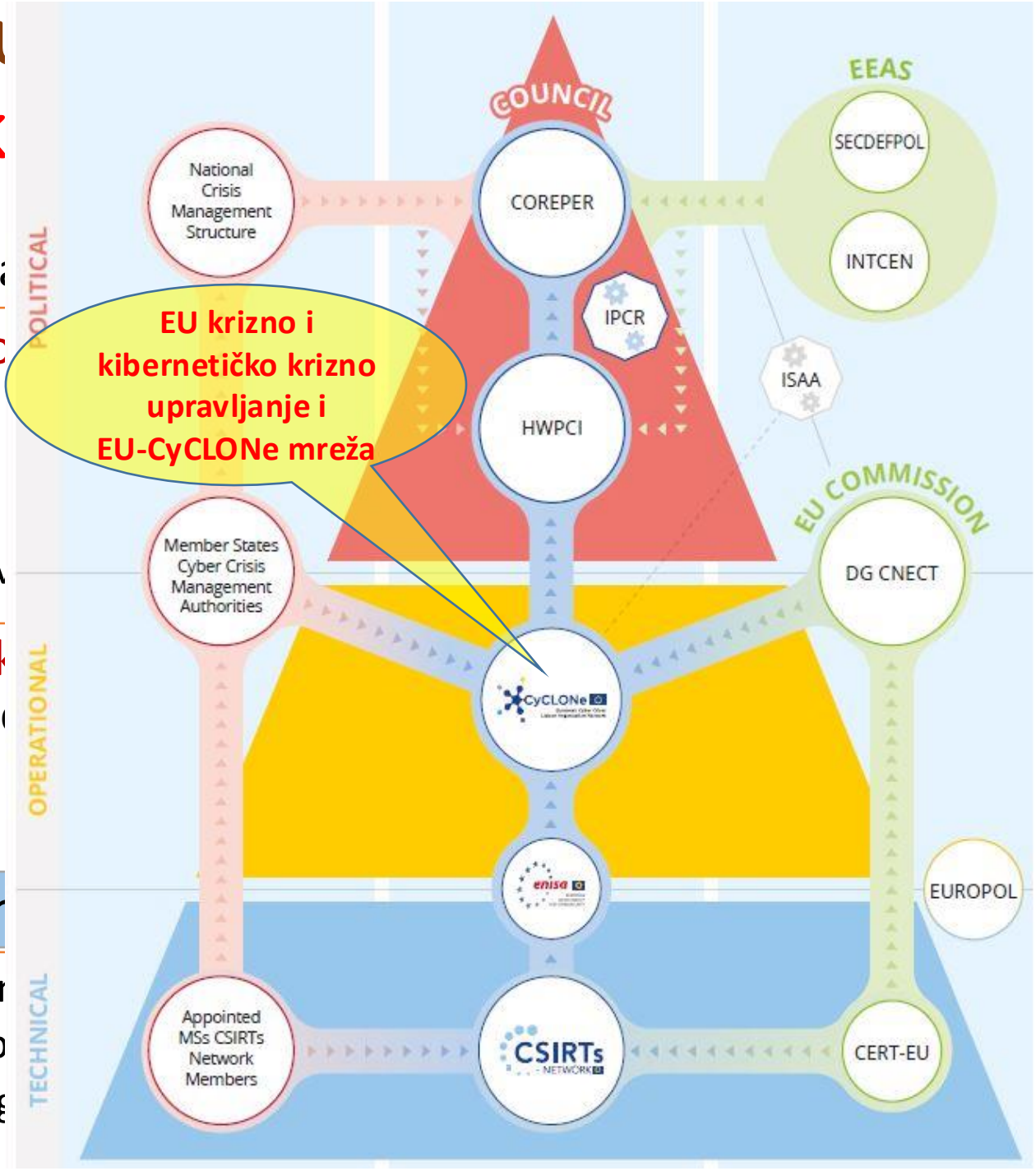
Tijelo odgov

- Koordinacija za upravljanje kibernetičkim k
  - SOA, MUP, MORH, MZO, UVNS, ZSIS, MPUDT, HAKOM,

Institucije koje sudjeluju koriste interne SOP dokumente

Sektorske i funkcionalr

- CERT/CSIRT/SOC nacionalna tijela sa svojim nadležn
- Funkcionalna područja kibernetičkog kriminala, kib
- Resorno nadležna ministarstva, regulatorna tijela, g



NCSC HR

Hvala na pažnji!

info@ncsc.hr