Medjunarodni standardi i regulative iz domena informacione bezbednosti

Jovan Bogićević – Cybersecurity Consultant
Jovan.bogicevic@rs.ey.com

The better the question. The better the answer.
The better the world works.

Building a better working world

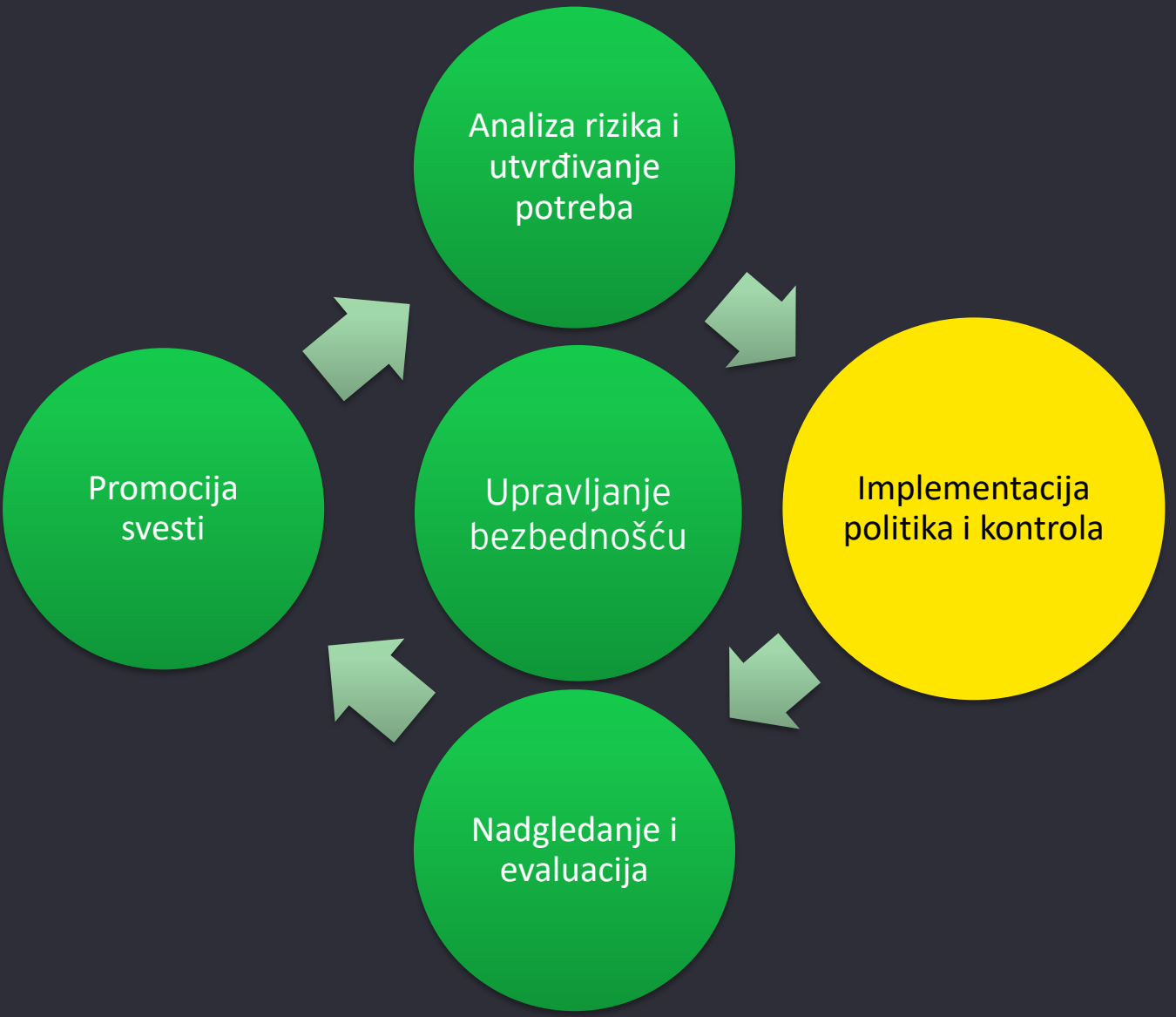
Agenda predavanja

- **Kontrolni okviri**
- **NIST**
- **MITTRE ATT&CK**

- **Medjunardni standardi i regulative**
- **NIS2 directive**
- **DORA**
- **Cybersecurity Act**
- **GDPR**
- **PCI DSS**
- **SOC reporting**

Kontrolni okviri

Upravljanje informacionom bezbednošću (eng. Security governance)



Upravljanje bezbednošću osigurava da su rizici identifikovani i da je adekvatno kontrolno okruženje uspostavljeno radi ublažavanja rizika.

Upravljanje bezbednošću obezbeđuje međusobne odnose između:

- procene rizika
- sprovođenje politika i kontrola kao odgovor na identifikovane rizike
- praćenje efikasnosti kontrola
- promovisanje svesti o očekivanjima

Kontrolni okviri i kontrole

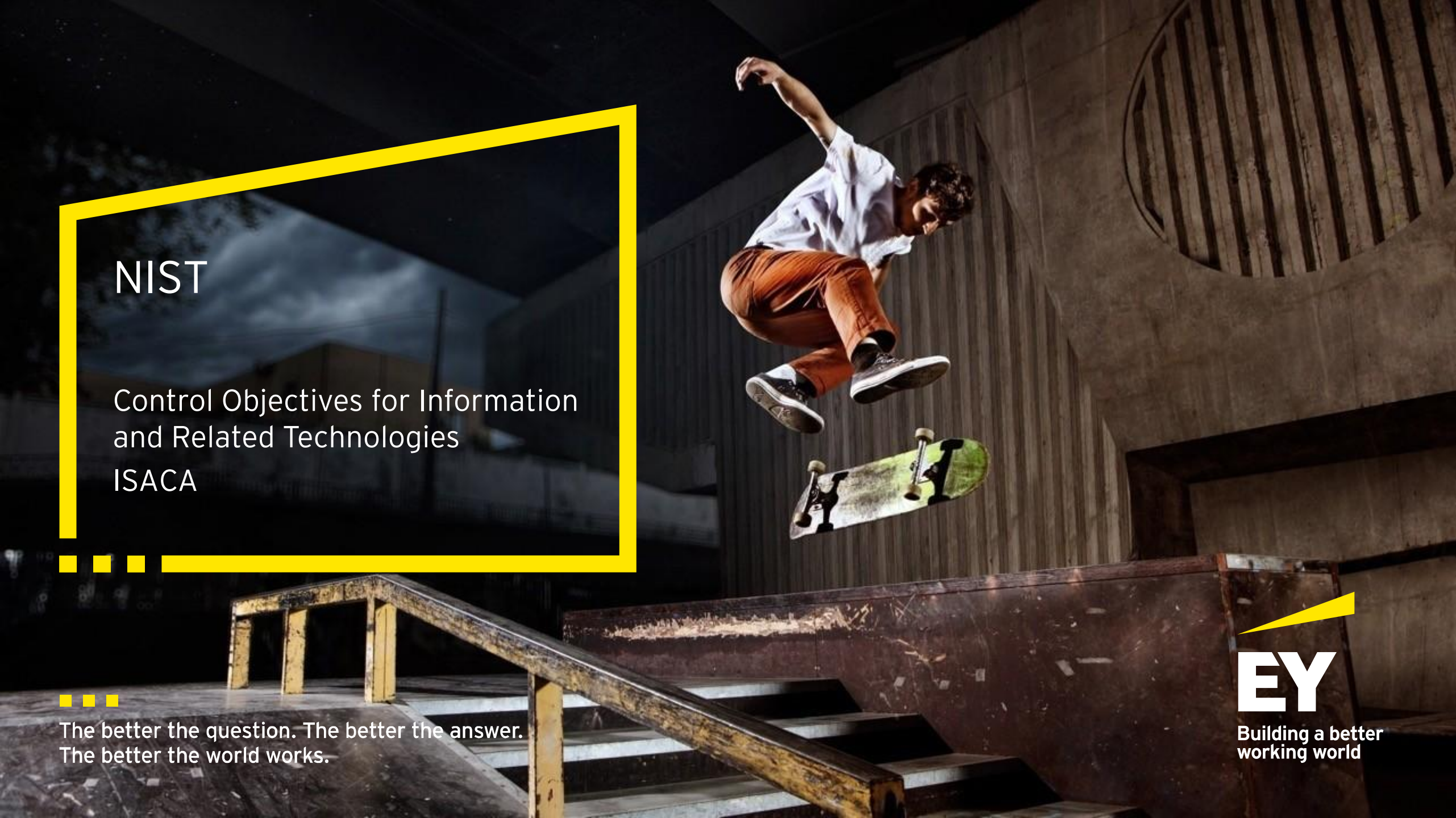
Kontrola, u širem smislu, predstavlja postupke, pravila, standarde i aktivnosti usmerene ka osiguranju da se određeni ciljevi ostvare na način koji je u skladu sa očekivanjima i standardima.

Kontrolni ciljevi: Specifični ciljevi koji se postavljaju kako bi se osiguralo da su procesi u skladu sa poslovnim ciljevima i strategijama upravljanja rizicima.

Kontrolne aktivnosti: Konkretne akcije koje se preduzimaju radi sprovođenja kontrolnih politika, procedura i standarda. Ove aktivnosti osiguravaju da se zadate direktive efektivno sprovode.

IT procesi: COBIT definiše IT procese kao skup aktivnosti i praksi koje se sprovode unutar organizacije kako bi se postigli određeni ciljevi upravljanja i kontrole. IT procesi po COBIT-u su strukturirani u domene i podržavaju sve aspekte IT upravljanja.

Kontrolni okvir pruža sveobuhvatni pristup za razvoj, implementaciju, praćenje i unapređenje praksi upravljanja i kontrole IT-a. Kontrole unutar okvira pomažu u osiguravanju da IT procesi i resursi budu usklađeni sa poslovnim ciljevima, da su rizici adekvatno upravljani, i da se vrednost koju IT pruža optimizuje.



NIST

Control Objectives for Information and Related Technologies

ISACA

The better the question. The better the answer.
The better the world works.

Building a better working world

Razumevanje NIST okvira

•NIST okvir za sajber bezbednost je skup dobrovoljnih smernica, najboljih praksi i standarda koji pomažu organizacijama da upravljaju i smanje rizik od sajber bezbednosti.
•Razvijen od strane Nacionalnog instituta za standarde i tehnologiju (NIST) u saradnji sa industrijom, vladom i akademskom zajednicom.
•Primenjiv na organizacije svih veličina i sektora.
•Cilj mu je da obezbedi zajednički jezik i sistematsku metodologiju za upravljanje rizikom od sajber bezbednosti.

NIST okvir

Funkcije

Funkcije predstavljaju najviši nivo apstrakcije uključen u Okvir. One deluju kao osnova okvira i sastoje se od pet kontinuiranih i paralelnih elemenata. Funkcija Identifikacije je prvi korak u procesu upravljanja sajber bezbednosnim rizicima. Ova funkcija pomaže organizacijama da razviju razumevanje poslovnog konteksta, resursa koji podržavaju kritične funkcije i povezanih sajber bezbednosnih rizika.

Kategorije

Svaka Funkcija je podeljena na Kategorije koje su grupe sajber bezbednosnih ishoda usko povezanih sa programskim potrebama i određenim aktivnostima. Na primer, unutar Funkcije Identifikacije, možete imati kategoriju poput "Upravljanje Imovinom", koja je fokusirana na identifikaciju i upravljanje podacima, osobljem, uređajima, sistemima i objektima.

Potkategorije

Kategorije su dalje podeljene na Potkategorije, koje su specifični ishodi tehničkih i/ili upravljačkih aktivnosti. One pružaju skup rezultata koji, kada se postignu, pomažu u ostvarivanju ishoda u njihovoj odgovarajućoj Kategoriji. Na primer, unutar kategorije "Upravljanje Imovinom", Potkategorija može biti "Fizički uređaji i sistemi unutar organizacije su inventarisani", što ukazuje na specifičnu akciju ili ishod koji doprinosi upravljanju imovinom.

Ključne komponente NIST okvira

Identifikacija (Identify)

Razviti organizaciono razumevanje za upravljanje sajber bezbednosnim rizikom sistema, imovine, podataka i sposobnosti.

- Upravljanje imovinom
- Poslovno okruženje
- Upravljanje
- Analiza rizika
- Strategija upravljanja rizikom
- Upravljanje rizikom snabdevanja
- Upravljanje imovinom

Zaštita (Protect)

Implementirati odgovarajuće zaštitne mere kako bi se osigurala isporuka kritičnih usluga.

- Kontrole pristupa
- Svest i Obuka
- Bezbednost Podataka
- Procesi i Procedure Zaštite Informacija
- Strategija upravljanja rizikom
- Održavanje
- Zaštitna Tehnologija

Detekcija (Detect)

Definisati odgovarajuće aktivnosti za identifikaciju pojave sajber bezbednosnog događaja.

- Anomalije i Događaji
- Stalno Praćenje Bezbednosti
- Procesi Detekcije

Odgovor (Respond)

Preduzeti akciju u vezi sa detektovanim sajber bezbednosnim incidentom.

- Planiranje Odgovora
- Komunikacije
- Analiza
- Ublažavanje
- Unapređenje

Oporavak (Recover)

Razviti i implementirati odgovarajuće aktivnosti za održavanje planova otpornosti i obnovu bilo kojih sposobnosti ili usluga oštećenih usled sajber bezbednosnog incidenta.

- Planiranje Oporavka
- **Poboljšanja**
- **Komunikacije**

NIST – Funkcija Identifikacija

1.Upravljanje Imovinom (ID.AM): Podaci, osoblje, uređaji, sistemi i objekti koji omogućavaju organizaciji da ostvari poslovne ciljeve su identifikovani i upravljani u skladu sa njihovim relativnim značajem za poslovne ciljeve i strategiju upravljanja rizikom.

2.Poslovno Okruženje (ID.BE): Misija, ciljevi, zainteresovane strane i aktivnosti organizacije su razumljivi i prioritetizovani; ove informacije se koriste za informisanje o ulogama, odgovornostima i odlukama o upravljanju sajber bezbednosnim rizikom.

3.Upravljanje (ID.GV): Politike, procedure i procesi za upravljanje i praćenje regulatornih, pravnih, rizika, okolinskih i operativnih zahteva organizacije su razumljivi i informišu upravljanje sajber bezbednosnim rizikom.

4.Procena Rizika (ID.RA): Organizacija razume sajber bezbednosni rizik za operacije organizacije (uključujući misiju, funkcije, imidž ili reputaciju), imovinu organizacije i pojedince.

5.Strategija Upravljanja Rizikom (ID.RM): Prioriteti, ograničenja, tolerancije na rizik i pretpostavke organizacije su uspostavljeni i koriste se za podršku operativnim odlukama o riziku.

6.Upravljanje Rizikom Lanca Snabdevanja (ID.SC): Prioriteti, ograničenja, tolerancije na rizik i pretpostavke organizacije su uspostavljeni i koriste se za podršku odlukama o riziku povezanim sa upravljanjem rizikom lanca snabdevanja. Organizacija ima i koristi procese za identifikaciju, procenu i upravljanje rizicima lanca snabdevanja.

Identifikacija (Identify)

Razviti organizaciono razumevanje za upravljanje sajber bezbednosnim rizikom sistema, imovine, podataka i sposobnosti.

- Upravljanje imovinom
- Poslovno okruženje
- Upravljanje
- Analiza rizika
- Strategija upravljanja rizikom
- Upravljanje rizikom snabdevanja
- Upravljanje imovinom

NIST – Funkcija Zaštita

1. Kontrola Pristupa (PR.AC): Pristup imovini i povezanim objektima je ograničen na ovlašćene korisnike, procese ili uređaje, i na ovlašćene aktivnosti i transakcije.

2. Svest i Obuka (PR.AT): Osoblju i partnerima organizacije se pruža obrazovanje o svesti o sajber bezbednosti i oni su adekvatno obučeni da obavljaju svoje dužnosti i odgovornosti povezane sa sajber bezbednošću u skladu sa povezanim politikama, procedurama i sporazumima.

3. Bezbednost Podataka (PR.DS): Informacije i zapisi (podaci) se upravljaju u skladu sa strategijom rizika organizacije kako bi se zaštitila poverljivost, integritet i dostupnost informacija.

4. Procesi i Procedure Zaštite Informacija (PR.IP): Bezbednosne politike (koje adresiraju svrhu, obim, uloge, odgovornosti, posvećenost menadžmenta i koordinaciju između organizacionih entiteta), procesi i procedure se održavaju i koriste za upravljanje zaštitom informacionih sistema i imovine.

5. Održavanje (PR.MA): Održavanje i popravke komponenti industrijske kontrole i informacionih sistema se izvode u skladu sa politikama i procedurama.

6. Zaštitna Tehnologija (PR.PT): Tehnička bezbednosna rešenja se upravljaju kako bi se osigurala bezbednost i otpornost sistema i imovine, u skladu sa povezanim politikama, procedurama i sporazumima.

Zaštita (Protect)

Implementirati odgovarajuće zaštitne mere kako bi se osigurala isporuka kritičnih usluga.

- Kontrole pristupa
- Svest i Obuka
- Bezbednost Podataka
- Procesi i Procedure Zaštite Informacija
- Strategija upravljanja rizikom
- Održavanje
- Zaštitna Tehnologija

NIST – Funkcija Detekcije i Odgovora

Funkcija Detekcije:

1. Anomalije i Događaji (DE.AE): Anomalna aktivnost se otkriva na vreme i razume se potencijalni uticaj događaja.
2. Stalno Praćenje Bezbednosti (DE.CM): Informacioni sistem i imovina se prate u diskretnim intervalima kako bi se identifikovali sajber bezbednosni događaji i verifikovala efikasnost zaštitnih mera.
3. Procesi Detekcije (DE.DP): Procesi i procedure detekcije se održavaju i testiraju kako bi se osigurala pravovremena i adekvatna svest o anomalnim događajima.

Detekcija (Detect)

- Anomalije i Događaji
- Stalno Praćenje Bezbednosti
- Procesi Detekcije

Funkcija Odgovora:

1. Planiranje Odgovora (RS.RP): Procesi i procedure odgovora se izvršavaju i održavaju kako bi se osigurao pravovremeni odgovor na otkrivene sajber bezbednosne događaje.
2. Komunikacije (RS.CO): Aktivnosti odgovora se koordiniraju sa unutrašnjim i spoljnim zainteresovanim stranama, po potrebi, uključujući spoljnu podršku od strane organa za sprovođenje zakona.
3. Analiza (RS.AN): Vrši se analiza kako bi se osigurao adekvatan odgovor i podržale aktivnosti oporavka.
4. Ublažavanje (RS.MI): Izvode se aktivnosti kako bi se sprečilo širenje događaja, ublažile njegove posledice i iskorenio incident.
5. Poboljšanja (RS.IM): Aktivnosti organizacionog odgovora se poboljšavaju uključivanjem naučenih lekcija iz trenutnih i prethodnih aktivnosti detekcije/odgovora.

Odgovor (Respond)

- Planiranje Odgovora
- Komunikacije
- Analiza
- Ublažavanje

NIST – Funkcija Oporavka

1.Planiranje Oporavka (RC.RP): Procesi i procedure oporavka se izvršavaju i održavaju kako bi se osigurao pravovremeni oporavak sistema ili imovine pogođene sajber bezbednosnim događajima.

2.Poboljšanja (RC.IM): Planiranje i procesi oporavka se poboljšavaju uključivanjem naučenih lekcija u buduće aktivnosti.

3.Komunikacije (RC.CO): Aktivnosti obnove se koordiniraju sa unutrašnjim i spoljnim stranama, kao što su koordinacioni centri, pružaoci internet usluga, vlasnici napadačkih sistema, žrtve, drugi CSIRT timovi i dobavljači.

Oporavak (Recover)

Planiranje Oporavka

Poboljšanja

Komunikacije

MITTRE ATT&CK okvir

The better the question. The better the answer.
The better the world works.

Building a better working world

Uvod u MITTRE ATT&CK okvir

Definicija: MITRE ATT&CK je globalno dostupna baza znanja o taktikama i tehnikama protivnika zasnovana na stvarnim posmatranjima sajber pretnji.

Kreator: Okvir je razvila neprofitna organizacija MITRE kako bi podržala istraživanje i razvoj u oblasti sajber bezbednosti.

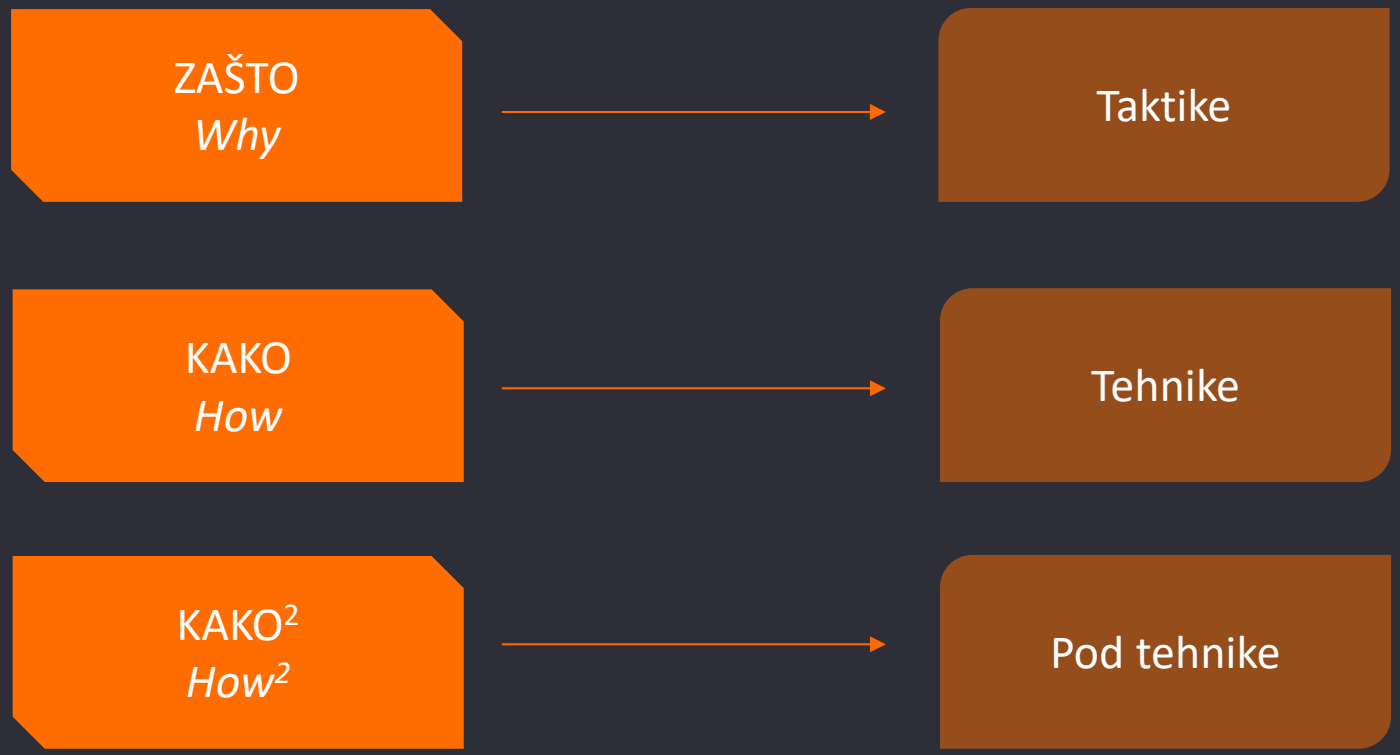
Svrha: Pružanje zajedničke taksonomije za stručnjake iz oblasti sajber bezbednosti kako bi razumeli, diskutovali i delili informacije o ponašanju sajber protivnika.

Upotreba: Modeliranje pretnji, procena bezbednosti, obuka i poboljšanje sajber bezbednosne posture.

Adversarial Tactics, Techniques, and Common Knowledge

Taktike, Tehnike i Zajedničko Znanje Protivnika

Struktura MITTRE ATT&CK okvira



Taktike (eng. Tactics): Predstavljaju "zašto" tehnike ATT&CK. To je taktički cilj protivnika: razlog za izvođenje akcije.

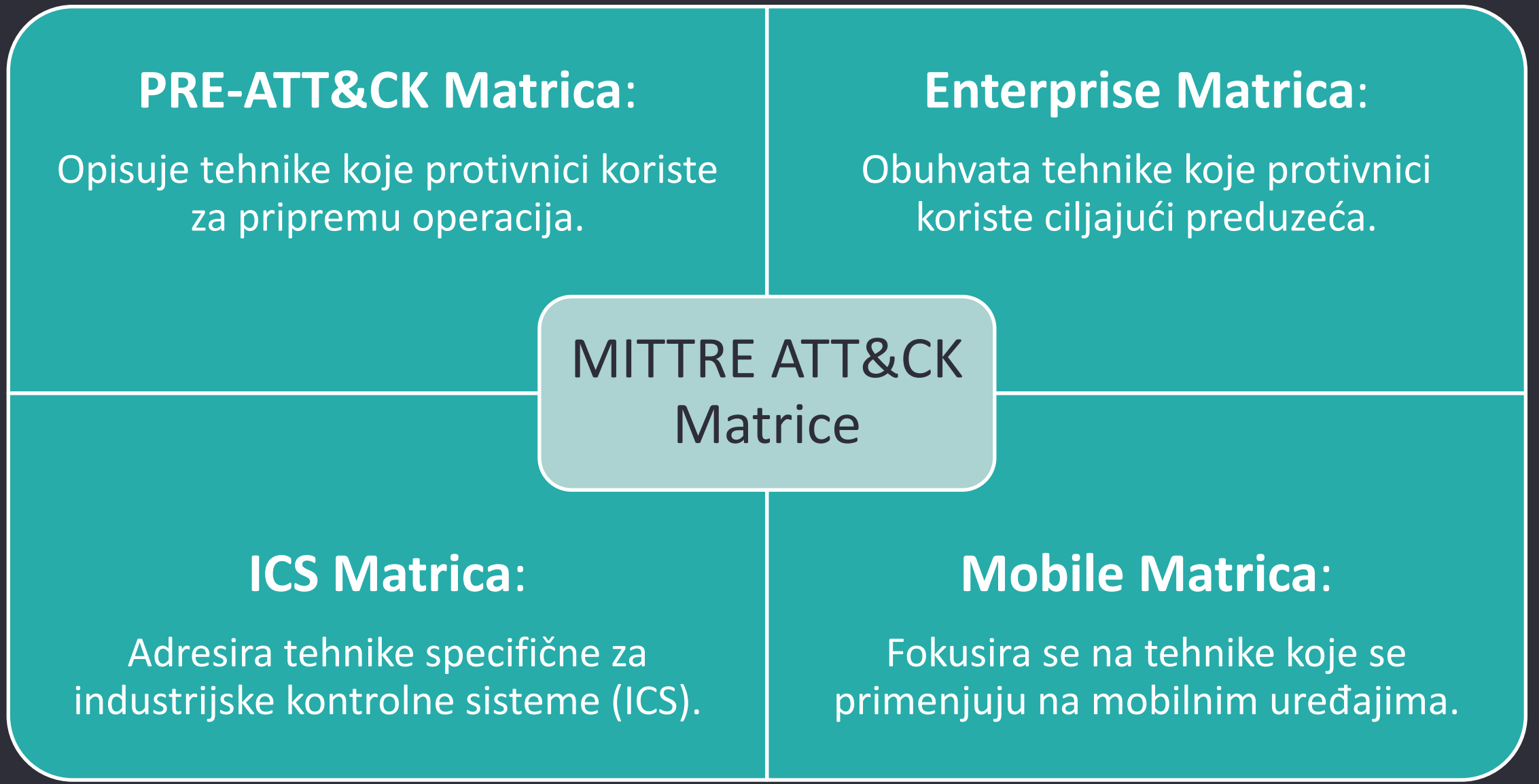
Tehnike (eng. Techniques): Opisuju "kako" protivnik postiže taktički cilj izvođenjem akcije.

Pod tehnike (eng. sub-techniques): Pružaju detaljniji opis metoda koje protivnici koriste za izvođenje tehnike.

Ublažavanja(eng.Mitigations): Predlažu načine za sprečavanje protivnika da izvede tehniku.

Detekcije (eng.Detection): Pružaju smernice o tome kako identifikovati da li je tehnika korišćena.

MITTRE ATT&CK MATRICE



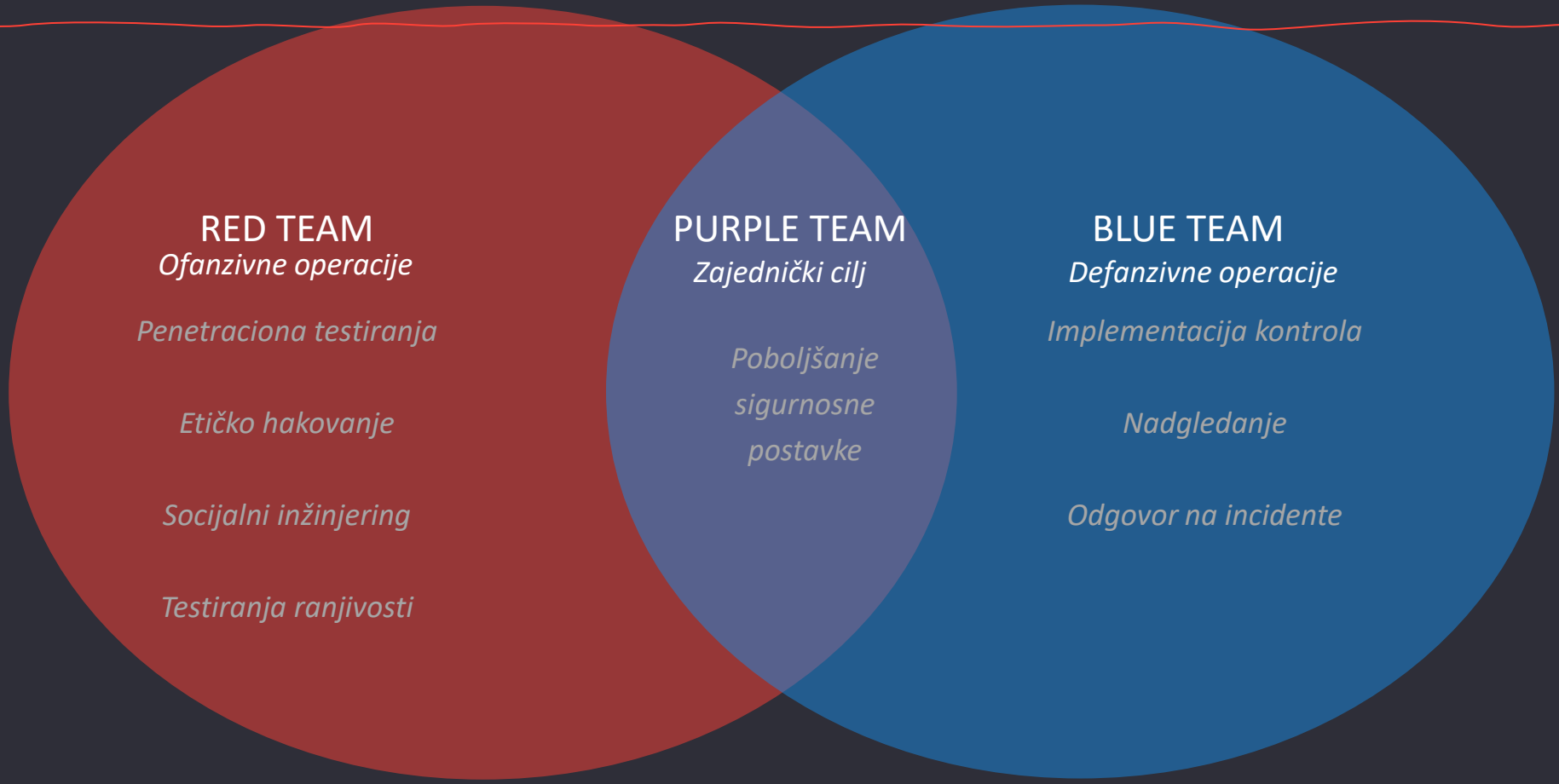
MITTRE ATT&CK U sajber odbrani

MITTRE ATT&CK

•**Red Tim**: Korišćenje ATT&CK za simulaciju ponašanja protivnika i testiranje odbrana.

•**Purple Tim**: Kolaborativni napori gde crveni i plavi timovi koriste ATT&CK za unapređenje bezbednosti.

•**Blue Tim**: Korišćenje ATT&CK za poboljšanje sposobnosti detekcije i odgovora.



Medjunarodne regulative

The better the question. The better the answer.
The better the world works.

Building a better working world

NIS2

The better the question. The better the answer.
The better the world works.

Building a better working world

NIS2 direktiva

1. NIS2 je novi evropski zakon koji ima za cilj povećanje sajber bezbednosti u regionu. Glavni cilj je povećanje otpornosti mrežnih i informacionih sistema za privatne i javne entitete u relevantnim sektorima.
2. Ako ste važan ili suštinski entitet u EU, imate rok do 17. oktobra 2024. godine da sprovedete obaveze navedene u direktivi. A ako pružate suštinsku ili važnu uslugu u EU iz zemlje EEA, mogli biste biti obavezani istim rokom.
3. Ako ne ispunite zahteve NIS2, možete se suočiti sa kaznom vezanom za promet u prethodnoj finansijskoj godini, u zavisnosti od tipa entiteta i prekršaja. Službeno telo je obezbedilo mehanizam sličan onom koji se koristi za kršenje GDPR-a

Important entities

NIS2 definiše dve kategorije za zemlje koje obuhvata: suštinske i važne

Suštinske kategorije:

Transport	**Energija**	**Bankarstvo**	**Finansijska tržišta**	**Snadbevanje vodom**
Digitalna infrastruktura	**Otpadne vode**	**Zdravstvo**	**Javna administracija**	**Prostor**

Važne kategorije:

Pošta I kurirske službe	**Proizvodnja**	**Waste management**	**Proizvodnja, prerada i distribucija hrane**
Digitalni pružaoci usluga	**Proizvodnja i distribucija hemikalija**		**Istraživanje**

Primena na vašu kompaniju zavisiće od sektora i obuhvata. Analiza uticaja na poslovanje bi trebalo da to utvrdi

Entiteti u obe kategorije će morati da ispunjavaju iste zahteve. Međutim, razlika će biti u nadzornim merama i kaznama.

Bitno: veliki energetski kriterijumi koji se primenjuju na NIS2

- Entiteti sa brojem zaposlenih većim od 250 ili prihodom većim od 50 miliona evra.
- Evropa se suočava sa isprepletenim izazovima rastuće potražnje za energijom i zaštitom svoje energetske infrastrukture od sajber pretnji.
- Neuspeh u povezanoj mreži može poremetiti ključne usluge.
- U sred geopolitičke neizvesnosti, rizik od destabilizacije energetske ravnoteže Evrope je realna briga.

Direktiva NIS2 ima za cilj unapređenje mera bezbednosti i proširenje njihovog obuhvata kako bi se rešili ovi problemi.

The NIS2 direktiva | zahtevi

Osnovni zahtevi u odnosu na opseg

Bitni i važni entiteti treba da preduzmu odgovarajuće i proporcionalne tehničke, operativne i organizacione mere kako bi upravljali rizicima koji ugrožavaju bezbednost mrežnih i informacionih sistema. Ovo se obično operacionalizuje putem poslovnog holističkog ISMS-a koji obuhvata oblast NIS2.

Sistem upravljanja Inf. Bezbednošću (ISMS)

Napomena: Imajte na umu da numerički redosled naveden u ovoj slici ne ukazuje na bilo koji specifični sekvencijalni proces ili hijerarhijski prioritet u vezi sa elementima sistema upravljanja bezbednošću informacija.

DORA
Digital Operation Resilience Act

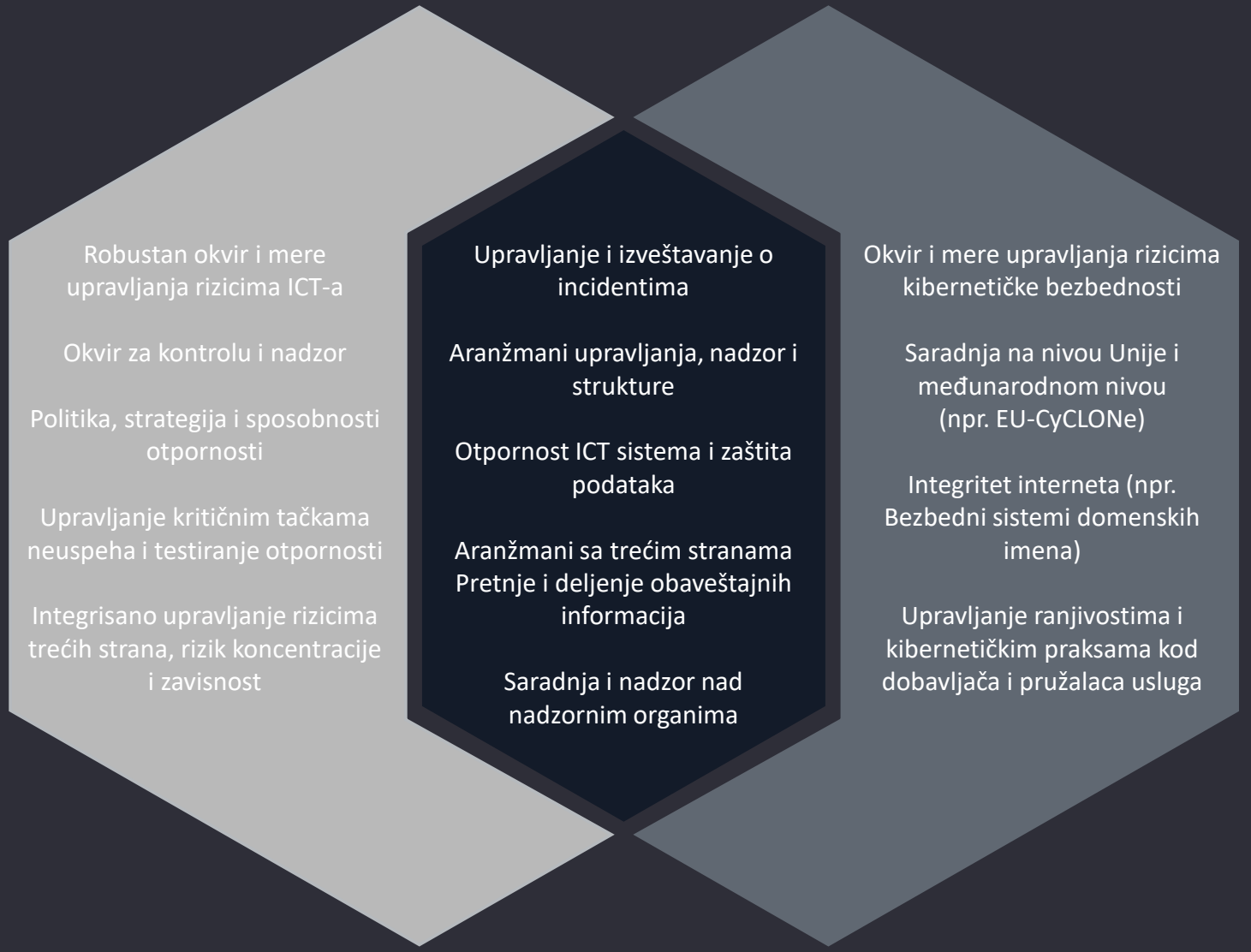
The better the question. The better the answer.
The better the world works.

Building a better working world

DORA, poseban zakon NIS2 direktive (finansijske institucije)

DORA

- Fokusiran je na organizacije u finansijskoj industriji.
- Usredsređen je na upravljanje ICT, rizike, otpornost i outsourcing ICT-a.
- Propisuje procedure, kontrole.
- Unapređeno testiranje i fokus na testiranju kontinuiteta i bezbednosti pod stresom.
- Fokus je na koncentracionim rizicima i izveštavanju/očekivanju incidenata.
- DORA se oslanja na NIS direktivu i adresira moguće preklapanje putem izuzeća lex specialis.



NIS2

- Fokusira se na nacionalni, nivo EU i međunarodni nivo i primenjuje se na različite industrije.
- Osnova za upravljanje rizicima kibernetičke bezbednosti i obaveze izveštavanja, fokusirana na mrežnu bezbednost i bezbednost informacija od suštinskog i važnog značaja.
- Fokusira se na mnoge autoritativne entitete poput CISRT-a, ENISA-e i Komisije.
- Fokusira se na usklađivanje politika, autoritativnih procesa kibernetičke bezbednosti na nacionalnom nivou.

Pregled DORA regulatornih oslonaca

Upravljanje

- Centralna uloga upravnog tela u usvajanju, upravljanju i praćenju internog okvira za upravljanje rizicima ICT-a;
- Ovlašćenje odgovornosti za interne ICT funkcije;
- Pratiti pravilnu primenu internih politika i procesa upravljanja rizicima ICT-a;
- Kontinuirano izveštavanje od strane ICT funkcija o incidentima i sprovedenim korektivnim rešenjima.

ICT upravljanje rizikom i kontinuitet poslovanja

- Procesi i procedure za integrisanu procenu i upravljanje rizicima, analizu pretnji, tolerancije na uticaj
- Tehničke i organizacione mere za zaštitu od i prevenciju ICT/kibernetičkih rizika, uključujući prediktivno praćenje i rano otkrivanje anomalija.
- Kontinuirano unapređenje, analiza korena problema i post-mortem analiza incidenata.
- Kontinuitet poslovanja, strategije za rezervne kopije i oporavak poslovanja nakon katastrofe.

Prijava incidenta i deljenje informacija

- Definicija i implementacija procesa i procedura za praćenje, upravljanje i evidentiranje ICT/kibernetičkih incidenata.
- Klasifikacija incidenata na osnovu pragova značajnosti definisanih od strane nadležnih organa.
- Izveštavanje o ICT incindentima nadležnim organima na osnovu ozbiljnosti.
- Transparentnost na tržištu.

Testiranje digitalne operativne otpornosti

- Osnovno testiranje za sve finansijske entitete.
- Napredno testiranje za značajne finansijske entitete (kriterijumi će biti definisani). Testiranje uključuje testiranje penetracije vođeno pretnjom.
- Definicija sveobuhvatnog programa testiranja digitalne operativne otpornosti uključujući kibernetičke aspekte i uključujući logiku TIBER-EU.

Rizik od trećih strana u vezi sa ICT-om

- Pregled postojećih ugovora o outsourcingu i snabdevanju sa pružaocima usluga ICT/kibernetičkih usluga pružanjem uniformnih minimalnih klauzula za različite učesnike na tržištu finansijskih usluga.
- Sastavljanje novih ugovora prema istim minimalnim klauzulama.
- Usvajanje strategije za praćenje i upravljanje rizicima koji proizilaze iz pružalaca usluga trećih strana.
- Održavanje i ažuriranje registra sa informacijama o svim ugovorima sa trećim dobavljačima ICT-a.

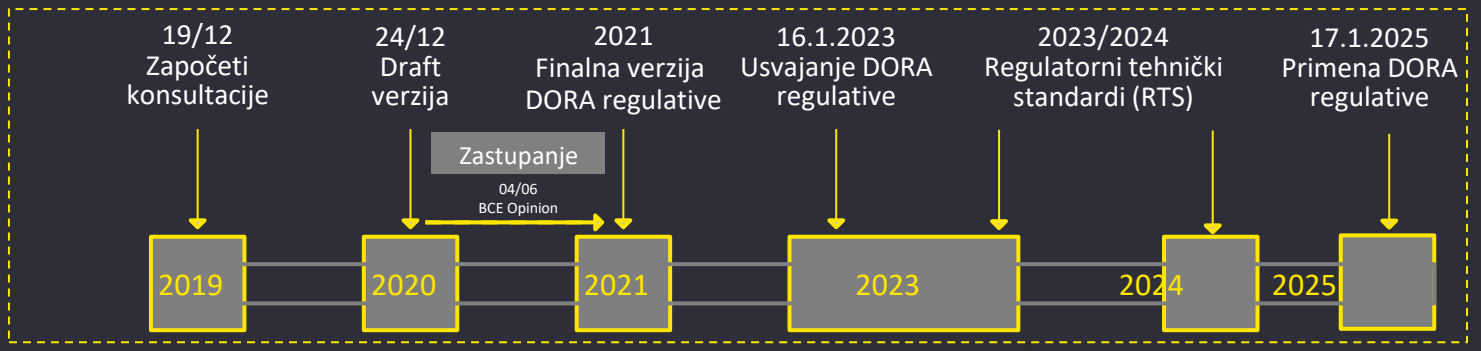
DORA, regulatorna putanja i primenljivost: šta je potrebno nadgledati?

*[…] Osnovni karakter predloženog EU DORA regulativa: **kibernetička bezbednosna revolucija za finansijski sistem EU**, sa izazovnim zajedničkim ciljevima. Trenutno **podizanje regionalnog standarda**, čineći EU finansijski sistem jačim i sa globalnim posledicama.*

Primenljivost

- DORA se primenjuje na oko 22.000 entiteta u oblasti finansijskih usluga (uključujući pružaoce usluga trećih strana u oblasti ICT-a).
- Opseg DORE obuhvata entitete u tradicionalnom finansijskom sektoru kao što su kreditne institucije, berze i klirinške kuće, alternativni menadžeri fondova, upravne kompanije, osiguravajuće kompanije, institucije za plaćanje, institucije za elektronski novac, kao i pružaoce usluga kriptovaluta, izdavaoce kripto-sredstava i izdavaoce tokena.

Zakonodavni prioces



GDPR

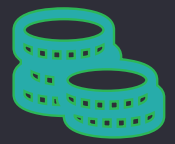
The better the question. The better the answer.
The better the world works.

Building a better working world

GDPR - uvod

Opšta uredba o zaštiti podataka (GDPR) je regulativa u zakonodavstvu EU o zaštiti podataka i privatnosti za sve pojedince koji su građani Evropske unije (EU) i Evropskog ekonomskog prostora (EEA). Takođe se bavi prenosom ličnih podataka van područja EU i EEA. GDPR ima za cilj pre svega da omogući pojedincima kontrolu nad njihovim ličnim podacima i da pojednostavi regulatorno okruženje za međunarodno poslovanje unifikacijom regulative unutar EU.

Opšta uredba o zaštiti podataka (GDPR) usvojena je 14. aprila 2016. godine i počela je da se primenjuje od 25. maja 2018. godine.



GDPR navodi da manje prekršaje mogu rezultirati kaznama do 10 miliona evra ili dva odsto globalnog prometa firme (što je god veće). Oni sa ozbiljnijim posledicama mogu imati kazne do 20 miliona evra ili četiri odsto globalnog prometa firme (što je god veće).

GDPR – aspekti i izazovi

GDPR utiče na organizacije na četiri nivoa

Pravni

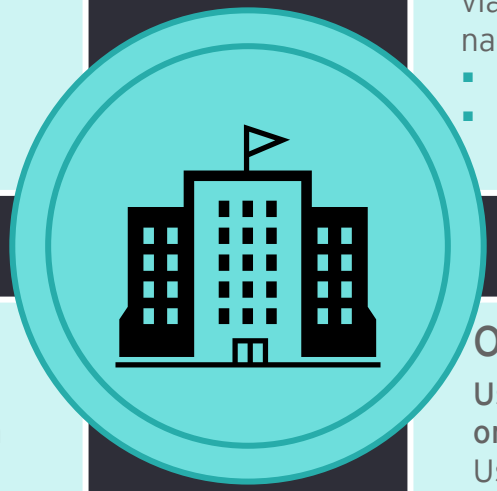
Interpretacija pravnog okvira:
Prenos zahteva za privatnost podataka u interne politike i spoljne komunikacione okvire kako bi se postigla usklađenost sa regulativom:

- Okvir za zaštitu podataka
- Izričita saglasnost

Poslovni model

Procena uticaja na poslovanje:
Procena uticaja na poslovni model kompanije. Koji protoci podataka su dopušteni? Kako to utiče na vlastite/spoljne delatnosti? Kako to utiče na izvore prihoda?

- Poslovni modeli
- Ugovori s pružaocima usluga



Tehnologija

Izbor pravih alata:
Implementacija tehnologije potrebne za osiguranje privatnosti podataka. Kako sprovoditi kontrole u svakom trenutku?

- Prenosivost podataka
- Ograničavanjem obrade
- Pravo na zaborav
- Povreda podataka
- Upravljanje trećom stranom

Organizacija

Uspostava zaštite podataka u organizaciji:
Uspostava provera kako bi se osigurala usklađenost tokom celog procesa. Koji deo organizacije će biti zadužen za zaštitu ličnih podataka?

- Privatnost pri projektovanju
- Procena uticaja na privatnost
- Službenik za zaštitu podataka

Koncept privatnosti predstavlja kontrolu nad podacima o ličnosti

Podaci o ličnosti

„Podatak o ličnosti" je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta

Ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta;

Primer

- Podaci o ličnosti (ime, JMBG, državljanstvo)
- Kontakt podaci (adresa, privremena adresa, broj telefona, e-mail adresa)
- Podaci o zdravstvenom stanju (sposobnost za rad, istorija bolesti, bolovanje)
- IP adresa, logovi pretrage, paterni ponašanja, itd.

Zašto je ovo važno za nas?

Kako bi na pravi način i u skladu sa zakonom vršili obradu podataka o ličnosti neophodno je da prepoznamo podatke o ličnosti i procese ili situacije u kojoj se vrši obrada podataka o ličnosti

Obrada posebnih vrsta podataka o ličnosti

Posebna vrsta podataka

- **Obrada podataka o ličnosti** je svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima, kao što su **prikupljanje**, **beleženje**, **razvrstavanje, grupisanje, odnosno strukturiranje, pohranjivanje, upodobljavanje ili menjanje, otkrivanje, uvid, upotreba, otkrivanje prenosom**, odnosno dostavljanjem, umnožavanje, širenje ili na drugi način činjenje dostupnim, upoređivanje, ograničavanje, brisanje ili uništavanje
- Obrada posebnih vrsta podataka zahteva veću zaštitu i zabranjena je sem u specifičnim uslovima koji su definisani zakonom.

Kategorije

Rasno ili etničko poreklo	Političko mišljenje, versko ili filozofsko uverenje	Članstvo u sindikatu
Genetski i biometrijski podaci	Podaci o zdravstvenom stanju	Podaci o seksualnom životu ili seksualnoj orijentaciji

Zašto je ovo važno za nas?

Važno je biti svestan koji podaci o ličnosti su kategorisani kao „podaci o ličnosti posebne vrste“ s obzirom da je generalno zabranjena obrada tih podataka sem u specijalnim slučajevima

Zakonitost obrade

Osnov za obradu

Saglasnost za obradu

Neophodno za izvršenje ugovora

Zaštita životno važnih interesa lica

Obavljane poslova od javnog interesa

Zakonska obaveza

Legitimni interes

Zašto je ovo važno za nas?

- Podaci o ličnosti se mogu obrađivati kada postoji zakonska osnova obrade
- Za svaku obradu podataka koja prevazilazi zakonom definisane osnove potrebno je prikupiti eksplicitnu saglasnost lica za obradu podataka

Zakon o zaštiti podataka u Zapadni Balkan

Država	Naziv zakona	Zakon zvanično usvojen	Započeto sprovođenje	Usklađenost sa GDPR-om
Srbija	Zakon o zaštiti ličnih podataka	13. November 2018.	21. August 2019.	**Da**
Kosovo	Zakon 06/L-082 o zaštiti ličnih podataka	14. Feb 2019	12. March 2019.	**Da**
Bosna i Hercegovina	Zakon o zaštiti ličnih podataka	23. May 2005. (last amended 2011.)	25. May 2006.	Ne
Crna Gora	Zakon o zaštiti ličnih podataka	23. dec 2008. (Last amended 2017.)	1 January 2009 (sa 6 meseci periodom usklađivanja – 1 June 2009)	Ne
Albanija	Zakon o zaštiti ličnih podataka broj.9887	10. mar 2008. (Last time amended 2014.)	21. mar 2008.	Ne
Severna Makedonija	Zakon o zaštiti ličnih podataka broj.42/40	16. February 2020.	24. February 2020.(sa 18 meseci periodom usklađivanja 24. August 2021.)	**Da**

**centar za istraživanje prava I digitalizacije*

GDPR i ZZPL (Zakon o zaštiti podataka o ličnosti) – Ključne razlike

GDPR	ZZPL
Kazne mogu iznositi do 20 miliona evra u prihodu ili 4% godišnjeg prihoda kompanije.	Najviša kazna u iznosu od 2 milliona RSD
Sadrži preambulu od 173 tačke koja dodatno razrađuje pravne norme i objašnjava svrhu odredbi GDPR-a.	Preambula je izostavljena, što dodatno otežava primenu Zakona o zaštiti podataka o ličnosti (na primer, zahtev "Privatnost dizajna" postoji u lokalnom zakonu, ali nije detaljno opisan kao u GDPR-u).
On reguliše način na koji se podaci izvoze izvan granica Evropske unije.	On reguliše izvoz svih podataka sa teritorije Srbije i postoje razlike u vezi sa pravnom osnovom za transfer ličnih podataka.

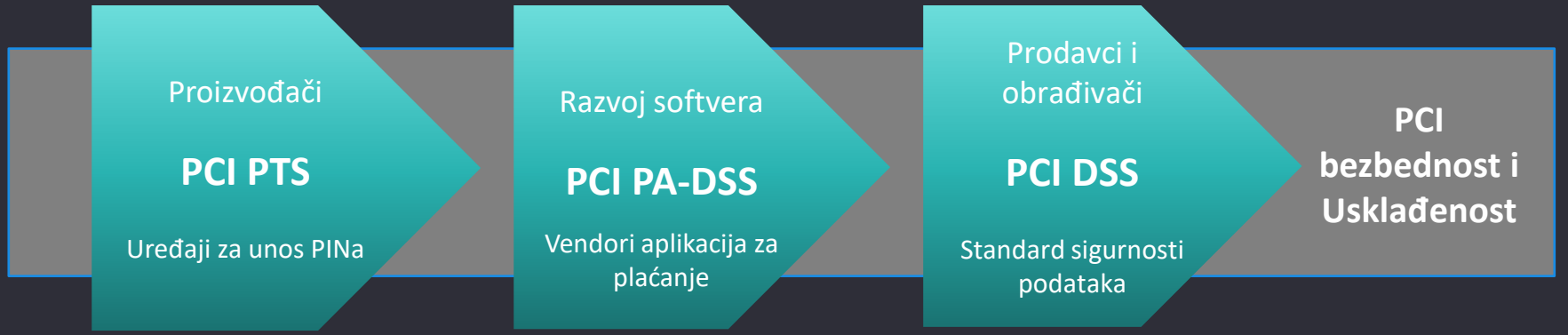
PCI DSS

The better the question. The better the answer.
The better the world works.

Building a better working world

Payment Card Industry Security Standards

Zaštita podataka vlasnika kartica



PCI DSS
Data Security Standard

PCI Standard za sigurnost podataka: Odnosi se na bilo koju entitet koji čuva, obrađuje i/ili prenosi podatke vlasnika kartice. Ako vaša firma prihvata ili obrađuje platne kartice, mora biti u skladu sa PCI DSS.

PA DSS
Payment Application

Standard bezbednosti podataka za platne aplikacije: Odnosi se na razvojne programere i integratore aplikacija koje čuvaju, obrađuju i/ili prenose podatke vlasnika kartica. Takođe se odnosi na aplikacije koje se prodaju, distribuiraju ili licenciraju trećim stranama.

PCI PTS
PIN Transaction Security

Zahtevi za sigurnost transakcija sa PIN-om: PCI PTS se odnosi na proizvođače koji definišu i implementiraju karakteristike uređaja i upravljanje za terminale za unos ličnog identifikacionog broja (PIN) koji se koriste za finansijske transakcije platnim karticama.

Payment Card Industry Data Security Standards (PCI-DSS)
Uvod u standard

O standardu:

- Standard održava Savet za sigurnosne standarde PCI (PCI Security Standards Council, LLC - PCI SSC), koji su osnovali American Express, Discover Financial Services, JCB, MasterCard Worldwide i Visa International.
- Primjenjuje se na sve članove i njihove agente (trgovce i pružaoce usluga) koji čuvaju, obrađuju ili prenose podatke vlasnika kartica na osnovu njihovih obima.
- Definiše zahteve za sigurnost i prakse za zaštitu informacija o računu i transakcijama.

Primenljivost i usklađenost:

- PCI DSS se primenjuje gde god se podaci o računu čuvaju, obrađuju ili prenose. Podaci o računu sastoje se od
    - Podataka o vlasniku kartice
    - Osetljivi podaci za autentifikaciju

Podaci o vlasniku kartice	Osetljivi podaci za autentifikaciju
▸ Primarni broj kartice (PAN) ▸ Ime nosioca kartice ▸ Datum isteka ▸ Servisni broj	▸ Podaci sa magnetne trake ili ekvivalent sa čipa kartice ▸ CAV2/ CVC2/ CVV2/ CID ▸ PINs/ PIN blokovi

Payment Card Industry Data Security Standards (PCI-DSS)
Zahtevi

Skeniranje mrežne sigurnosti

- Proces kojim se na daljinu proveravaju ranjivosti sistema entiteta korišćenjem ručnih ili automatizovanih alata. Sigurnosna skeniranja uključuju ispitivanje internih i eksternih sistema i izveštavanje o uslugama izloženim mreži. Skeniranja mogu identifikovati ranjivosti u operativnim sistemima, uslugama i uređajima koji bi mogli biti iskorišćeni od strane zlonamernih pojedinaca.

Usaglašenost sa PCI-DSS

- Trgovci i drugi entiteti koji čuvaju, obrađuju i/ili prenose podatke vlasnika kartica moraju biti u skladu sa PCI DSS.
- U zavisnosti od klasifikacije entiteta ili nivoa rizika (koji određuju pojedinačni brendovi platnih kartica), slede se sledeći procesi:
  - PCI DSS Određivanje obima – odrediti koje komponente sistema su pod upravom PCI DSS
  - Procena – ispitati usklađenost komponenti sistema u obimu
  - Kompenzacione kontrole – procenitelj validira alternativne tehnologije/kontrolne procese
  - Izveštavanje – procenitelj i/ili entitet podnosi potrebnu dokumentaciju
  - Pojašnjenja – procenitelj i/ili entitet pojašnjava/ažurira izjave iz izveštaja (ako je primenljivo) na zahtev banke koja ih je stekla ili brenda platne kartice.

Zahtevi

Izgradnja i održavanje sigurne mreže

- Zahtev 1: Instalirati i održavati konfiguraciju fajervola za zaštitu podataka
- Zahtev 2: Ne koristiti podrazumevane lozinke i druge sigurnosne parametre koje pruža dobavljač Sistema

Zaštita podataka vlasnika kartice

- Zahtev 3: Zaštiti čuvane podatke vlasnika kartice
- Zahtev 4: Šifrovati prenos podataka vlasnika kartice i osetljivih informacija preko javnih mreža

Održavanje programa upravljanja ranjivostima

- Zahtev 5: Koristiti i redovno ažurirati antivirusni softver
- Zahtev 6: Razvijati i održavati sigurne sisteme i aplikacije

Sprovođenje snažnih mera kontrole pristupa

- Zahtev 7: Ograničiti pristup podacima vlasnika kartice prema poslovnoj potrebi za znanjem
- Zahtev 8: Dodeliti jedinstveni ID svakoj osobi sa pristupom računaru
- Zahtev 9: Ograničiti fizički pristup podacima vlasnika kartice

Redovno praćenje i testiranje mreža

- Zahtev 10: Pratiti i nadgledati sav pristup mrežnim resursima i podacima vlasnika kartice
- Zahtev 11: Redovno testirati sigurnosne sisteme i procese

Održavanje politike informacione sigurnosti

- Zahtev 12: Održavati politiku informacione sigurnosti"

SOCR
Service Organisation Controls reporting

The better the question. The better the answer.
The better the world works.

Building a better working world

Revizije SOC-a i vrste izveštaja

(Service Organization Control - SOC) pomažu kompanijama da uspostave poverenje i sigurnost u svoje procese isporuke i kontrole. SOC pregled pomaže organizacijama da izveštavaju o efikasnosti svojih internih kontrola i zaštita pružajući nezavisne i korisne povratne informacije.

SOC 1

Prvo finansije

Bavi se internim kontrolama nad finansijskim izveštavanjem

SOC 2

Poverenje je dvosmerno

Bavi se bezbednosnim kontrolama

SOC 3

Javni SOC 2 izveštaj

Izmenjen SOC 2 report, što znači da je namenjen za javnost.

SOC za sajber

Sajber bezbednost

Pokazuje na koji način organzacija postiže sajber zahteve.

Koristiti kriterijume usluga poverenja,

Revizije SOC-a i vrste izveštaja

PRIVATNOST
- Kontrola pristupa
- Dvofaktorska autentikacija
- Enkripcija

INTEGRITET OBRADE
- Osiguravanje kvaliteta
- Monitoring procesa

SIGURNOST
- Network/application firewalls
- Dvofaktorska autentikacija
- Detekcija upada

DOSTUPNOST
- Monitoring performansi
- Oporavak poslovanja nakon katastrofe
- Postupanje u slučaju bezbednosnog incidenta

POVERLJIVOST
- Enkripcija
- Kontrola pristupa
- Mreža/aplikacija firewalls

**eng. Trust service criteria*

SOC 2 i SOC 3

Oba izveštaja **SOC 2** i **SOC 3** sprovode se prema standardima SSAE 18*, kako je navedeno od strane AICPA. SOC 2/3 definiše kriterijume za upravljanje podacima klijenata na osnovu pet "principa usluga poverenja" - bezbednosti, dostupnosti, integritet obrade, poverljivosti i privatnosti.

Za razliku od PCI DSS-a, koji ima vrlo stroge zahteve, izveštaji SOC 2 su jedinstveni za svaku organizaciju. U skladu sa specifičnim poslovnim praksama, svaka organizacija dizajnira svoje kontrole kako bi ispunila jedan ili više od principa poverenja

SOC 3 izveštaj je u osnovi izveštaj SOC 2 sa obrisanim informacijama. Namenjen je javnosti i obično je dostupan na veb stranici organizacije. Obzirom da SOC 2 izveštaj koristi kriterijume usluga poverenja, i SOC 3 će ih sadržati.

Ključne razlike

Izveštaj	SOC 2	SOC 3
Tip izveštaja	Tip I I Tip II	Tip II
Nivo detalja	Uključuje detaljne opise revizorskih kontrolnih testova, test procedura, ili test rezultata	Ne obuhvata detaljne opise revizorskih kontrolnih testova, test procedura, ili test rezultata
Mišljenje revizora	Da	Da
Privatnost	Privatni izveštaj (podeljeno samo sa klijentom)	Javni izveštaj – opšta svrha korišćenja (npr. Sajt organizacije)
Šta pokriva?	Interne kontrole za principe usluge poverenja	SOC 2 rezultati, krojeni za opštu populaciju
Kojim organizacijama je potreban?	Organizacije koje skladište, obrađuju ili prenose bilo kakve vrste podataka o korisnicima	Organizacije koje zahtevaju SOC 2, a žele da koriste usklađenost u marketinške svrhe prema široj javnosti

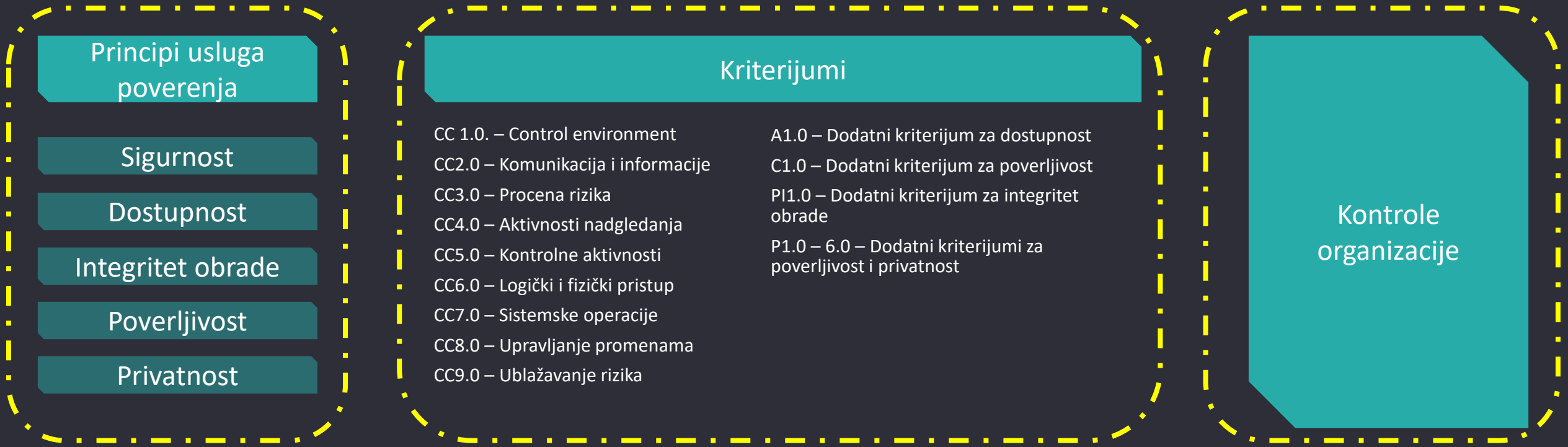
SOC 2 and SOC 3

Opseg i ciljevi SOC2 i SOC3

Pokazati da je organizacija uspostavila interne kontrole koje pokrivaju definisane principe poverenja usluga. Obim je definisan na osnovu postavljenih kriterijuma, fokalnih tačaka i internih kontrola.

Gde su kontrole u SOC2 i SOC3?

Jedini kriterijum koji je potreban za SOC 2 pregled je kriterijum sigurnosti, koji se takođe naziva i opštim kriterijumom. Kriterijum sigurnosti se naziva opštim kriterijumom jer se mnogi kriterijumi koji se koriste za evaluaciju sistema dele među svih pet Principa usluga poverenja



Pitanja