Okvir dobrih praksi

za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti

Verzija 1.0.

Listopad, 2019.

Sadržaj

Uvod

Hrvatski sabor je na sjednici održanoj 6. srpnja 2018. godine donio Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) (u daljnjem tekstu Zakon).

Cilj je ovog Zakona osigurati visoku razinu kibernetičke sigurnosti u pružanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti. Zakonom se uređuju postupci i mjere za postizanje tog cilja, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata i tehničkog tijela za ocjenu sukladnosti te nadzor provedbe i prekršajne odredbe.

Sektori obuhvaćeni Zakonom su energetika (električna energija, nafta, plin), prijevoz (zračni, željeznički, vodni, cestovni), bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba vodom za piće i njezina distribucija, digitalna infrastruktura, digitalne usluge te poslovne usluge za državna tijela.

Vlada Republike Hrvatske je temeljem Zakona, na sjednici održanoj 26. srpnja 2018. godine, donijela Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/2018) (u daljnjem tekstu Uredba).

Uredbom su utvrđene mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga, način njihove provedbe, kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti i druga bitna pitanja za obavještavanje o incidentima.

O Dokumentu

Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti (u daljnjem tekstu Dokument) predstavlja smjernice, preporuke i dobre prakse za ostvarivanje sukladnosti s mjerama sigurnosti operatora ključnih usluga opisanim u drugom dijelu Uredbe. Svrha ovog dokumenta je dvojaka. Osnovna mu je namjena služiti kao implementacijski vodič za operatore ključnih usluga prilikom ostvarivanja sukladnosti s mjerama sigurnosti, ali istodobno i kao vodič za nadležna sektorska tijela, tehnička tijela za ocjenu sukladnosti, vanjske i interne revizore koji će provoditi nadzor ili ocjenjivanje sukladnosti kod operatora ključnih usluga.

Dokument je temeljen na postojećim nacionalnim i međunarodnim regulatornim okvirima, normama i preporukama koje se odnose na područje izgradnje i upravljanja sustavima informacijske sigurnosti među kojima su:

- Technical Guidelines for the implementation of minimum security measures for Digital Service Providers
- ISO 27001
- NIST
- PCI-DSS
- Smjernice za upravljanje informacijskim sustavom Hrvatske narodne banke
- Indicators of Good Practice – NCSC-UK

Dokument će se ažurirati prema potrebama i temeljem iskustava stečenih prilikom procesa provedbe ocjene sukladnosti te će u novim inačicama biti naznačene izmjene.

Opis smjernica

Središnji dio ovog Dokumenta čine smjernice za dostizanje sukladnosti za svaki od članaka Uredbe kojima se propisuju mjere kibernetičke sigurnosti.

Svaka od smjernica sadrži opis postojećeg stanja koje ukazuje na jednu od dvije moguće razine sukladnosti:

- Nesukladnost – ukazuje na izostanak sukladnosti s Uredbom;
- Sukladnost – ukazuje na sukladnost s Uredbom;
- Razina Napredna sukladnost se ne koristi kao razina u formalnom postupku ocjene sukladnosti, već kao mogući smjer daljnjeg napretka operatorima ključnih usluga nakon dostizanja sukladnosti.

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Nisu predočeni dokazi da je mjera sigurnosti primijenjena - Ne postoje naznake da je proces uspostave mjere sigurnosti u tijeku
Sukladnost	- Postoje dokazi da je mjera sigurnosti primijenjena ili da je u visokom stupnju implementacije - Primijenjene su industrijske i stručne norme koje se odnose na specifičnu mjeru sigurnosti - Postoji uspostavljen proces nadzora provođenja sigurnosne mjere koji obuhvaća definirane odgovorne osobe, proces interne revizije mjere sigurnosti i sl.
(Napredna sukladnost)	- Postoje dokazi da su mjere sigurnosti uspostavljene u skladu s najnovijim tehničkim dostignućima koja se koriste u okviru najboljih sigurnosnih praksi - Postoje dokazi implementacije i korištenja naprednih tehničkih rješenja za nadzor, prepoznavanje i sprječavanje naprednih prijetnji kibernetičkoj sigurnosti

Uloga procesa procjene rizika

U postupku ostvarivanja sukladnosti s odredbama koje proizlaze iz Zakona i pripadajuće Uredbe, operatori ključnih usluga moraju kontinuirano i s oprezom procjenjivati trenutno stanje spremnosti i povezane rizike kojima su izloženi. Procjena rizika bi se trebala provoditi kroz čitav životni ciklus ključnih sustava: tijekom definiranja zahtjeva, nabave/razvoja, konfiguracije i uklanjanja.

Procjenom rizika bi operatori trebali donositi odluke o razinama na kojima će primijeniti određenu kontrolu u svrhu smanjenja rizika i ostvarivanja sukladnosti tako da odabiru specifične kontrole, mjere i sofisticirana tehnička rješenja koja će biti efikasna.

U skladu s gore navedenim, za očekivati je da određeni operator neće uspostaviti sustav u kojom će sve mjere imati najviši stupanj složenosti, već će se odluka o složenosti primijenjene mjere donositi u skladu s rezultatima procjene rizika.

Dokument donosi preporuke kako ostvariti sukladnost u smislu minimalnih zahtjeva koje je operator dužan zadovoljiti.

Poglavlje I - UPRAVLJANJE SIGURNOŠĆU MREŽNIH I INFORMACIJSKIH SUSTAVA

I.1 Uspostava i dokumentiranje politike upravljanja (Članak 6. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su uspostaviti i dokumentirati politiku upravljanja sigurnošću ključnih sustava.

(2) Politika upravljanja sigurnošću ključnih sustava mora:

- *definirati ciljeve i strateške smjernice očuvanja kontinuiteta poslovanja*
- *biti temeljena na procjeni i upravljanju rizicima*
- *opisati sustav upravljanja sigurnošću, uključujući interne nadzore provedbe mjera kibernetičke sigurnosti*
- *utvrditi donošenje potrebnih sigurnosno-operativnih procedura za ključne sustave, s poveznicama na druge interne akte koji reguliraju postojeće sigurnosno-operativne procedure, neovisno o tome odnose li se na ključne sustave ili sigurnost operatora u cjelini*
- *uključivati organizaciju i provedbu programa edukacije te stalnog podizanja svijesti o sigurnosti.*

(3) Politika upravljanja sigurnošću ključnih sustava donosi se u pisanom obliku i mora ju odobriti najviša upravljačka razina.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nema formalno usvojenu politiku upravljanja sigurnošću ključnih sustava (ili usporediv interni akt) koja je odobrena od strane Uprave
Sukladnost	- Operator ima formalno usvojenu politiku upravljanja sigurnošću ključnih sustava (ili usporediv interni akt) koja je odobrena od strane Uprave i sadrži sve elemente iz Stavka 2. - Svi zaposlenici koji sudjeluju u upravljanju i/ili koriste ključni sustav su upoznati sa sadržajem politike upravljanja sigurnošću ključnih sustava
Napredna sukladnost	- Operator ima formalno usvojenu politiku upravljanja sigurnošću ključnih sustava koja se redovito ažurira i odobrena je od strane Uprave - Postoje dokumentiran proces ažuriranja politike upravljanja sigurnošću ključnih sustava koji uzima u obzir relevantne promjene u sustavu, prošle računalno-sigurnosne incidente i moguće prijetnje

Mapiranje:

ISO27001: A.5 Information Security policies

NIST: ID.GV-1: Organizational information security policy is established

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel

I.2 Organizacijska struktura (Članak 7. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su odrediti osobu s najvišim rukovodnim ovlastima odgovornu za uspostavu i upravljanje sigurnošću ključnih sustava.

(2) Operatori ključnih usluga dužni su uspostaviti organizacijsku strukturu, s formalnom raspodjelom zadaća, ovlasti i odgovornosti kojom će se osigurati primjereno upravljanje sigurnošću ključnih sustava.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nema uspostavljenu i dokumentiranu organizacijsku strukturu odgovornosti u upravljanju sigurnošću ključnih sustava - Postoje značajni sukobi nadležnosti među dodijeljenim ulogama u sustavu upravljanja sigurnošću ključnih sustava
Sukladnost	- Operator je uspostavio organizacijsku strukturu u kojoj je osoba odgovorna za uspostavu i upravljanje sigurnošću ključnih sustava izravno odgovorna Upravi te postoje dokazi o redovitom informiranju Uprave o predmetnoj temi - Operator je uspostavio organizacijsku strukturu u kojoj osoba odgovorna za uspostavu i upravljanje sigurnošću ključnih sustava posjeduje odgovarajuće kompetencije iz domene informacijske sigurnosti - Postoji dokumentacija o svim ulogama u sustavu upravljanja ključnim sustavima - Ne postoji sukob nadležnosti među dodijeljenim ulogama u sustavu upravljanja sigurnošću ključnih sustava
Napredna sukladnost	- Operator je uspostavio organizacijsku strukturu u kojoj je osoba odgovorna za uspostavu i upravljanje sigurnošću ključnih sustava član Uprave s najvišim rukovodnim

	ovlastima te postoje dokazi o redovitom informiranju Uprave o predmetnoj temi - Postoji dokumentacija o svim ulogama u sustavu upravljanja ključnim sustavima (CISO, DPO, upravitelj kontinuitetom poslovanja, interni revizor) koja se redovito ažurira

Mapiranje:

ISO27001: A.6.1 Internal organization

NIST: ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.4

I.3 Provedba internih nadzora (Članak 8. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su uspostaviti sustav internog nadzora provedbe mjera kibernetičke sigurnosti određenih politikom upravljanja sigurnošću ključnih sustava, pri čemu bi poslovi internog nadzora moraju biti organizacijski odvojeni od organizacijske strukture odgovorne za ključne sustave.

(2) Interni nadzor iz stavka 1. ovoga članka provodi se najmanje jednom godišnje.

(3) Rezultati internog nadzora iz stavka 1. ovoga članka dostavljaju se, u pisanom obliku, odgovornoj osobi iz članka 7. stavka 1. ove Uredbe.

(4) Odgovorna osoba iz članka 7. stavka 1. ove Uredbe dužna je osigurati provedbu mjera kibernetičke sigurnosti u skladu s rezultatima internog nadzora iz stavka 1. ovoga članka.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze o formalnom usvajanju dokumentacije kojom se uspostavlja sustav internog nadzora provedbe mjera kibernetičke sigurnosti - Poslovi internog nadzora nisu organizacijski odvojeni od organizacijske strukture odgovorne za ključne sustave - Operator nije uspostavio proces internog nadzora koji provode osobe s odgovarajućim kompetencijama iz domene informacijske sigurnosti - Operator nije predočio rezultate internog nadzora provedenog u posljednjih 12 mjeseci

Sukladnost	- Operator je predočio dokaze o formalnom usvajanju dokumentacije kojom se uspostavlja sustav internog nadzora provedbe mjera kibernetičke sigurnosti koji je organizacijski odvojen od organizacijske strukture odgovorne za ključne sustave - Operator je uspostavio proces internog nadzora koji provode osobe s odgovarajućim kompetencijama iz domene informacijske sigurnosti - Operator je predočio rezultate internog nadzora provedenog u posljednjih 12 mjeseci - Operator je predočio dokaze da se provedba mjera kibernetičke sigurnosti provodi u skladu s rezultatima internog nadzora
Napredna sukladnost	- Operator je predočio dokaze o provođenju internog nadzora provedbe mjera kibernetičke sigurnosti nakon svake značajne promjene u ključnim sustavima

Mapiranje:

ISO27001: A.6.1 Internal organization

NIST: AU-1 Audit And Accountability Policy And Procedures

Poglavlje II - UPRAVLJANJE RIZICIMA

II.1 Uspostava sustava upravljanja rizicima (Članak 9. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su uspostaviti sustav upravljanja rizicima kojima je izložen ključni sustav.

(2) Sustav upravljanja rizicima iz stavka 1. ovoga članka mora uključivati:

- *metodologiju utvrđivanja rizika od incidenata*
- *određivanje odgovornih osoba za provođenje redovite procjene rizika od incidenata*
- *izradu ili odabir kataloga primjenjivih rizika i njegovo ažuriranje*
- *prihvaćeni način obrade rizika (izbjegavanje, ublažavanje, prijenos ili prihvaćanje rizika)*
- *popis preostalih rizika*
- *postupak donošenja formalne odluke o prihvaćanju preostalih rizika od strane najviše upravljačke razine.*

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze o uspostavi sustava upravljanja rizicima kojima je izložen ključni sustav - Uspostavljeni sustav upravljanja rizicima ne uključuje elemente opisane u Stavku 2. - Operator nije uspostavio proces procjene rizika koji provode osobe s odgovarajućim kompetencijama iz domene informacijske sigurnosti - Operator nije predočio rezultate procjene rizika provedene u posljednjih 12 mjeseci - Ne postoji dokaz o donošenju formalne odluke o prihvaćanju preostalih rizika od strane najviše upravljačke razine
Sukladnost	- Operator je predočio dokaze o uspostavi sustava upravljanja rizicima kojima je izložen ključni sustav - Uspostavljeni sustav upravljanja rizicima uključuje sve elemente opisane u Stavku 2. - Operator je uspostavio proces procjene rizika koji provode osobe s odgovarajućim kompetencijama iz domene informacijske sigurnosti - Operator je predočio rezultate procjene rizika provedene u posljednjih 12 mjeseci

	- Operator je predočio dokaz o donošenju formalne odluke o prihvaćanju preostalih rizika od strane najviše upravljačke razine
Napredna sukladnost	- Operator je predočio dokaze o provođenju postupka procjene rizika nakon svake značajne promjene u ključnim sustavima - Operator je predočio dokaze kojima se potvrđuje da najviša rukovodna razina redovito analizira i osigurava provedbu mjera kibernetičke sigurnosti u skladu s rezultatima procjene rizika

Mapiranje:

ISO27001: ISO27001:2013

NIST: RA-1 Risk Assessment policy and procedures

PCI DSS: 12.1.2

II.2 Procjena rizika (Članak 10. i 11. Uredbe)

Zahtjev

(1) Operatori ključnih usluga primjenjuju mjere za sprečavanje i ublažavanje učinaka incidenata razmjerno procjeni rizika kojemu je izložen njihov ključni sustav.

(2) Operatori ključnih usluga dužni su provoditi aktivnosti vezane za izgradnju, nadogradnju i održavanje ključnih sustava uvažavajući rezultate procjene rizika kojemu je izložen njihov ključni sustav.

(1) Operatori ključnih usluga dužni su kontinuirano ažurirati katalog rizika, uzimajući u obzir unutarnje i vanjske prijetnje koje se pojavljuju, novootkrivene ranjivosti, gubitak djelotvornosti postojećih mjera za sprečavanje i ublažavanje učinaka incidenata, promjene rizika uslijed promjene arhitekture informacijskih sustava, sve promjene koje utječu na sigurnost ključnih sustava, kao i rezultate prethodnih procjena rizika.

(2) Operatori ključnih usluga dužni su najmanje jednom godišnje provoditi procjenu rizika kojemu je izložen njihov ključni sustav i donositi odluku o prihvaćanju preostalih rizika.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze da se mjere za sprječavanje i ublažavanje učinaka incidenta primjenjuju razmjerno provedenoj procjeni rizika te da se aktivnosti

	vezane za izgradnju, nadogradnju i održavanje ključnih sustava provode u skladu s rezultatima procjene rizika - Operator nije predočio katalog rizika ili dokaze da se isti redovito održava uzimajući u obzir unutarnje i vanjske prijetnje - Operator nije predočio rezultate procjene rizika provedene u posljednjih 12 mjeseci
Sukladnost	- Operator je predočio dokaze da se mjere za sprječavanje i ublažavanje učinaka incidenta primjenjuju razmjerno provedenoj procjeni rizika te da se aktivnosti vezane za izgradnju, nadogradnju i održavanje ključnih sustava provode u skladu s rezultatima procjene rizika - Operator je predočio katalog rizika i dokaze da se isti redovito održava uzimajući u obzir unutarnje i vanjske prijetnje - Operator je predočio rezultate procjene rizika provedene u posljednjih 12 mjeseci
Napredna sukladnost	- Operator je predočio dokaze koji ukazuju da se sve mjere za sprječavanja i ublažavanje učinka incidenta te aktivnosti vezane za izgradnju, nadogradnju i održavanje ključnih sustava provode u skladu s rezultatima procjene rizika - Operator je predočio katalog rizika i dokumentirani proces redovitog ažuriranja istog uzimajući u obzir unutarnje i vanjske prijetnje te dokaze da je najviša rukovodna struktura uključena u odobravanje kataloga rizika

Mapiranje:

ISO27001: ISO27001:2013

NIST: RA-1 Risk Assessment policy and procedures

PCI DSS: 12.1.2

II.3 Identifikacija opreme, osoba i aktivnosti u okviru kojih se provodi procjena rizika (Članak 12. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su identificirati:

- *opremu od koje se sastoje ključni sustavi*
- *osobe koje imaju pravo pristupa ključnim sustavima i*
- *poslovne aktivnosti koje se obavljaju na ključnim sustavima ili su u potpori ključnih sustava.*

(2) Operatori ključnih usluga dužni su procjenom rizika obuhvatiti sve identificirane elemente iz stavka 1. ovoga članka.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokumentaciju kojom je identificirana oprema od koje se sastoje ključni sustavi, osobe koje imaju pravo pristupa ključnim sustavima i poslovne aktivnosti koje se obavljaju na ključnim sustavima ili su u potpori ključnih sustava - Operator nije predočio izvješće o procjeni rizika koje je obuhvatilo sve identificirane elemente
Sukladnost	- Operator je predočio dokumentaciju kojom je identificirana oprema od koje se sastoje ključni sustavi, osobe koje imaju pravo pristupa ključnim sustavima i poslovne aktivnosti koje se obavljaju na ključnim sustavima ili su u potpori ključnih sustava - Redovita izvješća o procjeni rizika obuhvaćaju sve identificirane elemente
Napredna sukladnost	-

Mapiranje:

ISO27001: ISO27001:2013

NIST: RA-1 Risk Assessment policy and procedures

PCI DSS: 12.1.2

II.4 Sprječavanje, otkrivanje i rješavanje incidenata te ublažavanje učinka incidenata (Članak 13. Uredbe)

Zahtjev

(1) Procjena rizika provodi se za identificiranu opremu, osobe i aktivnosti iz članka 12. ove Uredbe.

(2) Procjena rizika provodi se na temelju prihvaćenog kataloga rizika s obavezom procjene rizika najmanje za definirana područja zaštite ključnih sustava u poglavlju III. ove Uredbe.

(3) Procijenjeni rizici obrađuju se izbjegavanjem, ublažavanjem, prijenosom ili prihvaćanjem rizika.

(4) Za procijenjene sigurnosne rizike obrada se provodi izborom različitih sigurnosnih mjera i kontrola iz odgovarajuće međunarodne norme informacijske sigurnosti.

(5) Sigurnosne mjere i kontrole iz odgovarajuće međunarodne norme informacijske sigurnosti moraju omogućavati: odvraćanje, izbjegavanje, prevenciju, detekciju, reakciju i oporavak, djelujući na odgovarajući način na prijetnje i ranjivosti ključnih sustava, odnosno na utjecaje incidenata na ključne sustave.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze da se procjena rizika provodi za identificiranu opremu, osobe i aktivnosti iz Članka 12. Uredbe - Procjena rizika ne podrazumijeva obradu rizika izbjegavanjem, ublažavanjem, prijenosom ili prihvaćanjem rizika
Sukladnost	- Operator je predočio dokaze da se procjena rizika provodi za identificiranu opremu, osobe i aktivnosti iz Članka 12. Uredbe - Izvješća o procjeni rizika podrazumijevaju obradu rizika izbjegavanjem, ublažavanjem, prijenosom ili prihvaćanjem rizika, pri čemu sve značajne odluke o obradi rizika najviše razine odobrava najviša rukovodna razina
Napredna sukladnost	- Operator je predočio dokaze koji ukazuju da proces procjene rizika uključuje identificiranu opremu, osobe i aktivnosti iz Članka 12. Uredbe te da se svi procijenjeni rizici obrađuju jednom od spomenutih metoda - Operator provodi ponovljenu procjenu rizika nakon obrade svakog procijenjenog rizika - Operator provodi ponovljenu procjenu rizika nakon značajnijih promjena unutar ključnog sustava

Mapiranje:

ISO27001: ISO27001:2013

NIST: RA-1 Risk Assessment policy and procedures

PCI DSS: 12.1.2

II.5 Dokumentacija o procjeni rizika (Članak 14. Uredbe)

Zahtjev

Operatori ključnih usluga dužni su dokumentaciju nastalu provedbom procjene rizika kojemu je izložen njihov ključni sustav štititi na način koji osigurava pristup isključivo ovlaštenim osobama.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije dokazao da se cjelokupna dokumentacija nastala provedbom procjene rizika štiti na način koji osigurava pristup isključivo ovlaštenim osobama
Sukladnost	- Operator je predočio dokaze da se cjelokupna dokumentacija nastala provedbom procjene rizika štiti na način koji osigurava pristup isključivo ovlaštenim osobama
Napredna sukladnost	-

Mapiranje:

ISO27001: ISO27001:2013

NIST: RA-1 Risk Assessment policy and procedures

PCI DSS: 12.1.2

Poglavlje III – PODRUČJA ZAŠTITE KLJUČNIH SUSTAVA

III.1 Fizička sigurnost i sigurnost okruženja (Članak 15. Uredbe)

Zahtjev

Operatori ključnih usluga dužni su osigurati provedbu mjera koje se odnose na fizičku sigurnost i sigurnost okruženja ključnih sustava od štete uzrokovane kvarom sustava, ljudskim pogreškama, zlonamjernim djelovanjem ili djelovanjem prirodnih fenomena.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nema formalno usvojenu politiku fizičke sigurnosti i sigurnosti okruženja (ili usporediv interni akt) u kojoj bi se adresirala pitanja implementacije mjera kao što su kontrola okolišnih uvjeta (vatra, voda), kontrola pristupa štićenim prostorima (ključevi, elektronske brave, biometrija) - Operator nije predočio dokaze o dodijeljenim odgovornostima za područje fizičke sigurnosti i sigurnosti okruženja
Sukladnost	- Postoji formalno usvojena politika fizičke sigurnosti i sigurnosti okruženja (ili usporediv interni akt) koja uključuje opis lokacija i prostora koji su u opsegu politike i dodijeljene odgovornosti za područje fizičke zaštite i sigurnosti okruženja - Operator je predočio dokaze da su mjere fizičke sigurnosti i sigurnosti okruženja implementirane u skladu s rezultatima procjene rizika - Uspostavljen je tehnički sustav nadzora fizičke sigurnosti i sigurnosti okruženja koji se redovito prati
Napredna sukladnost	- Postoji dokumentirana i redovito održavana politika fizičke sigurnosti i sigurnosti okruženja (ili usporediv interni akt) koja uključuje opis lokacija i prostora koji su u opsegu politike i dodijeljene odgovornosti za područje fizičke zaštite i sigurnosti okruženja - Postoji dokumentacija o provedenoj evaluaciji mjera fizičke sigurnosti i sigurnosti okruženja koje su implementirane u skladu s rezultatima procjene rizika - Operator koristi najnaprednija tehnička rješenja kontrole pristupa koja se redovito prate, održavaju i unaprjeđuju

Mapiranje:
ISO27001: A.11

NIST: ID.AM-1: Physical devices and systems within the organization are inventoried, PR.AC-2: Physical access to assets is managed and, PR.AT-5: Physical and information security personnel understand roles & responsibilities, PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met, PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

PCI-DSS: Requirement 8 - Identify and authenticate access to system components: 8.6, Requirement 9 - Restrict physical access to cardholder data: all

III.2 Sigurnost opskrbe (Članak 16. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su osigurati dostupnost opreme, materijala, energenata i drugih resursa nužnih za redovno i kontinuirano funkcioniranje i održavanje ključnih sustava.

(2) Opskrbni lanac resursa iz stavka 1. ovoga članka mora uključivati procjenu sigurnosti svih odabranih izvođača i podizvođača, kao i praćenje izvora nabavljenih resursa.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa brige o sigurnosti opskrbe opreme, materijala, energenata i ostalih resursa nužnih za redovno i kontinuirano funkcioniranje i održavanje ključnih sustava - Ne postoje dokazi da je područje sigurnosti opskrbe obuhvaćeno postupkom procjene rizika
Sukladnost	- Operator je predočio dokaze uspostavljenog procesa brige o sigurnosti opskrbe opreme, materijala, energenata i ostalih resursa nužnih za redovno i kontinuirano funkcioniranje i održavanje ključnih sustava - Izvješća o provedenoj procjeni rizika ukazuju da je područje sigurnosti opskrbe obuhvaćeno postupkom procjene rizika
Napredna sukladnost	-

Mapiranje:
ISO27001: ISO/IEC/27001 A.11.2.2

III.3 Upravljanje ugovornim odnosima (Članak 17. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su redovito procjenjivati i na prihvatljivu razinu svesti rizike koji proizlaze iz ugovornih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave.

(2) Operatori ključnih usluga dužni su kontinuirano nadzirati način i kvalitetu pružanja ugovorenih poslova i usluga koje mogu utjecati na ključne sustave.

(3) Operatori ključnih usluga dužni su provesti postupak procjene rizika prije ostvarivanja ugovornog odnosa s pravnim i fizičkim osobama čije aktivnosti mogu utjecati na ključne sustave.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa procjene rizika ugovorenih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave - Ne postoji popis ugovorenih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave - Operator nije predočio dokaze o provedenoj procjeni rizika prije ostvarivanja ugovornih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave
Sukladnost	- Operator je predočio politiku sigurnosti koja uključuje stavke koje obuhvaćaju odnos operatora i ugovorenih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave - Postoje izvješća o procjeni rizika ugovorenih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave - Postoji popis preostalih rizika koji proizlaze iz odnosa s ugovornim stranama
Napredna sukladnost	- Postoji proces praćenja incidenata koji su proizišli iz ugovornih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave - Postoje dokazi nadzora i revizije ugovorenih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave

Mapiranje:

ISO27001: A.15.1 Information security in supplier relationships

NIST: PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

III.4 Upravljanje eksternalizacijom (Članak 18. Uredbe)

Zahtjev

(1) Operatori ključnih usluga koji za upravljanje i/ili održavanje ključnih sustava koriste vanjskog davatelja usluge, dužni su redovito procjenjivati i na prihvatljivu razinu svesti rizike koji se mogu u okviru eksternalizacije usluge pojaviti.

(2) Operatori ključnih usluga odgovorni su da pružatelj usluga iz stavka 1. ovoga članka u potpunosti primjenjuje mjere zaštite ključnih sustava propisane ovom Uredbom.

(3) Operatori ključnih usluga dužni su provesti postupak procjene rizika eksternalizacije usluge prije sklapanja ugovora o pružanju usluge.

(4) Ugovori iz stavka 3. ovoga članka moraju sadržavati klauzulu o obvezi omogućavanja nesmetanog nadzora nadležnog sektorskog tijela.

(5) Ugovori iz stavka 3. ovoga članka moraju sadržavati klauzulu o obvezi pružanja usluge i nakon raskida ugovora u razumnom roku koji omogućuje operatoru ključne usluge sklapanje ugovora s drugim vanjskim davateljem usluge ili organizaciju samostalnog izvršavanja usluge od strane operatora ključne usluge.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa procjene rizika koji se mogu pojaviti u okviru eksternalizacije usluge - Operator nije predočio popis usluga upravljanja ili održavanja ključnih sustava koje su eksternalizirane - Operator nije predočio izvješće o procjeni rizika koje uključuje procjenu rizika eksternalizacije - Operator nije predočio dokaze koji potvrđuju da je prije sklapanja ugovora o pružanju usluge provedena procjena rizika eksternalizacije - Operator nije predočio dokaze da ugovori o eksternalizaciji usluga sadrže: o Obvezu omogućavanja nesmetanog nadzora nadležnog sektorskog tijela o Obvezu pružanja usluge i nakon raskida ugovora u razumnom roku

Sukladnost	- Operator je predočio dokaze uspostavljenog procesa procjene rizika koji se mogu pojaviti u okviru eksternalizacije usluge - Operator je predočio popis usluga upravljanja ili održavanja ključnih sustava koje su eksternalizirane - Operator je predočio dokaze koji potvrđuju da je prije sklapanja ugovora o pružanju usluge provedena procjena rizika eksternalizacije - Operator je predočio dokaze da ugovori o eksternalizaciji usluga sadrže: o Obvezu omogućavanja nesmetanog nadzora nadležnog sektorskog tijela o Obvezu pružanja usluge i nakon raskida ugovora u razumnom roku
Napredna sukladnost	- Postoji proces praćenja incidenata koji su proizišli iz usluga koje su eksternalizirane - Postoje dokazi nadzora i revizije usluga koje su eksternalizirane

Mapiranje:

ISO27001: A.15.1 Information security in supplier relationships

NIST: PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

III.5 Kontrola pristupa prostorima (Članak 19. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera kojima se osigurava ovlašten i ograničen fizički i logički pristup prostorima u kojima se nalaze ključni sustavi, utemeljen na poslovnim i/ili sigurnosnim zahtjevima.

(2) Operatori ključnih usluga dužni su utvrditi i trajno ažurirati postupke kontrole pristupa prostorima iz stavka 1. ovoga članka, kojima moraju minimalno obuhvatiti:

- *definiranje popisa osoba s pravom pristupa*
- *postupke ulaska osoba bez trajnog prava pristupa*
- *nadzor kontrole pristupa.*

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa kontrole pristupa prostorima u kojima su smješteni ključni sustavi

	- Ne postoji popis osoba koje imaju pravo pristupa prostorima u kojima su smješteni ključni sustavi - Ne postoje dokumentirane procedure i postupci ulaska osoba bez trajnog prava pristupa - Operator nije predočio dokaze kontrole pristupa prostorima u kojima se nalaze ključni sustavi
Sukladnost	- Operator je predočio popis osoba koje imaju pravo pristupa prostorima u kojima su smješteni ključni sustavi - Operator je predočio dokumentirane procedure i postupke ulaska osoba bez trajnog prava pristupa - Postoje dokumentirana evidencija pristupa prostorima u kojima se nalaze ključni sustavi koja se redovito provjerava - Implementirane su mjere kontrole i nadzora pristupa u smislu korištenja mehanizama zaključavanja prostora i video nadzora
Napredna sukladnost	- Postoji uspostavljen proces interaktivnog nadzora kontrole pristupa prostorima u kojima su smješteni ključni sustavi koji uključuje: o Kontinuirano praćenje aktivnosti osoba koje pristupaju prostorima s ključnim sustavima o Redovitu provjeru prava kontrole pristupa od strane odgovornih osoba

Mapiranje:
ISO27001: A.9.1 Secure areas

III.6 Fizičko i logičko razdvajanje ključnih sustava (Članak 20. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su provesti fizičko i/ili logičko odvajanje ključnih sustava od svih ostalih mrežnih i informacijskih infrastruktura.

(2) Ako fizičko i/ili logičko odvajanje ključnih sustava nije moguće, operatori ključnih usluga dužni su skladu s procjenom rizika:

- *provesti mjere koje umanjuju preostali rizik nastao zbog nemogućnosti potpunog odvajanja*
- *dokumentirati i prihvatiti preostale rizike*
- *dokumentirati sve točke ključnog sustava u kojima odvajanje nije moguće.*

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokumentaciju kojom su jasno definirane granice ključnih sustava i točke „dodira“ s ostalim mrežnim i informacijskim sustavima - Operator nije predočio dokaze o provedenoj procjeni rizika koji proizlaze iz činjenice da ključni sustavi nisu fizički i/ili logički odvojeni od svih ostalih mrežnih i informacijskih infrastruktura
Sukladnost	- Operator je proveo fizičko i/ili logičko odvajanje ključnih sustava od svih ostalih mrežnih i informacijskih infrastruktura - Operator je predočio izvješće o procjeni rizika koji proizlaze iz činjenice da ključni sustavi nisu fizički i/ili logički odvojeni od svih ostalih mrežnih i informacijskih infrastruktura - Operator je proveo mjere za smanjenje rizika koje proizlaze iz činjenice da ključni sustavi nisu fizički i/ili logički odvojeni od svih ostalih mrežnih i informacijskih infrastruktura - Operator je predočio dokumentaciju kojom su jasno definirane točke ključnih sustava u kojima odvajanje od ostalih mrežnih i informacijskih infrastruktura nije moguće
Napredna sukladnost	- Operator je proveo i dokazao fizičko i/ili logičko razdvajanje ključnih sustava od ostalih mrežnih i informacijskih infrastruktura tako da ne postoji rizik da kompromitacija ostalih mrežnih i informacijskih infrastruktura utječe na kompromitaciju ključnih sustava

III.7 Kontrola pristupa ključnom sustavu (Članak 21. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera kojima se osigurava ovlašten i ograničen fizički i logički pristup ključnim sustavima, utemeljen na poslovnim i/ili sigurnosnim zahtjevima.

(2) Operatori ključnih usluga dužni su utvrditi i trajno ažurirati postupke kontrole pristupa ključnim sustavima, kojima moraju minimalno obuhvatiti:

- *postupke i sustave kontrole pristupa koji uključuju korištenje jedinstvenih identifikatora osoba i osiguravaju postupke autentifikacije*
- *mehanizme kontrole pristupa ključnim sustavima, koji moraju osigurati da istome pristupaju isključivo korisnici koji na to imaju pravo, a u skladu s poslovnim i/ili sigurnosnim zahtjevima*

- *sustav upravljanja korisničkim pravima pristupa, koji mora uključivati identifikacije, autentifikacije, autorizacije, evidentiranja, kao i stalni nadzor korisničkih prava pristupa*
- *sustav kontinuiranog praćenja pristupa ključnim sustavima koji minimalno mora omogućiti odobravanje i nadzor prava pristupa, praćenje i izvješćivanje u slučaju pokušaja neovlaštenog pristupa*
- *administratorski pristup ključnim sustavima koji se provodi u skladu s pravilima koja jamče korištenje sklopovske i programske opreme i mrežnog okruženja namijenjenog isključivo administratorskom pristupu*
- *redovitu procjenu učinkovitosti postupaka i pravila kontrole pristupa i po potrebi njihovo unaprjeđivanje*
- *redovitu reviziju dodijeljenih prava pristupa i njihovo oduzimanje u slučaju prestanka potrebe za istim.*

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa kontrole pristupa ključnim sustavima - Operator nije predočio dokumentiranu politiku i procedure kontrole pristupa (ili usporedive dokumente) - Operator nije dokazao korištenje postupaka kontrole pristupa ključnim sustavima iz Stavka 2. ovog zahtjeva
Sukladnost	- Operator je uspostavio proces kontrole pristupa ključnim sustavima - Operator je predočio dokumentiranu politiku kontrole pristupa (ili usporedivi dokument) - Operator je dokazao korištenje postupaka kontrole pristupa ključnim sustavima iz Stavka 2. ovog zahtjeva
Napredna sukladnost	- Operator je predočio dokumentaciju o provedenim testovima mehanizama kontrole pristupa ključnim sustavima - Operator je predočio dokaze redovite provjere i ažuriranja politika i procedura kontrole pristupa

Mapiranje:

ISO27001: A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1, ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1

NIST: PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

III.8 Dnevnik aktivnosti ključnih sustava (Članak 22. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su koristiti sustav za nadzor i bilježenje korisničkih aktivnosti na ključnom sustavu.

(2) Vrste zapisa koje se bilježe moraju minimalno obuhvaćati prijave i odjave korisnika sustava, otvaranje i zatvaranje korisničkih računa, promjene prava korisnika, promjene sigurnosnih prava na sustavu i podatke o funkcioniranju sustava koji pokrivaju odgovarajuće poslužitelje.

(3) Svaki zabilježeni zapis sustava za nadzor i bilježenje korisničkih aktivnosti mora minimalno sadržavati:

- *identitet korisnika sustava*
- *vrstu zapisa*
- *vrijeme zapisa*
- *logičku lokaciju ključnog sustava na koju se zapis odnosi.*

(4) Sustav za nadzor i bilježenje korisničkih aktivnosti mora:

- *omogućavati prikupljanje podataka o korisničkim aktivnostima sa svih dijelova ključnog sustava*
- *biti odvojen od sustava s kojih prikuplja podatke i*
- *uspostavljen na način da se maksimalno umanji mogućnost neovlaštene izmjene zapisa korisničkih aktivnosti.*

(5) Operatori ključnih usluga dužni su osigurati kontinuirano praćenje aktivnosti i provođenje postupka analize zapisa u slučaju incidenta.

(6) Zapisi u sustavu za nadzor i bilježenje korisničkih aktivnosti čuvaju se najmanje posljednjih 6 mjeseci.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa bilježenja korisničkih aktivnosti na ključnim sustavima - Operator nije dokazao korištenje sustava za nadzor i bilježenje korisničkih aktivnosti na ključnim sustavima na način kako je opisano u Stavcima 2, 3 i 4 zahtjeva (ili bilježenjem usporedivih zapisa i korištenjem usporedivih funkcionalnosti) - Operator nije predočio dokaze o provođenju postupaka analize zapisa u slučaju incidenta - Operator nije predočio dokaze da se zapisi u sustavu za nadzor i bilježenje ključnih korisničkih aktivnosti čuvaju najmanje 6 mjeseci
Sukladnost	- Operator je predočio dokaze uspostavljenog procesa bilježenja korisničkih aktivnosti na ključnim sustavima

	- Operator je dokazao korištenje sustava za nadzor i bilježenje korisničkih aktivnosti na ključnim sustavima na način kako je opisano u Stavcima 2, 3 i 4 zahtjeva (ili bilježenjem usporedivih zapisa i korištenjem usporedivih funkcionalnosti) - Operator je predočio dokaze o provođenju postupaka analize zapisa u slučaju incidenta - Operator je predočio dokaze da se zapisi u sustavu za nadzor i bilježenje ključnih korisničkih aktivnosti čuvaju najmanje 6 mjeseci
Napredna sukladnost	- Operator je predočio dokaze korištenja naprednih sustava bilježenja korisničkih aktivnosti na ključnim sustavima koji uvelike nadilaze funkcionalnosti i zahtjeve opisane u Stavcima 2, 3 i 4 zahtjeva

Mapiranje:

ISO27001: A.12.4

NIST: DE.CM: Security continuous monitoring

III.9 Zaštita podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu (Članak 23. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera zaštite podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu u svrhu zaštite povjerljivosti, raspoloživosti i cjelovitosti podataka.

(2) Operatori ključnih usluga dužni su utvrditi osjetljive podatke nad kojima je potrebno primijeniti kriptografske mehanizme zaštite tijekom njihove obrade, pohrane i prenošenja u ključnom sustavu u svrhu zaštite povjerljivosti i cjelovitosti podataka.

(3) Operatori ključnih usluga dužni su mjere iz stavaka 1. i 2. odgovarajuće primjenjivati i na prijenosne medije koji se koriste za obradu, pohranu ili pomoću kojih se prenose podaci u ključnom sustavu.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa zaštite podataka koji se obrađuju, pohranjuju i prenose u ključnim sustavima te na prijenosne medije koji se koriste - Operator nije predočio popis (ili usporediv dokument) osjetljivih podataka nad kojima je potrebno primijeniti

	kriptografske mehanizme koji osiguravaju primjerenu razinu zaštite - Operator nije predočio dokaze i pripadajuću suglasnost odgovorne osobe o nepostojanju podataka koje je potrebno štititi kriptografskim mehanizmima
Sukladnost	- Operator je predočio dokaze uspostavljenog procesa zaštite podataka koji se obrađuju, pohranjuju i prenose u ključnim sustavima te na prijenosne medije koji se koriste - Operator je predočio popis (ili usporediv dokument) osjetljivih podataka nad kojima je potrebno primijeniti kriptografske mehanizme koji osiguravaju primjerenu razinu zaštite - Operator je uspostavio kriptografske mehanizme koji osiguravaju primjerenu razinu zaštite podataka koji se obrađuju, pohranjuje i prenose u ključnim sustavima - Operator je predočio popis tipova prijenosnih medija koji se mogu koristiti za obradu, pohranu i prijenos podataka u ključnim sustavima - Operator je predočio politike ili procedure upravljanja kriptografskim ključevima (ili usporediv dokument) - Operator je predočio dokaze i pripadajuću suglasnost odgovorne osobe o nepostojanju podataka koje je potrebno štititi kriptografskim mehanizmima
Napredna sukladnost	- Operator je predočio dokaze o redovitim provjerama klasifikacije osjetljivih podataka koji se obrađuju, pohranjuju i prenose u ključnim sustavima - Operator je predočio dokaze o upravljanju (primjerenom uništavanju ili pohrani) podacima koji se više ne koriste

Mapiranje:

ISO27001: ISO/IEC 27001:2013 A.8.2.3, ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.12.1.4

III.10 Zaštita od zlonamjernog programskog koda (Članak 24. Uredbe)

Zahtjev

(1) Operator je dužan zaštiti ključni sustav od zlonamjernog programskog koda primjenom odgovarajućih sigurnosnih mjera i kontrola.

(2) Sigurnosne mjere i kontrole iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje zlonamjernog programskog koda unutar ključnog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnog sustava i održavanje kontinuiteta pružanja ključne usluge.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa zaštite od zlonamjernog programskog koda koji uključuje korištenje naprednih rješenja koja osiguravaju prepoznavanje i onemogućavanje zlonamjernog korisničkog koda - Sustav za zaštitu od zlonamjernog programskog koda ne uključuje funkcionalnosti zapisivanja i pohrane informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnih sustava i održavanje kontinuiteta pružanja ključnih usluga
Sukladnost	- Operator je predočio dokaze uspostavljenog procesa zaštite od zlonamjernog programskog koda koji uključuje korištenje naprednih rješenja koja osiguravaju prepoznavanje i onemogućavanje zlonamjernog programskog koda - Sustav za zaštitu od zlonamjernog programskog koda (Sustav) uključuje funkcionalnosti zapisivanja i pohrane informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnih sustava i održavanje kontinuiteta pružanja ključnih usluga - Operator je predočio dokaze o cjelokupnoj dokumentaciji funkcioniranja i procedure rada Sustava
Napredna sukladnost	- Operator je predočio dokaze korištenja naprednih sustava prepoznavanja zlonamjernog ponašanja u svim segmentima ključnih sustava - Operator je predočio rezultate periodičkih testova rada Sustava u smislu simuliranja računalnih napada koje bi Sustav trebao onemogućavati

III.11 Zaštita od narušavanja raspoloživosti ključnog sustava (Članak 25. Uredbe)

Zahtjev

(1) Operator je dužan zaštititi ključni sustav od računalnih napada koji mogu narušiti njegovu raspoloživost primjenom odgovarajućih sigurnosnih mjera i kontrola.

(2) Sigurnosne mjere i kontrole iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje računalnih napada koji mogu narušiti raspoloživost ključnog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnog sustava i održavanje kontinuiteta pružanja ključne usluge.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze uspostavljenog procesa zaštite od računalnih napada koji mogu narušiti njegovu raspoloživost - Sustav za zaštitu od računalnih napada koji mogu narušiti njegovu raspoloživost ne uključuje funkcionalnosti zapisivanja i pohrane informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnih sustava i održavanje kontinuiteta pružanja ključnih usluga
Sukladnost	- Operator je predočio dokaze uspostavljenog procesa zaštite od napada koji mogu narušiti raspoloživost ključnih sustava - Sustav za zaštitu od napada koji mogu narušiti raspoloživost ključnog sustava (Sustav) uključuje funkcionalnosti zapisivanja i pohrane informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnih sustava i održavanje kontinuiteta pružanja ključnih usluga - Operator je predočio dokaze, cjelokupnu dokumentaciju funkcioniranja i procedure rada Sustava - Operator je predočio rezultate periodičkih testova rada Sustava u smislu simuliranja računalnih napada koje bi Sustav trebao onemogućavati
Napredna sukladnost	- Operator je predočio dokaze korištenja naprednih sustava prepoznavanja i onemogućavanja napada koji mogu narušiti raspoloživost ključnih sustava

III.12 Razvoj i održavanje ključnih sustava (Članak 26. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su definirati načine, kriterije i postupke razvoja ključnih sustava, s posebnim naglaskom na važnost razmatranja sigurnosnih aspekata od početne faze projekta, a u skladu s donesenom metodologijom upravljanja projektima.

(2) Operatori ključnih usluga dužni su, u sklopu procesa razvoja ključnih sustava, uspostaviti i dokumentirati proces razvoja i isporuke sustava koji obuhvaća postupke analize i projektiranja, razvoja programske podrške, testiranja i uvođenja u produkcijski plan.

(3) Operatori ključnih usluga dužni su na odgovarajući način razdvojiti razvojnu, testnu i produkcijsku okolinu.

(4) Operatori ključnih usluga dužni su osigurati da sve razvijene programske komponente ključnog sustava, kao i nove sklopovske komponente ključnog sustava, prije uvođenja u produkcijski rad budu na odgovarajući način testirane i da ih odobre odgovorne osobe.

(5) Operatori ključnih usluga dužni su osigurati da se za sve programske komponente ključnog sustava, prije uvođenja u produkcijski rad, provede postupak provjere ranjivosti i penetracijskog testiranja.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) koji definiraju načine, kriterije i postupke razvoja ključnih sustava s posebnim naglaskom na važnost razmatranja sigurnosnih aspekata od početne faze projekta, a u skladu s donesenom metodologijom upravljanja projektima - Operator nije predočio dokumentaciju kojom je obuhvaćen proces razvoja i isporuke programske podrške ključnih sustava - Operator nije dokazao razdvojenost (logičku ili fizičku) razvojne, testne i produkcijske okoline - Operator nije predočio izvješća o testiranju programskih komponenti prije uvođenja u produkcijski rad - Operator nije predočio odobrenja od strane odgovornih osoba prije uvođenja programskih komponenti u produkcijski rad - Operator nije predočio izvješća (ili usporedive dokumente) o provedenim postupcima provjere ranjivosti i penetracijskih testiranja esencijalnih dijelova ključnih sustava prije uvođenja u produkcijski rad

Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) koji definiraju načine, kriterije i postupke razvoja ključnih sustava s posebnim naglaskom na važnost razmatranja sigurnosnih aspekata od početne faze projekta, a u skladu s donesenom metodologijom upravljanja projektima - Operator je predočio dokumentaciju kojom je obuhvaćen proces razvoja i isporuke programske podrške ključnih sustava - Operator je dokazao razdvojenost (logičku ili fizičku) razvojne, testne i produkcijske okoline - Operator je predočio izvješća o testiranju programskih komponenti prije uvođenja u produkcijski rad - Operator je predočio odobrenja od strane odgovornih osoba prije uvođenja programskih komponenti u produkcijski rad - Operator je predočio izvješća (ili usporedive dokumente) o provedenim postupcima provjere ranjivosti i penetracijskih testiranja esencijalnih dijelova ključnih sustava prije uvođenja u produkcijski rad - Operator je predočio metodu prepoznavanja esencijalnih dijelova ključnih sustava za koje je potrebno provesti postupke provjere ranjivosti i penetracijskih testiranja prije uvođenja u produkcijski rad
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa razvoja i održavanja ključnih sustava

Mapiranje:

ISO27001: A.14 System acquisition, development and maintenance

PCI-DSS: SA-3 System development lifecycle

III.13 Upravljanje projektima (Članak 27. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su utvrditi kriterije, načine i postupke upravljanja projektima razvoja i održavanja ključnih sustava iz članka 26. ove Uredbe.

(2) Operatori ključnih usluga dužni su za svaki projekt iz stavka 1. ovoga članka odrediti odgovornu osobu i projektni tim.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) kojima se utvrđuju kriteriji, načini i postupci upravljanja projektima razvoja i održavanja ključnih sustava - Operator nije predočio primjere projektne dokumentacije razvoja i održavanja ključnih sustava - Operator nije predočio dokaze o određivanju odgovornih osoba i projektnih timova za projekte razvoja i održavanja ključnih sustava
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive dokumente) kojima se utvrđuju kriteriji, načini i postupci upravljanja projektima razvoja i održavanja ključnih sustava - Operator je predočio primjere projektne dokumentacije razvoja i održavanja ključnih sustava - Operator je predočio dokaze o određivanju odgovornih osoba i projektnih timova za projekte razvoja i održavanja ključnih sustava
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa upravljanja projektima razvoja i održavanja ključnih sustava

Mapiranje:
ISO27001: A.6.1.5

III.14 Upravljanje sklopovskom imovinom (Članak 28. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su upravljati sklopovskom imovinom ključnog sustava tijekom cijelog njegovog životnog ciklusa.

(2) Postupak upravljanja sklopovskom imovinom mora obuhvatiti identifikaciju, evidentiranje, korištenje, održavanje, rashodovanje i kontrolirano uništavanje imovine.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja sklopovskom imovinom koji obuhvaća identifikaciju, evidentiranje, korištenje, održavanje, rashodovanje i kontrolirano uništavanje imovine

	- Operator nije predočio popis sklopovske imovine ključnih sustava koji uključuje osnovne informacije o toj imovini kao što je lokacija, vlasništvo i slično - Operator nije predočio izvještaje (ili usporedive dokumente) o rashodovanju i kontroliranom uništavanju sklopovske imovine ključnih sustava koja se koristi za pohranu podataka
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja sklopovskom imovinom koji obuhvaća identifikaciju, evidentiranje, korištenje, održavanje, rashodovanje i kontrolirano uništavanje imovine - Operator je predočio popis sklopovske imovine ključnih sustava koji uključuje osnovne informacije o toj imovini kao što je lokacija, vlasništvo i slično - Operator je predočio izvještaje (ili usporedive dokumente) o rashodovanju i kontroliranom uništavanju sklopovske imovine ključnih sustava koja se koristi za pohranu podataka
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa upravljanja sklopovskom imovinom ključnih sustava

III.15 Upravljanje promjenama programske imovine (Članak 29. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su upravljati promjenama programske imovine ključnih sustava.

(2) Postupak upravljanja programskom imovinom mora obuhvatiti minimalno:

- *utvrđivanje postojećih inačica programske imovine ključnih sustava*
- *identifikaciju i praćenje svih promjena inačica programske imovine ključnih sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost ključnog sustava*
- *evidentiranje svih promjena inačica programske imovine ključnih sustava onim slijedom kako su nastale zajedno s vremenom nastanka promjene.*

(3) Operatori ključnih usluga dužni su u slučaju svake značajnije promjene programske imovine ključnog sustava, u skladu s procjenom rizika, provesti postupak provjere ranjivosti i penetracijskog testiranja.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja promjenama programske imovine ključnih sustava - Operator nije predočio dokaze postojanja postupaka i dokumentacije upravljanja programskom imovinom koji obuhvaćaju: o Utvrđivanje postojećih inačica programske imovine ključnih sustava o Identifikaciju i praćenje svih promjena inačica programske imovine ključnih sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost ključnih sustava o Evidentiranje svih promjena inačica programske imovine ključnih sustava onim slijedom kako su nastale zajedno s vremenom nastanka promjene - Operator nije predočio izvješća o provedenim postupcima provjere ranjivosti i penetracijskog testiranja ključnih sustava od strane osoba kvalificiranih za provođenje tih poslova
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja promjenama programske imovine ključnih sustava - Operator je predočio dokaze postojanja postupaka i dokumentacije upravljanja programskom imovinom koji obuhvaćaju: o Utvrđivanje postojećih inačica programske imovine ključnih sustava o Identifikaciju i praćenje svih promjena inačica programske imovine ključnih sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost ključnih sustava o Evidentiranje svih promjena inačica programske imovine ključnih sustava onim slijedom kako su nastale zajedno s vremenom nastanka promjene - Operator je predočio izvješća (ili usporedive dokumente) o provedenim postupcima provjere ranjivosti i penetracijskih testiranja esencijalnih dijelova ključnih sustava nakon značajnijih promjena - Operator je predočio metodu identifikacije značajnih promjena ključnih sustava za koje je potrebno provesti postupke provjere ranjivosti i penetracijskih testiranja - Operator je predočio izvješća o provedenim postupcima provjere ranjivosti i penetracijskog testiranja ključnih

	sustava od strane osoba kvalificiranih za provođenje tih poslova
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa upravljanja promjenama programske imovine

Mapiranje:

ISO27001: ISO/IEC 27001:2013 A12.1.1, A.12.5.1, A.13.2.1, A.14.2.2

NIST: PR. IP-3: Configuration change control processes are in place

III.16 Konfiguracija ključnih sustava (Članak 30. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su osigurati:

- *da ključni sustavi sadrže isključivo sklopovsku i programsku opremu koja je nužna za nesmetano funkcioniranje i sigurnost sustava i*
- *da se na ključnom sustavu dopusti samo onaj podatkovni promet koji je nužan.*

(2) Ako uvjet iz stavka 1. ovoga članka nije moguće zadovoljiti, operatori ključnih usluga dužni su u skladu s procjenom rizika:

- *provesti mjere koje umanjuju preostali rizik nastao zbog nemogućnosti ograničenog korištenja sklopovske i programske opreme i nužnog podatkovnog prometa*
- *dokumentirati i prihvatiti preostale rizike.*

(3) Pravila kojima se definiraju ograničenja podatkovnog prometa, kao što su mrežne adrese, protokoli i portovi, potrebno je redovito obnavljati sukladno funkcionalnim i sigurnosnim potrebama ključnog sustava.

(4) Ograničenja podatkovnog prometa moraju se primjenjivati unutar ključnog sustava, između funkcionalnih podsustava, kao i kod vanjskih povezivanja ključnog sustava.

(5) Konfiguraciju ključnih sustava i popis svih elemenata koji čine ključni sustav potrebno je detaljno dokumentirati.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio dokaze da ključni sustavi sadrže isključivo sklopovsku i programsku opremu koja je nužna za nesmetano funkcioniranje i sigurnost sustava i nije predočio dokaze da se na ključnim sustavima dopušta samo onaj promet koji je nužan - Operator nije predočio dokaze o provedbi mjera procjene rizika koji je nastao zbog nemogućnosti ispunjavanja uvjeta iz Stavka 1

	- Operator nije predočio dokaze o redovitom obnavljanju ograničenja podatkovnog prometa sukladno funkcionalnim i sigurnosnim potrebama ključnih sustava te nije dokazao da se ograničenja podatkovnog prometa primjenjuju unutar ključnih sustava, između funkcionalnih podsustava i vanjskih povezivanja ključnih sustava - Operator nije predočio detaljnu dokumentaciju konfiguracije ključnih sustava
Sukladnost	- Operator je predočio dokaze da ključni sustavi sadrže isključivo sklopovsku i programsku opremu koja je nužna za nesmetano funkcioniranje i sigurnost sustava i predočio je dokaze da se na ključnim sustavima dopušta samo onaj promet koji je nužan - Operator je predočio dokaze o provedbi mjera procjene rizika koji je nastao zbog nemogućnosti ispunjavanja uvjeta iz Stavka 1 - Operator je predočio dokaze o redovitom obnavljanju ograničenja podatkovnog prometa sukladno funkcionalnim i sigurnosnim potrebama ključnih sustava te je dokazao da se ograničenja podatkovnog prometa primjenjuju unutar ključnih sustava, između funkcionalnih podsustava i vanjskih povezivanja ključnih sustava - Operator je predočio detaljnu dokumentaciju konfiguracije ključnih sustava
Napredna sukladnost	- Operator je predočio dokaze da se sklopovska i programska oprema redovito mijenja i ažurira - Operator je predočio dokaze da se podatkovni promet redovito analizira te se na temelju donesenih zaključaka propušta isključivo onaj promet koji je nužan

III.17 Preventivne provjere ranjivosti ključnih sustava (Članak 31. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su, u skladu s procjenom rizika, osigurati provođenje redovitih i kontinuiranih provjera ranjivosti ključnih sustava, osobito onih dijelova sustava koji koriste resurse na javno dostupnim mrežnim i informacijskim sustavima.

(2) Operatori ključnih usluga dužni su osigurati da se nedostatci i ranjivosti utvrđeni tijekom postupaka provjere ranjivosti i penetracijskog testiranja obrade kroz postupak upravljanja rizicima.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) kojima je obuhvaćeno područje redovitih i kontinuiranih provjera ranjivosti ključnih sustava - Operator nije predočio izvješća o provedenim postupcima provjere ranjivosti i penetracijskog testiranja ključnih sustava od strane osoba kvalificiranih za provođenje tih poslova - Operator nije predočio izvješća o procjeni rizika u kojima su obrađeni nedostatci i ranjivosti utvrđeni tijekom postupaka provjere ranjivosti i penetracijskog testiranja
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) kojima je obuhvaćeno područje redovitih i kontinuiranih provjera ranjivosti ključnih sustava - Operator je predočio izvješća o provedenim postupcima provjere ranjivosti i penetracijskog testiranja ključnih sustava od strane osoba kvalificiranih za provođenje tih poslova - Operator je predočio izvješća o procjeni rizika u kojima su obrađeni nedostatci i ranjivosti utvrđeni tijekom postupaka provjere ranjivosti i penetracijskog testiranja - Operator je predočio dokaze o provođenju korektivnih mjera koje proizlaze kao rezultat preventivnih provjera ranjivosti ključnih sustava
Napredna sukladnost	-

III.18 Upravljanje kontinuitetom poslovanja (Članak 32. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su identificirati poslovne procese bitne za osiguranje kontinuiteta poslovanja ključne usluge u slučajevima incidenata iz članka 35. ove Uredbe.

(2) Operatori ključnih usluga dužni su donositi operativne planove postupanja u svrhu osiguranja kontinuiteta poslovanja ključnih usluga, koji moraju minimalno uključivati:

- *konkretne tehničke procedure postupanja u svrhu oporavka ključne usluge*
- *jasne korake i odgovornosti za aktivaciju planova oporavka ključne usluge*
- *definirana vremena u kojima ključna usluga mora biti uspostavljena.*

(3) Operatori ključnih usluga dužni su periodično, u skladu s procjenom rizika, provesti i dokumentirati testiranje planova iz stavka 2. ovoga članka.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja kontinuitetom poslovanja - Operator nije predočio dokumentaciju identifikacije poslovnih procesa (ili usporedivu dokumentaciju) bitnih za osiguranje kontinuiteta poslovanja ključnih usluga u slučajevima incidenta - Operator nije predočio izvješće o provedenoj analizi utjecaja na poslovanje kojom su prepoznati i definirani: o Ključni procesi unutar ključne usluge o RTO parametar (*Recovery Time Objective)* o RPO parametar (*Recovery Point Objective)* - Operator nije predočio dokumentirane planove i procedure koje se primjenjuju u slučaju prekida kontinuiteta poslovanja uključujući jasnu i dokumentiranu proceduru za odgovornost aktivacije planova oporavka od strane najviših rukovodnih razina - Operator nije predočio dokaze kojima potvrđuje da implementirane tehničke kontrole omogućavaju oporavak u sukladnosti s parametrima definiranima analizom utjecaja na poslovanje - Operator nije predočio izvješće o procjeni rizika koje obrađuje domenu upravljanja kontinuitetom poslovanja - Operator nije predočio izvješća o provedenim redovnim/periodičnim testovima planova kontinuiteta poslovanja
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja kontinuitetom poslovanja - Operator je predočio dokumentaciju identifikacije poslovnih procesa (ili usporedivu dokumentaciju) bitnih za osiguranje kontinuiteta poslovanja ključnih usluga u slučajevima incidenta - Operator je predočio izvješće o provedenoj analizi utjecaja na poslovanje kojom su prepoznati i definirani: o Ključni procesi unutar ključne usluge o RTO parametar (*Recovery Time Objective)* o RPO parametar (*Recovery Point Objective)* - Operator je predočio dokumentirane planove i procedure koje se primjenjuju u slučaju prekida kontinuiteta poslovanja uključujući jasnu i dokumentiranu proceduru za odgovornost aktivacije planova oporavka od strane najviših rukovodnih razina

	- Operator je predočio dokaze kojima potvrđuje da implementirane tehničke kontrole omogućavaju oporavak u sukladnosti s parametrima definiranima analizom utjecaja na poslovanje - Operator je predočio izvješće o procjeni rizika koje obrađuje domenu upravljanja kontinuitetom poslovanja - Operator je predočio izvješća o provedenim redovnim/periodičnim testovima planova kontinuiteta poslovanja
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa upravljanja kontinuitetom poslovanja koji je redovito testiran i unaprjeđivan

Mapiranje:

ISO27001: ISO/IEC/27001:2013 A.17.1

NIST: PR. IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

III.19 Pričuvna pohrana (Članak 33. Uredbe)

Zahtjev

(1) Operatori ključnih usluga dužni su uspostaviti postupak upravljanja pričuvnom pohranom podataka koji su potrebni za ponovnu uspostava ključnih usluga u zahtijevanom vremenu.

(2) Postupak upravljanja pričuvnom pohranom mora obuhvaćati postupke izrade, pohrane i testiranja pričuvnih kopija podataka te oporavka podataka s pričuvnih kopija.

(3) Pričuvne kopije podataka moraju biti ažurne i pohranjene na jednoj ili više lokacija, od kojih najmanje jedna mora biti, u skladu s procjenom rizika, dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci.

Sigurnosne mjere i razine sukladnosti

Razina sukladnosti	Opis razine sukladnosti
Nesukladnost	- Operator nije predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja pričuvnom pohranom - Operator nije predočio dokumentaciju identifikacije ključnih podataka koje je potrebno pričuvno pohranjivati zbog potrebe ponovne uspostave ključnih usluga - Operator nije predočio dokaze da se pričuvni podaci čuvaju u skladu s parametrima definiranim planovima kontinuiteta poslovanja

	- Operator nije predočio izvješća o provedenim redovnim/periodičnim testovima oporavka pričuvnih podataka i testovima uspostave ključnih usluga korištenjem tih podataka - Operator nije predočio dokaze o pohrani pričuvnih podataka na izdvojenoj lokaciji - Operator nije predočio dokaze o provedenoj procjeni rizika kojom je definirana prihvatljiva udaljenost izdvojene lokacije od primarne lokacije
Sukladnost	- Operator je predočio formalno usvojene politike i procedure (ili usporedive interne akte) upravljanja pričuvnom pohranom - Operator je predočio dokumentaciju identifikacije ključnih podataka koje je potrebno pričuvno pohranjivati zbog potrebe ponovne uspostave ključnih usluga - Operator je predočio dokaze da se pričuvni podaci čuvaju u skladu s parametrima definiranim planovima kontinuiteta poslovanja - Operator je predočio izvješća o provedenim redovnim/periodičnim testovima oporavka pričuvnih podataka i testovima uspostave ključnih usluga korištenjem tih podataka - Operator je predočio dokaze o pohrani pričuvnih podataka na izdvojenoj lokaciji - Operator je predočio dokaze o provedenoj procjeni rizika kojom je definirana prihvatljiva udaljenost izdvojene lokacije od primarne lokacije
Napredna sukladnost	- Operator je predočio dokaze naprednog i optimiziranog procesa upravljanja pričuvnom pohranom koji je redovito testiran i unaprjeđivan

Postupak ocjene sukladnosti

Cilj postupka ocjene sukladnosti jest utvrditi provodi li operator mjere za postizanje visoke razine kibernetičke sigurnosti iz dijela drugog Uredbe.

U kontekstu gore predloženog sustava vrednovanja pojedine mjere, a imajući u vidu svrhu postupka ocjene sukladnosti, osobe koje provode postupak neće koristiti razinu „Napredna sukladnost", već isključivo utvrditi je li operator sukladan ili ne sukladan s pojedinom mjerom Uredbe.

Provoditelji postupka ocjenu sukladnosti mogu utvrđivati na jedan od ili više sljedećih načina:

- Pregledom dokumentacije (interni i vanjski dokumenti, izvješća, zapisnici, planovi i ostali relevantni dokumenti);
- Pregledom ključnih sustava (uvid u aplikacije, izvorni kod, konfiguracijska sučelja, konzolna sučelja i ostali relevantni dokumenti i pregledi);
- Razgovorom/intervjuom s osobama zaduženima za ključni sustav (Uprava, CISO, voditelj IT-a, djelatnici IT odjela, interni revizori i ostale relevantne osobe);
- Uvidom u fizičko stanje.

Tijekom postupka ocjene sukladnosti, osobe koje ga provode prikupljat će materijalne dokaze kojima se potvrđuje ili ne potvrđuje sukladnost operatora s Uredbom. Svi prikupljeni dokumenti koji ukazuju na nesukladnost s pojedinom mjerom Uredbe bit će sastavni dio Izvješća o ocjeni sukladnosti.

Po završetku postupka ocjene sukladnosti, a prije izrade konačnog izvješća o ocjeni sukladnosti, osobe koje provode ocjenu sukladnosti trebale bi održati završni sastanak s osobama nadležnima za uspostavu sustava informacijske sigurnosti kod operatora, prezentirati sve nesukladnosti uočene tijekom postupka ocjene sukladnosti te razjasniti sva moguća neslaganja oko statusa zatečenog stanja kod operatora.

Izvješće o ocjeni sukladnosti

Po završetku postupka ocjene sukladnosti, tijelo/institucija koji ga provodi izradit će Izvješće o ocjeni sukladnosti koje će dostaviti nadležnom sektorskom tijelu na daljnje postupanje. Nacrt Izvješća će prije dostave nadležnom sektorskom tijelu biti prezentiran operatoru kako bi se izbjegle moguće pogreške pri ocjeni i razjasnile moguće nejasnoće.

Uz osnovne informacije o vremenu, mjestu i tijelu/instituciji koja provodi i koja je predmet ocjene sukladnosti, Izvješće bi trebalo sadržavati sljedeće:

- Sažeti opis postojećeg zatečenog stanja za svaku od 30 mjera iz Uredbe;
- Prateću dokumentaciju koja ukazuje na nesukladnost;
- Nedvojbenu ocjenu sukladnosti pojedine mjere – sukladan/nije sukladan;
- Za svaku mjeru ocijenjenu kao nesukladnu, popis korektivnih mjera za ostvarenje sukladnosti;
- Izvješće za Upravu – sažetak.