REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

PRIPOROČILA ZA UPRAVLJANJE TVEGANJ DOBAVNIH VERIG

Avgust 2026

Uvodna pojasnila

Ta dokument predstavlja operativni priročnik, ki služi kot pripomoček pri pripravi in vzdrževanju lastne interne dokumentacije za upravljanje tveganj dobavne verige ter za izvajanje ocene tveganj varnosti dobavne verige oziroma posameznih (pomembnih) dobaviteljev subjektov oziroma zavezancev iz Zakona o informacijski varnosti (ZInfV-1).

Priporočila v tem priročniku niso enotna receptura, ki bi jo bilo mogoče neposredno prenesti v vsako okolje. Vsak zavezanec jih uporabi ob ugotavljanju, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige ter upoštevanju svojih specifik: velikosti in organiziranosti, sektorja in narave storitev, izpostavljenosti tveganjem, števila in strukture dobaviteljev ter razpoložljivih virov. Slednje izhaja iz načela sorazmernosti, na katerem temeljita tako Direktiva (EU) 2022/2555 (NIS2) kot ZInfV-1: varnostni ukrepi naj bodo sorazmerni s tveganji, ki jim je zavezanec izpostavljen, ob upoštevanju ranljivosti, ki so specifične za posameznega neposrednega dobavitelja/ponudnika storitev. Manjši subjekt/zavezanec lahko metodologijo smiselno poenostavi (npr. oceno omeji na ključne dobavitelje in uporabi le najbolj relevantne parametre), subjekt/zavezanec s kompleksno ali kritično dobavno verigo pa jo razširi (npr. pogostejše ocene, dodatna merila, strožji pragovi).

Dokument vsebinsko sledi dokumentom ENISA Good Practices for Supply Chain Cybersecurity (2023), Technical Implementation Guidance on Cybersecurity Risk Management Measures (junij 2025) in Threat Landscape 2025 ter upošteva določbe standarda ISO/IEC 27036 (Kibernetska varnost – odnosi z dobavitelji) in standarda ISO/IEC 27001:2022 (Informacijska varnost, kibernetska varnost in varovanje zasebnosti – Sistemi upravljanja informacijske varnosti).

Ta dokument se uporablja kot priporočilo oziroma pripomoček in ni predpis. Upoštevanje priporočil samo po sebi ne pomeni skladnosti z ZInfV-1, prav tako odstopanje od njih samo po sebi ne pomeni kršitve. Pristojni nadzorni organ izpolnjevanje zakonskih obveznosti presoja v vsakem primeru posebej, ob upoštevanju načela sorazmernosti in obstoječih oziroma prepoznanih tveganj ter dejanskih okoliščin oziroma posebnosti posameznega subjekta oziroma zavezanca.

Uporabljeni viri in literatura:

- *Zakon o informacijski varnosti (Uradni list RS, št. 40/25);*
- *Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024, o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022 (Informacijska varnost, kibernetska varnost in varovanje zasebnosti – Sistemi upravljanja informacijske varnosti);*
- *Standard ISO/IEC 27036-1:2021, ISO/IEC 27036-2:2022 in ISO/IEC 27036-3:2023 ter ISO/IEC 27036-4:2016 (Kibernetska varnost – odnosi z dobavitelji);*
- *Standard ISO/IEC 27002:2022 (Informacijska varnost, kibernetska varnost in varovanje zasebnosti – Kontrole informacijske varnosti);*
- *Standard ISO/IEC 27005:2022 (Napotki za obvladovanje tveganj informacijske varnosti);*
- *Standard ISO 22301:2019 (Varnost in odpornost – Sistemi upravljanja neprekinjenega poslovanja);*
- *Tehnična specifikacija CEN/TS 18026:2024;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *Good Practices for Supply Chain Cybersecurity, ENISA, 2023;*
- *Threat Landscape 2025, ENISA, oktober 2025;*
- *Technical Implementation Guidance on Cybersecurity Risk Management Measures, ENISA, junij 2025.*

KAZALO

Izdajatelj in avtor dokumenta: Urad Vlade Republike Slovenije za informacijsko varnost. Vsebino je pripravil Matjaž Mravljak, pri pripravi pa sta sodelovala še Borut Jakopin in Renato Burazer (zunanji sodelavec). Dokument je izdan v elektronski obliki, verzija 1.0, avgust 2026.

1. Uvod

V sodobnem poslovnem okolju, kjer so dobavne verige vse bolj kompleksne in globalizirane, predstavljajo tveganja v dobavni verigi enega izmed ključnih izzivov za organizacije. Obvladovanje tveganj v dobavni verigi vključuje sistematično identifikacijo, oceno, ublažitev in spremljanje potencialnih tveganj, ki lahko vplivajo na kontinuiteto poslovanja, finančno stabilnost, ugled in skladnost z regulativami.

Tveganja lahko izhajajo iz različnih virov, kot so kibernetski napadi, naravne nesreče, geopolitični dejavniki, finančna nestabilnost dobaviteljev ali pomanjkljivosti v varnostnih ukrepih. Po podatkih *ENISA Threat Landscape 2025*[1] **predstavljajo tveganja v dobavni verigi 10,6 % zabeleženih primerov začetnega dostopa**, pri čemer napadalci aktivno izkoriščajo posredne poti prek tretjih ponudnikov in odvisnosti, vključno z zlorabo kibernetskih odvisnosti v odprtih repozitorijih, zlonamernih razširitev brskalnikov in izkoriščanjem slabih varnostnih politik pogodbenih ponudnikov (dobaviteljev). Posebej so izpostavljeni sektorji, kot so telekomunikacije, logistika in proizvodnja, kjer državno podprte skupine (npr. UNC5221, *Salt Typhoon*) ciljajo na dobavne verige za pridobivanje strateških podatkov in zaščitene intelektualne lastnine, kar se ujema z njihovimi globalnimi strateškimi cilji[2].

Proces obvladovanja tveganj v dobavni verigi mora biti usklajen z regulativnim okvirom, ki poudarja pomen varnosti v dobavni verigi. V Sloveniji je to urejeno z Zakonom o informacijski varnosti (ZInfV-1), ki je v naš pravni red prenesel Direktivo (EU) 2022/2555 (NIS2). Materialno podlago za obvladovanje tveganj dobavne verige daje deseta točka drugega odstavka 22. člena ZInfV-1, po kateri morajo bistveni in pomembni subjekti zagotoviti varnost dobavne verige z določitvijo ustreznih minimalnih zahtev, povezanih z informacijsko in kibernetsko varnostjo, za ključne dobavitelje ali ponudnike storitev, pri čemer se zahteve nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev. Posebej je relevanten četrti odstavek 22. člena ZInfV-1, ki določa: "Bistveni in pomembni subjekti morajo pri presoji in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev, ter splošno kakovost proizvodov in praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Ugotavljati morajo, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige, poleg tega lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih Skupina za sodelovanje pripravi v sodelovanju z Evropsko komisijo in agencijo ENISA v skladu s prvim odstavkom 22. člena Direktive 2022/2555/EU."

Navedena določba ZInfV-1 poudarja obveznost bistvenih in pomembnih subjektov za celovito presojo ranljivosti dobaviteljev, vključno s kakovostjo kibernetskih praks in varnih razvojnih postopkov, ter neposredno preverjanje izvajanja varnostnih ukrepov, z upoštevanjem usklajenih ocen ENISA za kritične verige (kadar so te ocene na voljo).

Določbe 22. člena se uporabljajo skupaj z 20. členom ZInfV-1, ki odgovornim osebam nalaga odobritev ukrepov za obvladovanje tveganj in nadzor nad njihovim izvajanjem, ter z 21. členom, ki ureja varnostno dokumentacijo. Izdelki metodologije iz tega priročnika – politika varnosti dobavne verige, register dobaviteljev in ocene tveganj posameznih dobaviteljev – so

[1] https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf.

[2] V istem poročilu je najpogostejši vektor začetnega dostopa *phishing* (60 %), sledi izkoriščanje ranljivosti (21,3 %); poročilo zajema obdobje od 1. julija 2024 do 30. junija 2025.

zato sestavni del varnostne dokumentacije zavezanca, njihov sprejem pa je v pristojnosti odgovorne osebe.[3]

Za subjekte iz sektorjev digitalne infrastrukture in upravljanja storitev IKT – ne glede na to, ali so razvrščeni med bistvene ali pomembne subjekte – ki so: ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnega centra, ponudniki omrežij za dostavo vsebin, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja, se za te subjekte, kadar spadajo v področje uporabe Izvedbene uredbe Komisije (EU) 2024/2690 z dne 17. oktobra 2024, neposredno uporabljajo njene določbe, ki določa tehnične in metodološke zahteve za ukrepe obvladovanja tveganj za varnost omrežij in informacijskih sistemov v skladu z NIS2. V petem poglavju Dodatka (Annex I) se specifično naslavlja varnost v dobavni verigi z zahtevami, kot so:

- **Ocena tveganj**: Identifikacija in ocenjevanje kibernetskih tveganj iz odnosov s tretjimi osebami, vključno z ranljivostmi specifičnimi za določene dobavitelje.
- **Izbira dobaviteljev**: Vzpostavitev kriterijev za izbiro dobaviteljev, katerih kibernetske prakse ustrezajo zahtevanim standardom, vključno s kakovostjo proizvodov in varnimi razvojnimi postopki.
- **Pogodbeni ukrepi/določbe**: Določitev pogojev v pogodbah za zagotavljanje skladnosti dobaviteljev z varnostnimi standardi, vključno z "*flow-down*" zahtevami za poddobavitelje.
- **Spremljanje in preverjanje**: Redno spremljanje skladnosti dobaviteljev, preverjanje izvajanja ukrepov in vzdrževanje evidence dobaviteljev za sledenje tveganjem.
- **Ukrepi za odpornost**: Celovit pristop k obvladovanju tveganj v verigi, ki vključuje redundanco, testiranje in transparentnost.
- **Nabava, razvoj in vzdrževanje**: Poleg 5. poglavja je za izbiro dobaviteljev in za nabavo IKT produktov ter storitev relevantno tudi 6. poglavje Priloge (varnost pri nabavi, razvoju in vzdrževanju omrežnih in informacijskih sistemov).[4]

Navedene določbe Izvedbene uredbe Komisije (EU) dopolnjujejo nacionalni okvir ZInfV-1 in zagotavljajo enotne standarde za posebno kategorijo zavezancev v celotni EU, kar je ključno za čezmejne dobavne verige.[5]

2. Namen

Ta dokument temelji na priloženem MS Excel orodju (preglednici) za izvedbo ocene tveganj ključnega dobavitelja v dobavni verigi in združuje regulatorne zahteve za zagotavljanje

[3] Pri načrtovanju uskladitve je treba upoštevati prehodne roke po ZInfV-1: 19. junij 2026 za zavezance po prejšnjem zakonu in za operaterje po ZEKom-2 ter 19. december 2026 za nove bistvene in pomembne subjekte.

[4] Uredba (EU) 2024/2847 (CRA) – kibernetska odpornost produktov ustvarja obveznosti postopoma: 11. 9. 2026 – začetek obveznosti poročanja o varnostnih ranljivostih, ki jih napadalci že izkoriščajo in o pomembnih incidentih, ki lahko vplivajo na varnost izdelkov z digitalnimi elementi; 11. 12. 2027 – polna uporaba uredbe.

[5] Za bistvene in pomembne subjekte iz sektorjev bančništva in infrastrukture finančnega trga je treba upoštevati, da je na področju obvladovanja tveganj, povezanih s tretjimi ponudniki storitev IKT, v veljavi specialni predpis Uredba (EU) 2022/2554 (DORA), zlasti njeno V. poglavje. Ti subjekti uporabljajo zahteve DORE glede pogodbenih določil, registra informacij o pogodbenih dogovorih, izhodnih strategij in nadzora nad kritičnimi ponudniki storitev IKT. Priporočila iz tega dokumenta zanje predstavljajo dopolnilno metodološko pomoč in ne nadomeščajo zahtev navedene uredbe.

skladnosti. Namenjen je kot praktičen vodnik za izvedbo procesa ocene tveganj ključnih dobaviteljev.

Dokument vključuje interpretacijo ključnih elementov, korake za izvedbo ocene ter obrazložitve posameznih elementov oziroma parametrov. S tem želimo omogočiti organizacijam, da učinkovito ocenijo in obvladajo tveganja, povezana s ključnimi dobavitelji, ter zmanjšajo potencialne vplive na poslovanje oziroma izvajanje storitev, hkrati pa izpolnjujejo obveznosti po ZInfV-1 oziroma Izvedbeni uredbi Komisije (EU).

Proces ocene tveganj je zasnovan na polkvantitativni in kvalitativni analizi, kjer se tveganje izračuna kot zmnožek pomembnosti dobavitelja in ocene stanja pri dobavitelju. To omogoča razvrstitev tveganj v kategorije od nizkega do kritičnega, kar olajša prioritetizacijo ukrepov in zagotavlja skladnost z regulatornim okvirom (ZInfV-1 in Izvedbena uredba Komisije (EU)). Pri ocenjevanju po posameznih parametrih se prva dimenzija razume kot pomembnost (relevantnost) posameznega parametra za konkretno dobavno razmerje, druga pa kot ocena stanja pri dobavitelju. Poleg povprečne vrednosti velja pravilo kritičnega parametra: za vsak posamezen parameter s stopnjo tveganja 16 ali več priporočamo takojšnjo uvedbo ukrepov, ne glede na povprečje celotne ocene.

3. Proces izvedbe ocene tveganj

Proces izvedbe ocene tveganj v dobavni verigi je strukturiran v obliki MS Excel preglednice, ki vsebuje dve glavni komponenti: lestvice za ocenjevanje in tabelo za analizo posameznih parametrov. V nadaljevanju so navedeni koraki za izvedbo procesa, skupaj z interpretacijo in obrazložitvijo elementov. Ocena naj upošteva zahteve iz ZInfV-1 (npr. presoja ranljivosti in preverjanje ukrepov v skladu s četrtim odstavkom 22. člena ZInfV-1) oziroma 5. poglavja dodatka Izvedbene uredbe Komisije (EU) (npr. ocena tveganj, izbira in spremljanje dobaviteljev), kar pomeni vključitev ocen specifičnih ranljivosti pri dobaviteljih, pogodbenih obveznosti in evidence za spremljanje. Poleg tega se priporoča upoštevanje ugotovitev iz dokumenta *ENISA Threat Landscape 2025*, kjer je navedeno opozorilo na povečano izpostavljenost "*secret sprawl*" v repozitorijih (povečanje za 25 % med 2023 in 2024) ter napade, kot je na primer kompromitacija tretjega dobavitelja v verigi pri Nokii za izvedbo kraje izvorne kode. Lahko pričakujemo, da se bodo vektorji napada z razvojem tehnologije in zmogljivosti umetne inteligence spreminjali, zato je ključno redno spremljanje analitičnih poročil in obveščevalnih podatkov ter upoštevanje teh pri ocenah tveganj in izvajanju ukrepov.

Metodologija v tem dokumentu sledi dobrim praksam ENISA (*Good Practices for Supply Chain Cybersecurity, 2023*) in je strukturirana okoli petih področij: strateški korporativni pristop, upravljanje tveganj dobavne verige, upravljanje odnosov z dobavitelji, obravnava ranljivosti ter kakovost produktov in praks dobaviteljev. Parametri v MS Excel preglednici so razvrščeni in interpretirani v tem okviru. Pristop je skladen tudi s standardom ISO/IEC 27036, ki varnost informacij v odnosih z dobavitelji obravnava skozi celoten življenjski cikel odnosa (načrtovanje, izbira, pogodba, upravljanje in prekinitev).

3.1 Priprava na izvedbo ocene tveganj

- **Izberite ključnega dobavitelja in določite tip dobavitelja:** Najprej vzpostavite seznam vseh neposrednih dobaviteljev in ponudnikov storitev ter jih razvrstite glede na kritičnost. Nato določite ključne dobavitelje, pri katerih je zaradi vpliva na storitve, podatke, procese ali varnost potrebna poglobljena ocena (npr. single point of failure ali dobavitelj ključnih produktov/storitev). Uporabite kriterije, kot so vpliv na produkcijo, finančna izpostavljenost, obseg dostopa, substitutabilnost, zgodovina incidentov,

specifične ranljivosti dobavitelja in zmožnost zamenjave z nadomestnim ponudnikom, v skladu z ZInfV-1. Določite tip dobavitelja: proizvajalec, integrator, MSP/MSSP ponudnik, SaaS ponudnik ali ponudnik oblačnih storitev (ENISA poroča o primerih, kot je kompromitacija storitvenega ponudnika Plus Service marca 2025, ki je ohromila sistem za vozovnice v Italiji in vplivala na tisoče potnikov)[6].

- **Zberite potrebne podatke**: Pridobite informacije o dobavitelju prek javno dostopnih podatkov, pred pripravljenih vprašalnikov, izdanih certifikatov, poročil o presojah ali intervjujev. To vključuje dokumentacijo o varnostnih politikah in ukrepih, finančni stabilnosti, preteklosti, kompetencah ključnega kadra, varnih razvojnih postopkih in dokazila o varnostih zahtevah za njihove ključne (pod)dobavitelje v njihovi dobavni verigi.
- **Upoštevajte zunanje vire informacij**: Pred izvedbo ocene preverite rezultate usklajenih ocen tveganja kritičnih dobavnih verig na ravni EU, morebitne omejitve, izključitve ali opozorila pristojnih organov (URSIV, ENISA) glede visoko tveganih dobaviteljev, javno znane incidente pri dobavitelju in razpoložljive obveščevalne podatke o grožnjah.
- **Razumite lestvice**: Pred ocenjevanjem preglejte lestvice iz MS Excel preglednice "Lestvice", ki služijo kot osnova za objektivno ocenjevanje. Prilagodite jih regulativnim zahtevam, npr. višjo pomembnost za parametre, povezane s ranljivostmi dobaviteljev in varnimi razvojnimi postopki (4. odstavek 22. člena ZInfV-1).
- **Koncentracijsko tveganje in *vendor lock-in***: Pri kritičnih dobaviteljih ocenite odvisnost od enega ponudnika, regije, podatkovnega centra, poddobavitelja ali tehnologije ter možnost zamenjave, prenosa podatkov/storitev, nadomestnega vira in izvedbe izhodne strategije. Kjer je relevantno, dokumentirajte tudi čas, strošek in tehnične omejitve izhoda.
- **Dokazljivost ocene**: Pri vsakem pomembnem kriteriju zabeležite vir in kakovost dokaza (npr. samoizjava, dokumentarni dokaz, neodvisna presoja/certifikat, tehnično preverjanje ali revizija). Ocena naj bo sledljiva do konkretnega dokaza, datuma in odgovornega ocenjevalca. Pri opredelitvi sprejemljivih dokazil priporočamo uporabo primerov dokazil iz dokumenta ENISA Technical Implementation Guidance on Cybersecurity Risk Management Measures (ver. 1.0, 26. junij 2025) in pripadajoče preslikovalne tabele (Mapping table, ver. 1.2), ki varnostne zahteve preslikuje na standarda ISO/IEC 27001:2022 in ISO/IEC 27002:2022 ter na tehnično specifikacijo CEN/TS 18026:2024. Raven dokaza sama po sebi ne spreminja ocene, vpliva pa na zanesljivost sklepa in na pogostost ponovne presoje.
- **Veliki mednarodni dobavitelji in standardizirani pogoji poslovanja**: Pri velikih mednarodnih dobaviteljih – na primer pri globalnih ponudnikih oblačnih in programskih storitev ali pri proizvajalcih industrijske, procesne in omrežne opreme – zavezanec praviloma nima pogajalske moči za individualne varnostne zahteve. Pogodbe so sklenjene po vnaprej pripravljenih splošnih pogojih, pogosto prek posrednika (distributerja, partnerja ali sistemskega integratorja), tak dobavitelj pa običajno ne izpolnjuje individualnih vprašalnikov in ne priznava pravice do presoje pri sebi. To ne

[6] **Dodatni kriterij – koncentracijsko tveganje in vendor lock-in**: Pri kritičnih dobaviteljih ocenite odvisnost od enega ponudnika, regije, podatkovnega centra, poddobavitelja ali tehnologije ter možnost zamenjave, prenosa podatkov/storitev, nadomestnega vira in izvedbe izhodne strategije. Kjer je relevantno, dokumentirajte tudi čas, strošek in tehnične omejitve izhoda.

pomeni, da obveznost iz desete točke drugega odstavka in četrtega odstavka 22. člena ZInfV-1 odpade; spremeni se le način njenega izpolnjevanja. Namesto neposredne izmenjave se zavezanec opre na standardizirana in javno dostopna dokazila, pogodbeni vzvod pa uveljavlja tam, kjer ga dejansko ima. Priporočamo naslednji pristop:

- Nadomestna dokazila namesto vprašalnika: Uporabite javno dostopne certifikate in poročila neodvisnih presojevalcev (ISO/IEC 27001 z izrecno navedbo obsega, ISO/IEC 27017 in ISO/IEC 27018, poročila tipa SOC 2 Type II), varnostno dokumentacijo proizvajalca (varnostni bilteni, opis varnostne arhitekture, kosovnica programske opreme, politika usklajenega razkrivanja ranljivosti, objavljeni roki podpore in konec življenjske dobe), objavljene zaveze glede lokacije obdelave podatkov ter tipske pogodbe o obdelavi osebnih podatkov. Pri vsakem parametru zabeležite raven dokaza; pri teh dobaviteljih gre praviloma za neodvisno presojo ali javno dokumentacijo in ne za samoizjavo, kar je z vidika dokazljivosti ugodneje kot izpolnjen vprašalnik.
- Presoja obsega, ne zgolj obstoja dokazila: Pri standardiziranih dokazilih je ključno vprašanje, ali certifikat oziroma poročilo pokriva prav tisto storitev, različico, regijo in okolje, ki jih uporablja zavezanec. Neujemanje obsega certificiranja z naročeno storitvijo je pri velikih ponudnikih pogostejša vrzel kot odsotnost certifikata.
- Model deljene odgovornosti: Pri oblačnih in programskih storitvah dokumentirajte razmejitev odgovornosti med ponudnikom in zavezancem, torej kaj zagotavlja ponudnik in kaj ostaja obveznost zavezanca (konfiguracija, upravljanje identitet in dostopov, varnostne kopije, dnevniki, šifriranje, obvladovanje ranljivosti v lastnem delu). Tveganje, ki ga po tem modelu ni mogoče prenesti na ponudnika, se obravnava z lastnimi ukrepi in se ne sme šteti za pokrito zgolj zato, ker gre za uveljavljenega ponudnika.
- Pogodbeni vzvod prek posrednika: Kadar je pogodba sklenjena prek distributerja, partnerja ali sistemskega integratorja, se varnostne zahteve, roki obveščanja o incidentih in podpora pri izpolnjevanju obveznosti priglasitve po ZInfV-1 dogovorijo s posrednikom, ki je pogodbena stranka zavezanca. Posrednik je tudi naslovnik zahteve za prenos varnostnih zahtev navzgor po verigi (ang. *Flow-Down*) v okviru, ki ga dopušča njegovo razmerje s proizvajalcem. Pri javnem naročanju je smiselno varnostne zahteve umestiti že v razpisno dokumentacijo, ko je pogajalska moč največja.
- Ravnanje, kadar dokazil ni mogoče pridobiti: Če dobavitelj ne zagotovi niti standardiziranih dokazil, tega ne ocenite kot »ni relevantno«. Pomanjkanje dokazljivosti se odrazi v slabši oceni stanja, obvladuje pa se z nadomestnimi ukrepi na strani zavezanca: omejitvijo obsega dostopov in podatkov, ki jih dobavitelj obdeluje, segmentacijo in nadzorom povezav, lastnim spremljanjem in hrambo dnevnikov, načrtom neprekinjenega poslovanja za primer izpada storitve ter redundanco ali pripravljeno izhodno strategijo.
- Koncentracijsko tveganje kot težišče ocene: Pri globalnih ponudnikih je pogosto ključno tveganje koncentracija in ne posamezna kontrola. Ocenite učinek izpada, enostranske spremembe pogojev poslovanja, prenehanja podpore za produkt ali umika s trga, pa tudi čas, strošek in tehnične omejitve zamenjave. Pri kritičnih storitvah upoštevajte rezultate usklajenih ocen tveganja kritičnih dobavnih verig na ravni EU ter morebitna opozorila ali omejitve pristojnih organov glede posameznih ponudnikov.
- Dokumentiranje prizadevanja in sprejem preostalega tveganja: Nezmožnost pridobitve dokazil ali izvedbe presoje se skupaj z izvedenimi poskusi, prejetimi odgovori, nadomestnimi ukrepi in datumom sprejema preostalega tveganja s strani vodstva zabeleži v register dobaviteljev. Dokumentirano prizadevanje in utemeljena odločitev

vodstva sta v nadzornem postopku bistveno drugačno izhodišče kot odsotnost obravnave dobavitelja.
Enak pristop se smiselno uporabi tudi pri dobaviteljih, ki niso mednarodne družbe, imajo pa primerljivo pogajalsko moč ali standardizirane pogoje poslovanja (na primer monopolni ali edini certificirani ponudniki na trgu). Merilo ni velikost dobavitelja, temveč dejanska možnost zavezanca, da vpliva na pogodbene in varnostne pogoje.

Lestvica pomembnosti (1-5):

Ocena	Oznaka	Opis
1	**Manj pomemben dobavitelj**	Manj kritičen vidik, neznaten potencialni vpliv na poslovanje.
2	**Srednje manj pomemben dobavitelj**	Omejen potencialni vpliv, predvsem na podporne/procesne aktivnosti.
3	**Srednje pomemben dobavitelj**	Opazen potencialni vpliv na poslovanje, možne krajše, še obvladljive motnje ključnih procesov.
4	**Zelo pomemben dobavitelj**	Velik potencialni vpliv na ključne procese, občutne motnje ključnih procesov ali izgube.
5	**Ključen dobavitelj**	Kritično za delovanje organizacije, popolna prekinitev ključnih procesov, potencialni daljši izpad je nesprejemljiv, velike izgube.

***Opomba:** Ta lestvica meri, kako pomemben je določen dobavitelj za organizacijo. Višja vrednost pomeni večji potencialni vpliv na poslovanje.

Lestvica ocene stanja pri dobavitelju (1-5):

Ocena	Oznaka	Opis
1	**Odlično urejeno**	Skladno z najboljšimi praksami in standardi (sprejete ustrezne varnostne politike, implementacija varnostnih ukrepov), redno preverjanje (certifikati).
2	**Dobro urejeno**	Večina dobrih praks uvedena (certifikati).
3	**Zadovoljivo**	Osnovni standard izpolnjen, nekaj manjših pomanjkljivosti.
4	**Delno urejeno**	Večje vrzeli, brez dosledne prakse.
5	**Ni urejeno ali zelo slabo urejeno**	Le minimalni ali ad-hoc ukrepi.

***Opomba:** pri tej lestvici – drugače kot pri lestvici pomembnosti – višja vrednost pomeni slabše stanje – na to bodite pozorni tudi pri vnosu ocen v MS Excel orodje.

Ta lestvica ocenjuje, kako dobro je dobavitelj urejen na določenem področju. Nižja vrednost pomeni boljšo pripravljenost in manjše tveganje.

Lestvica razvrstitve tveganj (1-25):

Stopnja	Kategorija	Priporočen odziv
1–5	**Nizko tveganje**	Redno spremljanje.
6–10	**Zmerno tveganje**	Ukrepi po presoji in redno spremljanje.
11–15	**Srednje tveganje**	Načrtovani ukrepi, preverba ob naslednji redni oceni.

16–20	**Visoko tveganje**	Priporočamo takojšnjo uvedbo ukrepov z roki in nosilci, pogodbene dodatke in izredno presojo.
21–25	**Kritično tveganje**	Priporočamo takojšnje ukrepe, seznanitev vodstva in pripravo izhodne strategije, če ukrepi niso pravočasno izvedeni.

***Opomba k razponom:** ker je stopnja tveganja zmnožek dveh celih števil od 1 do 5, so dosegljive le vrednosti 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 20 in 25. Razponi 11–15, 16–20 in 21–25 so zato le delno zasedeni, v kategorijo kritičnega tveganja pa pade izključno vrednost 25. Organizacija lahko razpone uskladi z dosegljivimi vrednostmi (na primer 1–5 nizko, 6–9 zmerno, 10–12 srednje, 15–16 visoko, 20–25 kritično).

Prevladujoče pravilo: ne glede na izbrane razpone priporočamo, da se parameter, pri katerem je pomembnost ocenjena s 5 in ocena stanja s 3 ali več, vedno obravnava najmanj kot visoko tveganje in se eskalira, tudi če je zmnožek nižji od 16. S tem se prepreči, da bi edini ponudnik ključne storitve z osnovnim, a pomanjkljivim stanjem ostal v kategoriji, ki predvideva zgolj preverbo ob naslednji redni oceni.

Sprejem preostalega tveganja: Za vsako pomembno preostalo tveganje je treba določiti odgovorno osebo za sprejem, utemeljitev, veljavnost sprejema, rok ponovnega pregleda in povezavo z organizacijskim okvirom sprejemljive ravni tveganja. Za tveganja nad določenim pragom se določi obvezna eskalacija na pristojno vodstveno raven.

V tem dokumentu se za prioritetizacijo uporablja indikativna ocena izpostavljenosti dobaviteljskemu tveganju kot produkt pomembnosti dobavitelja in ocene stanja pri dobavitelju (Pomembnost × Ocena stanja). Model 5 × 5 je metodološko orodje tega dokumenta in ni z zakonom ali Izvedbeno uredbo (EU) 2024/2690 predpisana univerzalna formula za izračun tveganja. Po izvedbi ukrepov se določi preostalo tveganje in preveri njegova skladnost z določeno sprejemljivo ravnjo tveganja organizacije. Ker je stopnja tveganja zmnožek dveh celih števil od 1 do 5, so možne le vrednosti 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 20 in 25. Za prikaz rezultatov se priporoča barvna matrika 5 × 5 (toplotni prikaz), ki je preglednejša od zgolj številčnih pasov.

3.2 Izvedba ocene tveganj

Uporabite razdelek "Analiza tveganj" iz priloženega MS Excela. Za vsak naveden parameter (od 1 do 20) najprej ocenite pomembnost dobavitelja za vašo organizacijo (pri posameznem parametru to pomeni relevantnost parametra za konkretno dobavno razmerje), nato izvedite oceno stanja pri dobavitelju. Na podlagi obeh ocen izračunajte stopnjo tveganja in dodajte potrebne opombe (npr. dodatne ukrepe, nosilca ukrepov, datum izvedbe, ipd.). V nadaljevanju so posodobljene obrazložitve posameznih parametrov, dopolnjene z ugotovitvami iz dokumenta *ENISA Threat Landscape 2025*:

- **1. Kritičnost storitve dobavitelja in njegova vloga v dobavni verigi**: Ocenite, kako kritična je storitev za vaše poslovanje (npr. vpliv na OT/produkcijo, druge ključne procese). Če je dobavitelj edini vir, dodelite visoko pomembnost (4-5).

  Ocena stanja: Preverite trenutno stanje prek pogodb, upoštevajte rezultate analize vpliva na poslovanje in upoštevajte specifične ranljivosti, značilne za posameznega dobavitelja (ENISA izpostavlja trende, kot je Operacija Digital Eye iz sredine 2024, ki je ciljala na IT ponudnike v južni Evropi za infiltracijo v dobavne verige).

- **2. Vrsta in občutljivost obdelanih podatkov**: Razmislite o osebnih podatkih, poslovnih skrivnostih ali reguliranih podatkih (posebne vrste osebnih podatkov, tajni

podatki). Visoka pomembnost, če gre za občutljive osebne podatke, poslovne skrivnosti ali tajne podatke.

Ocena stanja: temelji na preverbi, ali ima dobavitelj vzpostavljeno klasifikacijo podatkov, pravila ravnanja z zaupnimi podatki, sklenjeno pogodbo o obdelavi podatkov (kjer je to relevantno) ter dokazila o tehničnih ukrepih zaščite (šifriranje, nadzor dostopa, ločevanje podatkov naročnikov).

- **3. Sistem upravljanja varovanja informacij in izdani certifikati** (ISO/IEC 27001, ISO 22301, ISO/IEC 27017, ISO/IEC 27040, ISO/IEC 42001, ipd.): Preverite prisotnost formalnega sistema upravljanja varnosti informacij (SUVI) in sistema upravljanja neprekinjenega poslovanja (SUNP), veljavnost izdanih certifikatov. Visoka pomembnost za skladnost.

  Ocena stanja: temelji na veljavnih relevantnih certifikatih, obsegu njihove veljavnosti in dokazih o dejanskem izvajanju kontrol ter na rezultatih rednih internih in eksternih presoj. Certifikat ISO/IEC 27001 sam po sebi ni dokaz, da je konkretna storitev ali dobavna veriga brez tveganj; preverite tudi obseg certificiranja in relevantnost kontrol za naročeno storitev.

- **4. Varnostne politike in organizacija ter upravljanje informacijske varnosti**: Ocenite vzpostavljene varnostne politike, določitev vlog (CISO, DPO, ipd.). Pomembnost je visoka za organizacije z občutljivimi podatki.

  Ocena stanja: temelji na preverbi obstoječe dokumentacije, njenem izvajanju in ustrezni organizacijski strukturi (npr. matrika *RACI*).

- **5. Kontrole dostopa in upravljanje identitet**: Vključuje implementacijo večfaktorske avtentikacije (*MFA*), princip najmanjših privilegijev in druge pomembne ukrepe za preprečevanje nepooblaščenega dostopa.

  Ocena stanja: temelji na preverjanju implementacije prek izvedenih presoj. Merilo ocenjevanja: MFA za ves oddaljeni in administrativni dostop = ocena 1–2; MFA le delna = 3; brez MFA za administrativni dostop = 4–5.

- **6. Omrežna varnost in segmentacija**: VLAN, DMZ, požarni zidovi, VPN, ipd. Pomembno za zaščito pred kibernetskimi grožnjami.

  Ocena stanja: temelji na analizi arhitekture omrežja dobavitelja in sistema upravljanja komunikacij: preverite segmentacijo okolij (produkcija/razvoj/test), ločeno in nadzorovano pot za oddaljeni dostop (VPN z MFA), obstoj požarnih zidov s periodičnim pregledom pravil ter ločitev omrežja, prek katerega dobavitelj dostopa do vaših sistemov.

- **7. Šifriranje podatkov**: Šifriranje podatkov v mirovanju in med prenosom. Visoka pomembnost za zaščito podatkov.

  Ocena stanja: temelji na preverjanju upoštevanja uporabe ustreznih standardov in protokolov (npr. AES-256, TLS 1.2 ali novejši, priporočeno TLS 1.3).

- **8. Zaščita končnih točk, dnevniki dogodkov, SIEM, IDS/IPS, SOC storitve**: Antivirus, EDR/XDR, centralno zbiranje dnevniških dogodkov in njihovo ohranjanje. Ključno za zaznavanje incidentov in uspešen odziv.

  Ocena stanja: temelji na preverbi uporabljenih orodij, zagotavljanju ohranjanja dnevniških dogodkov in vzpostavitvi SOC storitev. Priporočeno merilo ocenjevanja:

centralno zbiranje dnevnikov s hrambo, določeno na podlagi tveganja in potreb po dokazljivosti, ter stalno (24/7) spremljanje = ocena 1–2; zbiranje brez stalnega spremljanja = 3; brez centralnega zbiranja dnevnikov = 4–5. Navedeni pragovi so priporočila metodologije in ne pomenijo, da ZInfV-1 ali ISO/IEC 27001 univerzalno predpisujeta določeno dolžino hrambe dnevniških zapisov ali stalno (24/7) spremljanje. Ustrezno raven določi zavezanec, v skladu z zavezujočimi predpisi in na podlagi tveganja ter potreb po dokazljivosti.

- **9. Upravljanje ranljivosti in posodabljanje**: Izvajanje varnostnih posodobitev (ang. *Patch Management*), izvajanje varnostnih pregledov in vdornih testov. Pomembno za preprečevanje izkoriščanja ranljivosti. Preglejte urnike in poročila; vključite varne razvojne postopke po ZInfV-1.

  Ocena stanja: temelji na sposobnosti dobavitelja za pravočasno obravnavo ranljivosti, pri čemer se roki določajo glede na kritičnost, izpostavljenost in možnost izkoriščanja. Kot interno priporočilo lahko organizacija uporabi strožje ciljne roke (npr. za aktivno izkoriščane ali internetno izpostavljene kritične ranljivosti). Pokritost sredstev naj bo merjena glede na relevantni obseg storitve. Preverite tudi, ali ima dobavitelj politiko usklajenega razkrivanja ranljivosti (CVD), ali objavlja varnostna obvestila (ang. Security Advisories) in ali za dobavljeno programsko opremo zagotavlja kosovnico programske opreme (SBOM); SBOM naj se zahteva tam, kjer je glede na naravo proizvoda ali storitve relevanten in sorazmeren. Uredba (EU) 2024/2847 (CRA) ima lastno področje uporabe za proizvode z digitalnimi elementi, zato njene zahteve ni primerno predstavljati kot univerzalno zahtevo za vse dobavitelje ali vse storitve.

- **10. Poddobavitelji (tretje strani):** Obvladovanje podizvajalcev - "*flow-down*" varnostne zahteve in preglednost dobavne verige. Visoka pomembnost za celotno verigo, v skladu s 5. poglavjem dodatka Izvedbene uredbe Komisije (EU) 2024/2690, ki zahteva oceno tveganj pri poddobaviteljih, pogodbeno zagotavljanje ukrepov in redno spremljanje.

  Ocena stanja: temelji na preverbi, ali dobavitelj vodi evidenco svojih ključnih poddobaviteljev, ali varnostne zahteve pogodbeno prenaša nanje (klavzule flow-down), ali izvaja ocene tveganj svojih poddobaviteljev ter ali je pripravljen razkriti kritične odvisnosti v svoji dobavni verigi (koncentracija storitev pri istem ponudniku, tveganja četrtih strani).

- **11. Upravljanje tveganj in skladnost**: Formalni procesi, register tveganj, notranje/zunanje presoje je ključnega pomena za proaktivno obvladovanje tveganj. Pogostost ponovne ocene se določi na podlagi tveganja in sprememb; za kritične dobavitelje se priporoča najmanj letni pregled ter dodatni pregled ob pomembnih spremembah, incidentih, novih ranljivostih, spremembi poddobaviteljev ali drugih dogodkih, ki lahko vplivajo na tveganja.

  Ocena stanja: temelji na obstoju formalnega procesa upravljanja tveganj, ažurnega registra tveganj ter dokazilih o izvedenih notranjih in zunanjih presojah v zadnjih 12 mesecih.

- **12. Kontinuiteta poslovanja (NNP/NO)**: Politika in Načrt neprekinjenega poslovanja ter Načrt obnovitve po katastrofi, redundanca, varnostne kopije, testiranja. Pomembno za odpornost in v skladu z zahtevami iz Izvedbene uredbe Komisije (EU) 2024/2690 za pristop k obvladovanju tveganj v dobavni verigi.

Ocena stanja: temelji na obstoju in ažurnosti načrta neprekinjenega poslovanja in načrta obnovitve po katastrofi, dokazilih o testiranjih (vsaj letno), varnostnem kopiranju, opredeljenih ciljih RTO/RPO za storitve, ki jih dobavitelj zagotavlja naročniku, ter preverbi redundance ključnih zmogljivosti.

- **13. Fizična varnost lokacij**: Kontrola vstopa, videonadzor. Visoka pomembnost za fizične grožnje.

  Ocena stanja: Preglejte uvedene varnostne ukrepe: nadzor fizičnega dostopa do prostorov z opremo in podatki (kontrola pristopa, evidenca vstopov), videonadzor, režim za obiskovalce in zunanje izvajalce ter dokazila (poročila presoj, certifikat, ogled lokacije za kritične storitve).

- **14. Lokacija podatkov in pravno okolje**: Država gostovanja, skladnost z GDPR / ZVOP-2 in/ali ZKI-1. Pomembno za skladnost.

  Ocena stanja: Analizirajte prenose podatkov in lokacije podatkov v mirovanju: preverite, kje se podatki obdelujejo in shranjujejo (EU/EGP ali tretje države), pravno podlago morebitnih prenosov v tretje države (npr. standardne pogodbene klavzule), seznam pod-obdelovalcev in jurisdikcijska tveganja države dobavitelja.

- **15. Upravljanje incidentov**: Proces zaznavanja, obravnave in poročanja incidentov ter SLA za obveščanje naročnika. Pomembno za hitro odzivanje; skladno z ZInfV-1 za izmenjavo podatkov v dobavni verigi.

  Ocena stanja: Preverite ali je vzpostavljen sistem za zaznavo in odziv na incidente, ali so določene vloge in odgovornosti za odzivanje na incident ter ali je izdelan načrt odzivanja na incidente. Merilo ocenjevanja: pogodbeno dogovorjen rok obveščanja naročnika, ki je sorazmeren s kritičnostjo storitve in omogoča naročniku izpolnitev njegovih lastnih zakonskih obveznosti = ocena 1–2; rok dogovorjen, vendar manj primeren glede na tveganje = 3; brez pogodbene obveznosti obveščanja = 4–5. Pogodbeni rok obvestila dobavitelja ni nadomestilo za zakonske roke poročanja pristojnemu organu.

- **16. Varstvo osebnih podatkov** (če je relevantno): DPA, DPIA. Visoka pomembnost za skladnost z ZVOP-2/GDPR.

  Ocena stanja: Preverite vloge, odgovornosti in ukrepe: ali je sklenjena pogodba o obdelavi (DPA), ali je imenovana pooblaščena oseba za varstvo podatkov (kjer je obvezno), ali se vodijo evidence dejavnosti obdelave, ali so izvedene ocene učinka (DPIA) za tvegane obdelave ter kakšen je postopek ob kršitvi varstva podatkov (obveščanje naročnika brez odlašanja). Kot dokazilo o sistemskem pristopu je lahko relevanten tudi certifikat po ISO/IEC 27701 (sistem upravljanja informacij o zasebnosti), pri čemer velja enako kot pri ISO/IEC 27001: certifikat ne nadomešča presoje obsega certificiranja in dejanskega izvajanja kontrol.

- **17. Transparentnost, poročanje, evidence**: Redna poročila, evidence varnostnih dogodkov in deljenje informacij z naročnikom. Ključno za zaupanje in skladnost z ZInfV-1 ter za izmenjavo podatkov v dobavni verigi; vzdržujte evidenco dobaviteljev.

  Ocena stanja: Ocenite sposobnost in pripravljenost dobavitelja za deljenje tehničnih podrobnosti incidentov (»*root cause*«, taktike/tehnike, IoC) ter ali pogodba vsebuje

obveznost poročanja v rokih, usklajenih z ZInfV-1 oziroma Izvedbeno uredbo Komisije (EU) 2024/2690.[7]

- **18. Finančna stabilnost in zanesljivost**: Reference dobavitelja, finančna stabilnost in kompetence ključnih zaposlenih (pomembno za dolgoročno partnerstvo).

  Ocena stanja: Analizirajte finančne izkaze (letni promet, zadolženost, izpostavljenost) in reference dobavitelja; ocenite ustreznost kompetenc ključnih zaposlenih, ki so pomembne za zagotavljanje storitev.

- **19. Zgodovina varnostnih incidentov**: Pretekli incidenti in ukrepi. Visoka pomembnost za učenje iz napak.

  Ocena stanja: Preglejte zgodovino varnostnih incidentov in odziv nanje iz vseh razpoložljivih virov (ENISA navaja primere, kot je kompromitacija ponudnika *Berliner Verkehrsbetriebe* maja 2025, ki je vplivala na podatke 180.000 strank, ter *Repsolov* incident).

- **20. Kultura varnosti in ozaveščanje**: Usposabljanja in »*security by design*«. Ključno za človeški faktor; vključite v presojo praks kibernetske higiene dobaviteljev po ZInfV-1 in 8. poglavjem dodatka Izvedbene uredbe Komisije (EU) 2024/2690.

  Ocena stanja: Preverite izvajanje osnovnih usposabljanj in ozaveščanj s področja informacijske in kibernetske varnosti pri dobavitelju, izvajanje testiranj (npr. phishing testi) ter obdobnih usposabljanj in ozaveščanj.

Po ocenjevanju izračunajte stopnjo tveganja za vsak parameter in povprečno vrednost za celotno oceno. Za parametre z visokim tveganjem (nad 15) dokumentirajte ukrepe za skladnost z regulativami, vključno s preverjanjem izvajanja varnostih ukrepov pri dobaviteljih. Povprečna vrednost je zgolj orientacijski kazalnik in ne sme zakriti posameznih kritičnih odklonov; zato ob povprečju vedno prikažite tudi število parametrov po posameznih kategorijah tveganja. Za vsak parameter s stopnjo tveganja 16 ali več priporočamo takojšnjo uvedbo ukrepov ne glede na povprečje, o vsakem parametru s stopnjo 21 ali več pa priporočamo, da se nemudoma seznani vodstvo.

3.3 Analiza rezultatov ocene tveganj in ukrepi

- **Razvrstite tveganja po lestvici (nizko do kritično)**: Poudarek na tistih ukrepih, ki vplivajo na ranljivosti dobaviteljev (ZInfV-1) ali dobavno verigo (Izvedbena uredba Komisije (EU) 2024/2690). Upoštevajte ENISA ugotovitve o konvergenci groženj, kjer se mešajo kibernetski kriminal, državno sponzorirane kibernetske operacije in »hacktivizem«.

- **Prioritetizirajte ukrepe**: Za visoka/kritična tveganja razvijte akcijski načrt (npr. dodatne presoje, pogodbeni dodatki z varnostnimi zahtevami, redno spremljanje skladnosti, izhodna strategija). ENISA priporoča krepitev zaščite tretjih strani z nadzorom dostopa, spremljanjem in ukrepi za odpornost, vključno z osnovno kibernetsko higieno in upravljanjem ranljivosti. Priporočeni odzivi po kategorijah: zmerno/srednje tveganje – ukrepi po presoji in redno spremljanje; visoko tveganje (16–20) – akcijski načrt z roki in nosilci, pogodbeni dodatki, izredna presoja; kritično tveganje (21–25) – takojšnja

7 Izvedbena uredba Komisije 2024/2690 tudi določa, kdaj se posamezni incident za posameznega zavezanca iz sektorjev digitalne infrastrukture in upravljanja storitev IKT (npr. ponudnik storitev zaupanja, ponudnik DNS, ponudnik upravljanih varnostnih storitev, ipd.) šteje za pomembnega - kar vpliva na zakonsko obveznost poročanja o incidentih.

obravnava pri vodstvu, zmanjšanje odvisnosti od dobavitelja in aktivacija izhodne strategije, če ukrepi v dogovorjenem roku niso izvedeni.

- **Spremljajte:** Redno ponovite oceno (vsaj letno), periodično preverjajte izvajanje ukrepov pri dobaviteljih. Pri tem upoštevajte rezultate usklajenih ocen kritičnih dobavnih verig na ravni EU, ki jih koordinira ENISA (npr. za 5G, oblačne storitve, podmorske kable) ter priporočila URSIV. Oceno ponovite tudi izredno: ob pomembnem incidentu pri dobavitelju, spremembi njegovega lastništva, ključnih podizvajalcev ali pravnega okolja oziroma ob novih opozorilih pristojnih organov. Priporočamo, da rezultate ocene, akcijski načrt in preostala tveganja formalno sprejme vodstvo organizacije (podpisno polje v MS Excel orodju), kar je skladno s smernicami ENISA in pomembno dokazilo v morebitnem nadzornem postopku.

3.4 Prekinitev dobavnega razmerja in izstop (ang. *Exit Strategy*)

Standard ISO/IEC 27036 obravnava varnost informacij skozi celoten življenjski cikel odnosa z dobaviteljem, vključno s fazo prekinitve. Ta faza je z vidika tveganja pogosto najbolj izpostavljena, saj se v njej hkrati odpravljajo dostopi, prenašajo podatki in prekinja podpora. Priporočamo, da organizacija za vsakega ključnega dobavitelja predvidi naslednje korake:

- **Načrtovanje izstopa**: Pred prekinitvijo pripravite načrt izstopa z nosilci, roki, ocenjenimi stroški in tehničnimi omejitvami. Pri kritičnih dobaviteljih naj bo načrt pripravljen že ob sklenitvi pogodbe in redno preverjan.
- **Ravnanje s podatki**: Zagotovite vračilo podatkov v dogovorjeni in uporabni obliki, nato pa dokazljiv izbris pri dobavitelju in njegovih poddobaviteljih (ustrezno potrdilo o izbrisu), ob upoštevanju rokov hrambe po drugih predpisih.
- **Odvzem dostopov in vračilo sredstev**: Odvzemite vse logične in fizične dostope (uporabniški računi, ključi, certifikati, VPN, oddaljeni dostop), zagotovite vračilo opreme ter preverite, da dostopi ne ostanejo aktivni pri poddobaviteljih.
- **Zaključek in učenje**: Posodobite register dobaviteljev, dokumentirajte razlog prekinitve in ugotovitve za prihodnje izbire dobaviteljev ter obvestite notranje deležnike, ki so bili odvisni od storitve.

4. Program upravljanja tveganj dobavne verige

Ocena tveganj v organizacijah z nižjo stopnjo zrelosti pogosto predstavlja občasno aktivnost, običajno enkrat letno. Zrelejše organizacije upravljajo tveganja kot kontinuiran proces, ki skupaj z obstoječimi in načrtovanimi ukrepi usmerja vire ter zagotavlja celovito in usklajeno delovanje vseh deležnikov. Priporočamo, da program upravljanja tveganj dobavne verige postane sestavni del obvladovanja tveganj na ravni organizacije in ne ostane ločena naloga varnostne funkcije.

Program v tem pomenu ni nov dokument, temveč povezava obstoječih elementov v ponovljiv cikel: politike varnosti dobavne verige, registra dobaviteljev, ocen tveganj po metodologiji iz 3. poglavja, akcijskih načrtov in pogodbenih zahtev. Njegov namen je, da se stanje dobavne verige spremlja med posameznimi ocenami in ne zgolj ob njih.

4.1 Elementi programa

Priporočamo, da program opredeli vsaj naslednje:

- **Obseg in nosilce**: kateri dobavitelji so vključeni (praviloma vsi ključni in vsi, ki dostopajo do omrežnih in informacijskih sistemov ali do podatkov), kdo je skrbnik posameznega dobavnega razmerja, kdo je nosilec ocene tveganja in kdo odloča o sprejemu preostalega tveganja. Razdelitev vlog je smiselno zapisati v matriki odgovornosti (npr. RACI).
- **Letni načrt ocen**: seznam dobaviteljev z datumi naslednje redne ocene, določenimi glede na kritičnost dobavitelja in raven razpoložljivega dokaza; pri kritičnih dobaviteljih najmanj letno, pri ostalih lahko v daljšem ciklu.
- **Sprožilce izredne ocene**: pomemben incident pri dobavitelju ali njegovem poddobavitelju, sprememba lastništva ali obvladovanja, zamenjava ključnega poddobavitelja, sprememba lokacije obdelave podatkov, javno razkrita kritična ranljivost v produktu dobavitelja, prenehanje podpore za produkt, opozorilo ali omejitev pristojnega organa ter bistvena sprememba obsega storitve.
- **Vire podatkov za spremljanje med ocenami** (točka 4.2).
- **Načrt preverjanja in testiranja** (točka 4.3).
- **Kazalnike in poročanje vodstvu** (točka 4.4).
- **Povezavo z drugimi procesi**: z nabavo in javnim naročanjem, upravljanjem sprememb, obvladovanjem incidentov in priglasitvijo po ZInfV-1, neprekinjenim poslovanjem ter krovnim registrom tveganj organizacije.
- **Letni pregled programa samega**: ali so bili načrtovani pregledi izvedeni, ali so ukrepi iz akcijskih načrtov zaključeni v rokih in ali so merila ocenjevanja še ustrezna.

4.2 Viri obveščevalnih in analitičnih podatkov

V praksi to pomeni, da se organizacija ne opira zgolj na podatke, ki jih prejme neposredno od dobavitelja, temveč jih dopolni z neodvisnimi dostopnimi viri. Priporočamo, da program določi, katere vire spremljate, kdo jih spremlja in kako pogosto:

- obvestila in opozorila pristojnih organov (URSIV, SI-CERT, GOV-CERT) ter agencije ENISA, vključno z rezultati morebitnih usklajenih ocen tveganja kritičnih dobavnih verig na ravni EU;
- baze ranljivosti, katalogi dejansko izkoriščanih ranljivosti in varnostna obvestila proizvajalcev za produkte, ki jih uporabljate;
- objave dobavitelja o incidentih, spremembah storitve, koncu življenjske dobe produktov in spremembah poddobaviteljev;
- javno dostopni podatki o poslovanju, lastništvu in obvladovanju dobavitelja in
- lastni podatki: dnevniški zapisi o dostopih dobavitelja, ugotovitve presoj, zabeležena odstopanja od dogovorjene ravni storitve in zgodovina incidentov v konkretnem dobavnem razmerju.

Ugotovitve iz teh virov se beležijo v registru dobaviteljev in po potrebi sprožijo izredno oceno.

4.3 Preverjanje in skupno testiranje scenarijev

Preverjanje lastnih zmogljivosti in zmogljivosti dobavitelja ter njegovega obvladovanja lastne dobavne verige, torej prenosa zahtev navzgor po verigi (ang. *Flow-Down*), je smiselno organizirati tako, da sta v načrtovanje in izvedbo vključeni obe strani. Priporočamo:

- **Namizne vaje z dobaviteljem** (ang. *Tabletop Exercise*) za scenarije, kot so izpad storitve, izsiljevalska programska oprema pri dobavitelju, kompromitacija poddobavitelja in odtujitev podatkov naročnika; pri kritičnih dobaviteljih najmanj enkrat letno.
- **Preizkus komunikacijske poti**: ali kontaktni točki in eskalacijska pot delujeta tudi zunaj delovnega časa in ali so pogodbeno dogovorjeni roki obveščanja o incidentu dejansko izvedljivi glede na roke priglasitve po ZInfV-1.
- **Preizkus izhodnega načrta**, vsaj v obliki namizne vaje: ali so predpostavke o času, stroških in tehnični izvedljivosti prenosa storitve realne.
- **Preverjanje predpostavk načrtov neprekinjenega poslovanja in obnovitve**, ki se opirajo na dobavitelja (cilji RTO/RPO, razpoložljivost in obnovljivost varnostnih kopij, dosegljivost podpore).

S takšnimi testi se delno ali v celoti preverjajo tudi predpostavke, na katerih temeljijo odzivni scenariji za kibernetske napade, izhodni načrti, načrti neprekinjenega poslovanja in načrti obnovitve. Zapisniki in ugotovitve vaj so dokazilo o dejanskem izvajanju ukrepov in so praviloma bolj prepričljivi kot pogodbene zaveze in samoizjave.

4.4 Kazalniki in poročanje vodstvu

Ker odgovorne osebe po 20. členu ZInfV-1 odobrijo ukrepe za obvladovanje tveganj in nadzorujejo njihovo izvajanje, potrebujejo redno in časovno primerljivo sliko stanja. Priporočamo majhen nabor kazalnikov, ki se spremljajo skozi čas:

- delež ključnih dobaviteljev z veljavno oceno tveganja, ki ni starejša od predvidenega cikla;
- število parametrov s stopnjo tveganja 16 ali več in gibanje tega števila med obdobji;
- delež ukrepov iz akcijskih načrtov, izvedenih v dogovorjenem roku;
- delež ključnih dobaviteljev s pogodbeno urejenimi varnostnimi zahtevami, roki obveščanja o incidentih in razkritjem poddobaviteljev;
- število preostalih tveganj, ki jih je sprejelo vodstvo, in datumi njihovih naslednjih pregledov in
- število incidentov, ki so izvirali iz dobavne verige, in povprečen čas od zaznave do obvestila naročniku.

Priporočamo najmanj letno poročilo vodstvu, ki zajema stanje kazalnikov, spremembe v profilu tveganja dobavne verige, sprejeta preostala tveganja in predlog prednostnih nalog za naslednje obdobje. Poročilo in odločitve vodstva so del varnostne dokumentacije po 21. členu ZInfV-1.

5. Zaključek

Obvladovanje tveganj v dobavni verigi je ključno za zagotavljanje odpornosti in konkurenčnosti organizacije, kar so tudi zahteve regulatornega okvira: ZInfV-1 (četrti odstavek 22. člena, za presojo ranljivosti in preverjanje ukrepov) in Izvedbena uredba Komisije (EU) 2024/2690 (5. poglavje dodatka, za oceno, izbiro in spremljanje dobaviteljev).

ENISA poudarja, da so tveganja dobavne verige sistemska: posamezen incident pri enem dobavitelju lahko prizadene več sto ali tisoč organizacij. Zato obvladovanje tveganj v dobavni verigi ne more biti enkraten projekt, ampak stalni del korporativnega upravljanja tveganj in sistema upravljanja varovanja informacij.

Z izvedbo sistematične ocene, kot je opisana v tem dokumentu in podprta s preglednico v MS Excel orodju, lahko identificirate šibke točke in jih proaktivno naslovite, hkrati pa zagotovite skladnost z regulatornim okvirjem. V dokumentih *ENISA Threat Landscape for Supply Chain Attacks 2021* in kasnejša poročila ENISA Threat Landscape ter *ENISA Threat Landscape 2025* je poudarjena potreba po celovitem in sistematičnem pristopu, vključno z upravljanjem ranljivosti (npr. hitro popravljanje kritičnih CVE-jev v orodjih, kot so *Microsoft Exchange* ali *Citrix*) in zaščito pred AI-podprtimi napadi na dobavne verige, kot so zastrupljeni modeli in zadnja vrata.

Priporočamo integracijo tega procesa v širši sistem upravljanja tveganj, vključno z rednimi presojami, sodelovanjem z dobavitelji in upoštevanjem ENISA smernic ter priporočil URSIV. S tem boste zmanjšali potencialne izgube, izboljšali skladnost, prispevali k dvigu varnostne kulture in okrepili zaupanje v dobavno verigo.

6. Kratice in okrajšave

V dokumentu in prilogah so uporabljene naslednje kratice in okrajšave:

Kratica	Pomen
AES	napredni šifrirni standard (ang. *Advanced Encryption Standard*)
AI	umetna inteligenca (ang. *Artificial Intelligence*)
CISO	vodja informacijske varnosti (ang. *Chief Information Security Officer*)
CRA	Akt o kibernetski odpornosti – Uredba (EU) 2024/2847 (ang. *Cyber Resilience Act*)
CSF	okvir kibernetske varnosti NIST (ang. *Cybersecurity Framework*)
CVD	usklajeno razkrivanje ranljivosti (ang. *Coordinated Vulnerability Disclosure*)
CVE	javno evidentirana ranljivost (ang. *Common Vulnerabilities and Exposures*)
DMZ	demilitarizirano območje (ang. *Demilitarized Zone*)
DNS	sistem domenskih imen (ang. *Domain Name System*)
DORA	Uredba (EU) 2022/2554 o digitalni operativni odpornosti za finančni sektor
DPA	pogodba o obdelavi osebnih podatkov (ang. *Data Processing Agreement*)
DPIA	ocena učinka v zvezi z varstvom podatkov (ang. *Data Protection Impact Assessment*)

DPO	pooblaščena oseba za varstvo podatkov (ang. *Data Protection Officer*)
EDR	zaznavanje in odzivanje na končnih napravah (ang. *Endpoint Detection and Response*)
EGP	Evropski gospodarski prostor
ENISA	Agencija Evropske unije za kibernetsko varnost
EU	Evropska unija
GDPR	Splošna uredba o varstvu podatkov – Uredba (EU) 2016/679
HR	kadrovsko področje (ang. *Human Resources*)
IDS/IPS	sistem za zaznavanje / preprečevanje vdorov (ang. *Intrusion Detection / Prevention System*)
IKT	informacijsko-komunikacijske tehnologije
IoC	indikator kompromitacije (ang. *Indicator of Compromise*)
ISO/IEC	Mednarodna organizacija za standardizacijo / Mednarodna elektrotehniška komisija
IT	informacijska tehnologija
MFA	večfaktorska avtentikacija (ang. *Multi-Factor Authentication*)
MSP / MSSP	ponudnik upravljanih storitev / ponudnik upravljanih varnostnih storitev (ang. *Managed Service Provider / Managed Security Service Provider*)
NIS2	Direktiva (EU) 2022/2555 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji
NIST	Nacionalni inštitut za standarde in tehnologijo (ZDA)
NNP / NO	načrt neprekinjenega poslovanja / načrt obnovitve po katastrofi
OT	operativna tehnologija (ang. *Operational Technology*)
RACI	matrika odgovornosti (ang. *Responsible, Accountable, Consulted, Informed*)
RS	Republika Slovenija
RTO / RPO	ciljni čas okrevanja / ciljna točka okrevanja (ang. *Recovery Time Objective / Recovery Point Objective*)
SaaS	programska oprema kot storitev (ang. *Software as a Service*)
SBOM	kosovnica programske opreme (ang. *Software Bill of Materials*)
SIEM	sistem za upravljanje varnostnih informacij in dogodkov (ang. *Security Information and Event Management*)
SLA	dogovor o ravni storitev (ang. *Service Level Agreement*)
SOC	varnostno-operativni center (ang. *Security Operations Centre*)
SUNP	sistem upravljanja neprekinjenega poslovanja
SUVI	sistem upravljanja varovanja informacij
TLD	vrhnja domena (ang. *Top-Level Domain*)
TLS	protokol za varen prenos podatkov (ang. *Transport Layer Security*)
URSIV	Urad Vlade Republike Slovenije za informacijsko varnost
VLAN	navidezno lokalno omrežje (ang. *Virtual Local Area Network*)
VPN	navidezno zasebno omrežje (ang. *Virtual Private Network*)
XDR	razširjeno zaznavanje in odzivanje (ang. *Extended Detection and Response*)

ZDIJZ	Zakon o dostopu do informacij javnega značaja (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15, 7/18, 141/22 in 40/25 – ZInfV-1)
ZInfV-1	Zakon o informacijski varnosti (Uradni list RS, št. 40/25)
ZKI-1	Zakon o kritični infrastrukturi (Uradni list RS, št. 102/24)
ZVOP-2	Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22)

Priloge:

- Priloga 1: Vprašalnik za dobavitelja;
- Priloga 2: MS Excel orodje za oceno tveganj dobavitelja, z registrom dobaviteljev (ločen dokument-datoteka);
- Priloga 3: Register dobaviteljev – specifikacija podatkovnih polj;
- Priloga 4: Kontrolni seznam pogodbenih določb.
- Priloga 5: Preslikava parametrov na kontrole ISO/IEC 27002:2022 in regulatorne zahteve.

Priloga 1: Vprašalnik za dobavitelja

Namen: Vprašalnik izpolni dobavitelj oziroma ponudnik storitev. Odgovori in priložena dokazila so podlaga za oceno stanja pri dobavitelju po metodologiji iz tega dokumenta. Pri sklicevanju na Izvedbeno uredbo (EU) 2024/2690 se 5. poglavje uporablja le za subjekte, za katere je ta uredba neposredno uporabljiva; za druge zavezance je vsebina uporabljena kot priporočilo dobre prakse. Četrti odstavek 22. člena ZInfV-1 se uporablja v obsegu, ki je relevanten za konkretnega zavezanca. Podatki se obravnavajo kot podatki zaupne narave.

Navodilo: Pri vsakem vprašanju v stolpec Odgovor vpišite: DA / DELNO / NE / NI RELEVANTNO. V zadnji stolpec vpišite kratko pojasnilo in navedite priložena dokazila (certifikati, politike, poročila presoj, rezultati testiranj). Parameter 1 (kritičnost storitve) oceni naročnik sam in ni predmet vprašalnika.

Pri velikih mednarodnih dobaviteljih, ki individualnih vprašalnikov ne izpolnjujejo, se namesto vprašalnika uporabijo standardizirana in javno dostopna dokazila po postopku iz poglavja 3.1 tega dokumenta; vprašalnik v tem primeru služi kot notranji kontrolni seznam za pregled zbranih dokazil.

Splošni podatki o dobavitelju:

Naziv in matična številka:	
Naslov in država sedeža:	
Vrsta produktov / storitev za naročnika:	
Varnostna kontaktna oseba (ime, e-naslov, telefon):	
Vprašalnik izpolnil (ime, funkcija):	
Datum izpolnitve:	

Vprašanja za dobavitelja:

Št.	Vprašanje	Odgovor*	Pojasnilo in dokazila
A. Upravljanje varnosti in skladnost (parametri 3, 4, 11)			
1	Ali imate vzpostavljen in certificiran sistem upravljanja varovanja informacij (npr. ISO/IEC 27001)? Navedite certifikate, obseg in veljavnost.		
2	Ali izvajate redne notranje in zunanje presoje ter vodstvene preglede? Kdaj je bila zadnja presoja?		
3	Ali imate sprejete varnostne politike in imenovane odgovorne vloge (npr. CISO, DPO)?		
4	Ali imate formalen proces upravljanja tveganj in ažuren register tveganj?		
B. Varovanje podatkov (parametri 2, 7, 14, 16)			
5	Ali imate vzpostavljeno klasifikacijo podatkov in pravila ravnanja z zaupnimi podatki?		
6	Ali podatke naročnika logično ali fizično ločujete od podatkov drugih strank?		
7	Ali so podatki šifrirani med prenosom (TLS 1.2 ali novejši) in v mirovanju (npr. AES-256)?		

Št.	Vprašanje	Odgovor*	Pojasnilo in dokazila
8	V kateri državi se podatki naročnika obdelujejo in shranjujejo? Ali se prenašajo v tretje države in na kateri pravni podlagi?		
9	Ali ste pripravljeni skleniti pogodbo o obdelavi osebnih podatkov (DPA) in navesti seznam pod-obdelovalcev?		
10	Ali vodite evidence dejavnosti obdelave in izvajate ocene učinka (DPIA) za tvegane obdelave?		
C. Tehnični varnostni ukrepi (parametri 5, 6, 8)			
11	Ali uporabljate večfaktorsko avtentikacijo (MFA) za ves oddaljeni in administrativni dostop?		
12	Ali izvajate načelo najmanjših privilegijev in redne preglede dostopnih pravic?		
13	Ali so okolja segmentirana (produkcija/razvoj/test) in je oddaljeni dostop mogoč le prek nadzorovane poti (VPN z MFA)?		
14	Ali centralno zbirate dnevniške zapise? Koliko časa jih hranite?		
15	Ali imate vzpostavljeno stalno (24/7) spremljanje varnostnih dogodkov (SOC, lasten ali pogodbeni)?		
D. Ranljivosti in razvoj (parameter 9)			
16	V kakšnem roku praviloma odpravite kritične ranljivosti na sistemih, ki podpirajo storitev za naročnika?		
17	Ali izvajate redne varnostne preglede in vdorne teste? Kdaj je bil zadnji in kdo ga je izvedel?		
18	Ali imate politiko usklajenega razkrivanja ranljivosti (CVD) in objavljate varnostna obvestila?		
19	Ali za dobavljeno programsko opremo zagotavljate kosovnico programske opreme (SBOM)?		
20	Ali pri razvoju uporabljate varne razvojne postopke (security by design, pregled kode)?		
21	Ali so vaši produkti skladni z zahtevami Uredbe (EU) 2024/2847 (CRA)? Navedite izjavo o skladnosti in informacije o vzdrževanju.		
E. Dobavna veriga – poddobavitelji (parameter 10)			
22	Ali vodite seznam svojih ključnih poddobaviteljev, ki sodelujejo pri storitvi za naročnika? Ali ste ga pripravljeni razkriti?		
23	Ali varnostne zahteve pogodbeno prenašate na poddobavitelje (flow-down) in ocenjujete njihova tveganja?		
24	Ali naročnika vnaprej obvestite o zamenjavi ključnega poddobavitelja?		
F. Neprekinjeno poslovanje in incidenti (parametra 12, 15)			
25	Ali imate načrt neprekinjenega poslovanja in načrt obnovitve po katastrofi? Kdaj sta bila nazadnje testirana?		
26	Kakšne cilje RTO/RPO zagotavljate za storitev, ki jo izvajate za naročnika?		
27	Ali imate načrt odzivanja na incidente z določenimi vlogami in odgovornostmi?		
28	V kakšnem roku obvestite naročnika o incidentu, ki vpliva ali bi lahko vplival na storitev?		
G. Fizična varnost (parameter 13)			
29	Ali je fizični dostop do prostorov z opremo in podatki nadzorovan (kontrola pristopa, evidenca vstopov, videonadzor)?		
30	Ali imate urejen režim za obiskovalce in zunanje izvajalce?		
H. Transparentnost, stabilnost in kultura (parametri 17–20)			

Št.	Vprašanje	Odgovor*	Pojasnilo in dokazila
31	Ali naročniku zagotavljate redna poročila o varnosti in delite tehnične podrobnosti incidentov (vzrok, ukrepi)?		
32	Priložite osnovne finančne podatke (letni promet, boniteta) in ključne reference.		
33	Ali ste v zadnjih 36 mesecih zaznali pomemben varnostni incident? Opišite incident in izvedene ukrepe.		
34	Ali izvajate redna usposabljanja in ozaveščanja zaposlenih s področja informacijske varnosti (vključno s preizkusi, npr. phishing testi)?		
I. Odvisnost, lastništvo in nove tehnologije (parametri 1, 10, 14, 18)			
35	Ali obstajajo za storitev, ki jo izvajate za naročnika, znane odvisnosti od enega ponudnika, regije, podatkovnega centra ali tehnologije? Kakšni so predvideni roki, stroški in tehnične omejitve prenosa storitve na drugega ponudnika ali nazaj na naročnika?		
36	Kdo je lastnik oziroma obvladujoča oseba družbe in v kateri jurisdikciji ima sedež? Ali se zavezujete naročnika vnaprej obvestiti o spremembi lastništva ali obvladovanja?		
37	Ali se podatki naročnika uporabljajo za učenje ali izboljševanje modelov umetne inteligence oziroma ali pri izvajanju storitve uporabljate zunanje ponudnike storitev umetne inteligence? Če da, navedite obseg, pravno podlago in ponudnike.		

** DA / DELNO / NE / NI RELEVANTNO*

Izjava: Izjavljamo, da so navedeni podatki točni in resnični ter da bomo naročnika brez odlašanja obvestili o vseh bistvenih spremembah, ki vplivajo na podane odgovore (vključno s spremembo ključnih poddobaviteljev, lastništva ali lokacije obdelave podatkov).

Odgovorna oseba dobavitelja (ime, funkcija):	
Kraj in datum:	
Podpis in žig:	

Priloga 3: Register dobaviteljev – specifikacija podatkovnih polj

Za subjekte, za katere se uporablja Izvedbena uredba (EU) 2024/2690, je register neposrednih dobaviteljev in ponudnikov storitev z zahtevano vsebino iz točke 5.2 Priloge izrecna regulatorna zahteva. Za druge zavezance po ZInfV-1 se vodenje registra priporoča kot ustrezen način za sistematično upravljanje in dokazovanje obvladovanja tveganj dobavne verige. Vodi se kot ločen zavihek v MS Excel orodju in redno ažurira; spodnja tabela določa obvezna podatkovna polja.

Podatkovno polje	Opis / vir podatka
Zaporedna številka	Enolična oznaka dobavitelja v registru.
Dobavitelj (naziv, matična številka)	Uradni naziv in identifikacija pravne osebe.
Tip dobavitelja	Proizvajalec / integrator / MSP-MSSP / SaaS / oblak (glej opombe k tipologiji).
Produkti in storitve	Seznam IKT produktov oziroma storitev, ki jih dobavitelj zagotavlja (zahteva točke 5.2 Priloge Izvedbene uredbe Komisije (EU) 2024/2690).
Varnostna kontaktna oseba dobavitelja	Ime, e-naslov, telefon; dosegljivost ob incidentih.
Skrbnik pogodbe pri naročniku	Odgovorna oseba za dobavno razmerje na strani organizacije.
Kritičnost dobavitelja (1–5)	Po lestvici pomembnosti iz tega dokumenta.
Datum in rezultat zadnje ocene	Povprečna stopnja tveganja ter število parametrov s stopnjo 16 ali več.
Status ukrepov	Odprti / v izvajanju / zaključeni; nosilec in rok.
Datum naslednje redne ocene	Praviloma 12 mesecev od zadnje ocene.
Datum poteka pogodbe	Za pravočasno obnovo oziroma aktivacijo izhodne strategije.
Sprejem preostalega tveganja	Datum in podpisnik (vodstvo) sprejema preostalega tveganja.
Lokacija obdelave podatkov	Države oziroma regije obdelave in hrambe; pravna podlaga morebitnih prenosov v tretje države.
Ključni poddobavitelji	Znani poddobavitelji, ki sodelujejo pri storitvi; datum zadnjega razkritja.
Raven dokaza	Samoizjava / dokumentarni dokaz / neodvisna presoja ali certifikat / tehnično preverjanje; vpliva na pogostost ponovne ocene.
Način pogodbenega razmerja	Neposredna pogodba ali pogodba prek posrednika (distributer, partner, integrator); naziv posrednika.

Priloga 4: Kontrolni seznam pogodbenih določb

Kontrolni seznam se uporabi ob sklepanju novih pogodb in ob pregledu obstoječih pogodb z dobavitelji, uvrščenimi v register (Priloga 3). Za subjekte, za katere se uporablja Izvedbena uredba (EU) 2024/2690, predstavlja točka 5.1 Priloge regulatorno izhodišče; za druge zavezance je seznam priporočilo za pogodbeno ureditev varnostnih zahtev in dobrih praks ENISA (Good Practices for Supply Chain Cybersecurity, 2023). Za vsako določbo se označi: vključena / delno vključena / ni vključena, z rokom za uskladitev.

Pogodbena določba	Namen / vsebina
Varnostne zahteve in standardi	Minimalne varnostne zahteve naročnika, sklic na standarde (npr. ISO/IEC 27001) in politiko varnosti dobavne verige.
Varnostna kontaktna oseba	Imenovanje kontaktnih oseb za varnost na obeh straneh in njihova dosegljivost.
Obveščanje o incidentih	Rok (priporočeno 24 ur ali manj), način in vsebina obvestila o incidentu, ki vpliva na storitev; podpora naročniku pri izpolnjevanju obveznosti priglasitve po ZInfV-1.
Pravica do presoje (ang. *Right to Audit*)	Pravica naročnika do presoje oziroma revizije izvajanja varnostnih ukrepov pri dobavitelju, vključno z možnostjo nenapovedanih pregledov za kritične storitve.
Zahteve za poddobavitelje (ang. *Flow-Down*)	Prenos varnostnih zahtev na poddobavitelje, seznam ključnih poddobaviteljev in soglasje naročnika k njihovi zamenjavi.
Preverjanje osebja	Varnostno preverjanje in zaupnostne zaveze osebja dobavitelja z dostopom do kritičnih sredstev naročnika.
Upravljanje ranljivosti in posodobitev	Roki za odpravo kritičnih ranljivosti, zagotavljanje varnostnih posodobitev skozi celotno pogodbeno obdobje, CVD politika.
Zagotovilo o odsotnosti nedokumentiranih funkcij	Izjava, da produkt oziroma storitev ne vsebuje skritih funkcij ali stranskih vrat.
SBOM	Za programsko opremo: zagotavljanje kosovnice programske opreme in obveščanje o ranljivostih komponent.
SLA in merila kakovosti	Ravni storitev, merila kakovosti, poročanje in posledice kršitev.
Kontinuiteta in obnovitev	Cilji RTO/RPO, obveznost testiranja načrtov ter pravica naročnika do vpogleda v rezultate testiranj.
Lokacija obdelave in prenosi podatkov	Določitev lokacij obdelave, pogoji za prenos v tretje države, skladnost z GDPR in ZVOP-2 (DPA, kjer je relevantno).
Konec življenjske dobe produkta	Obveščanje o prenehanju podpore, prehodne rešitve in ravnanje s podatki ob koncu življenjske dobe.
Izhodna strategija (*exit* klavzula)	Vračilo oziroma izbris podatkov, prenos storitve na naročnika ali tretjega, prehodna podpora in razumni roki.
Odgovornost in pogodbene kazni	Odgovornost za škodo zaradi kršitev varnostnih obveznosti in pogodbene kazni.
Dokazila o skladnosti	Obveznost predložitve veljavnih certifikatov, poročil o presojah in navedbe obsega certificiranja ter obveščanja o njihovem prenehanju ali spremembi.
Sprememba lastništva ali obvladovanja	Obveznost predhodnega obvestila naročnika o spremembi lastništva, obvladovanja ali sedeža ter pravica naročnika do ponovne ocene tveganja.

Priloga 5: Preslikava parametrov na kontrole in regulatorne zahteve

Namen: preglednica povezuje 20 parametrov ocene iz tega dokumenta s kontrolami standarda ISO/IEC 27002:2022, s poglavji Priloge Izvedbene uredbe Komisije (EU) 2024/2690 in z določbami ZInfV-1. Namenjena je dokazovanju sistematičnosti ocene v nadzornem postopku, pripravi notranje varnostne dokumentacije in usklajevanju z obstoječim sistemom upravljanja varovanja informacij.

Opozorilo: preslikava je informativna in poenostavljena. Sklici na Prilogo Izvedbene uredbe Komisije (EU) 2024/2690 so navedeni na ravni poglavja, ne posameznih podtočk; sklici na ZInfV-1 se nanašajo na najbolj relevantne določbe in ne izključujejo drugih.

Parameter ocene	Kontrole ISO/IEC 27002:2022	Poglavje Priloge Uredbe (EU) 2024/2690	ZInfV-1 oziroma drug predpis
1. Kritičnost storitve in vloga v dobavni verigi	5.19, 5.21, 5.30	5	22/2/10 in 22/4
2. Vrsta in občutljivost obdelanih podatkov	5.12, 5.13, 8.10, 8.12	5, 12	22/2/10; GDPR, ZVOP-2
3. SUVI in izdani certifikati	ISO/IEC 27001:2022; 5.1, 5.35, 5.36	1, 7	21. člen
4. Varnostne politike in organizacija	5.1, 5.2, 5.4	1, 2	20. in 21. člen
5. Kontrole dostopa in upravljanje identitet	5.15–5.18, 8.2, 8.5	11	22/2
6. Omrežna varnost in segmentacija	8.20–8.23	6, 11	22/2
7. Šifriranje podatkov	8.24	9	22/2
8. Zaščita končnih točk, dnevniki, SIEM, SOC	5.7, 8.7, 8.15, 8.16	3, 8	22/2; 25. člen (priglasitev)
9. Upravljanje ranljivosti in posodabljanje	8.8, 8.19, 8.25, 8.30	6, 8	22/4 (varni razvojni postopki)
10. Poddobavitelji (tretje strani)	5.21, 5.22	5	22/2/10 in 22/4
11. Upravljanje tveganj in skladnost	ISO/IEC 27005; 5.35, 5.36	2, 7	22/1 in 22/2
12. Kontinuiteta poslovanja (NNP/NO)	ISO 22301; 5.29, 5.30, 8.13, 8.14	4	22/2
13. Fizična varnost lokacij	7.1–7.4	13	22/2
14. Lokacija podatkov in pravno okolje	5.23, 5.31, 5.34	5, 12	GDPR, ZVOP-2, ZKI-1
15. Upravljanje incidentov	5.24–5.28	3	25. do 27. člen
16. Varstvo osebnih podatkov	ISO/IEC 27701; 5.31, 5.34	5	GDPR (28. člen), ZVOP-2
17. Transparentnost, poročanje, evidence	5.22, 5.28, 6.8	3, 5	22/2/10; 25. člen
18. Finančna stabilnost in zanesljivost	(ni neposredne kontrole; poslovni kriterij)	5	22/4 (splošna kakovost praks)
19. Zgodovina varnostnih incidentov	5.24, 5.27	3, 5	22/4
20. Kultura varnosti in ozaveščanje	6.3, 8.28	8, 10	20. člen; 22/2

Legenda: oznaka 22/2/10 pomeni deseto točko drugega odstavka 22. člena ZInfV-1, oznaka 22/4 pa četrti odstavek istega člena.