SLOVENSKI INŠTITUT ZA REVIZIJO

LJUBLJANA

ZAKLJUČNO DELO

ZA STROKOVNI NAZIV

PREIZKUŠENA NOTRANJA REVIZORKA

Zasnova svetovalnega posla o možnih izboljšavah obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfv-1 in direktive NIS 2

Februar 2025

Maja Hmelak

MAJA HMELAK, vpisana v izobraževalni program pri Slovenskem inštitutu za revizijo za pridobitev strokovnega naziva Preizkušeni notranji revizor, izjavljam, da sem avtorica tega zaključnega dela in v skladu s prvim odstavkom 21. člena Zakona o avtorski in sorodnih pravicah dovoljujem objavo zaključnega dela v elektronski obliki na zaprtem delu spletnih strani Slovenskega inštituta za revizijo.

Povzetek

Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske odpornosti v Uniji (v nadaljevanju: NIS 2) in novi Zakon o informacijski varnosti (v nadaljevanju: ZInfV-1)[1] bosta organizacijam nalagala znatne kadrovske in finančne vložke. Namen zaključnega dela je pripraviti predlog načrta za izvedbo svetovalnega posla, ki izhaja iz zahtev osnutka ZInfV-1 in direktive NIS 2, s poudarkom na skladnosti s predpisi ter širšem zagotavljanju kibernetske odpornosti.

Pri pripravi predloga sem želela preseči zgolj formalno skladnost z osnutkom ZInfV-1 in direktivo NIS 2. Cilj je bil zasnovati svetovalni posel, ki se osredotoča na širšo krepitev kibernetske odpornosti organizacij ter omogoča notranji reviziji, da s sistematičnim pristopom prispeva k izboljšanju upravljanja, obvladovanja tveganj in notranjih kontrol. Zato sem združila ključne zahteve predpisov z izbranim okvirom upravljanja informacijske varnosti in iz njiju izpeljala praktične pripomočke za izvedbo posla, kot so delovni programi in vprašalniki, ki lahko olajšajo oceno skladnosti in kibernetske odpornosti.

Predlagani svetovalni posel sem zasnovala na visoki vsebinski ravni, s poudarkom na strateških in organizacijskih vidikih. Strukturiran pristop vključuje prepoznavanje, ocenjevanje in obvladovanje tveganj ter delovne programe in vprašalnike, prilagojene zahtevam ZInfV-1, NIS 2 in okvira BSI. Pri zasnovi sem poskrbela za prilagodljivost, da bi bil predlog uporaben za različne organizacije, ne glede na njihovo velikost ali kompleksnost informacijskega okolja.

Ključna dodana vrednost, ki sem jo želela doseči, je praktična naravnanost svetovalnega posla. Namen je bil oblikovati generičen pristop, ki omogoča izvedbo učinkovitih notranjerevizijskih svetovalnih poslov ne le pri izpolnjevanju zahtev predpisov, temveč tudi pri vzpostavitvi trajne kibernetske odpornosti, kar lahko dolgoročno prispeva k uspešnosti in varnosti poslovanja organizacij.

[1] Naloga izhaja iz osnutka z označbo EVA 2023-1544-0005 z dne 15. 5. 2024, objavljenega na spletni strani eUprava, [URL: https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290], dostopano 17. 10. 2024.

Kazalo vsebine

1 Uvod

1.1 Kratka predstavitev problemskega področja

Organizacije se soočajo z naraščajočimi kibernetskimi grožnjami. Za izboljšanje splošne kibernetske odpornosti so zakonodajalci na ravni EU in nacionalni ravni sprejeli več predpisov, namenjenih najbolj ranljivim organizacijam. Poleg tega je EU sprejela več direktiv, ki urejajo področje informacijske varnosti v ključnih sektorjih, na primer na področju financ transport in drugi. V pripravi so še dodatni predpisi, ki bodo vplivali na različne vidike kibernetske odpornosti, kot so varnost strojne in programske opreme ter zaščita pred grožnjami, kot so lažne novice. Čeprav ti pravni akti obravnavajo različne vidike informacijske varnosti, so tesno povezani in se medsebojno dopolnjujejo.

Za zagotavljanje skladnosti z novimi predpisi bodo organizacije morale izvesti vrsto ukrepov, vključno s številnimi izboljšavami notranjega nadzornega okolja. Eden izmed predpisov, ki bo zahteval pomembne prilagoditve , je direktiva NIS 2, ki nadomešča leta 2016 sprejeto Direktivo o varnosti omrežij in informacijskih sistemov (v nadaljevanju: Direktiva NIS 1).

Direktiva NIS 1 in iz nje izhajajoči Zakon o informacijski varnosti (v nadaljevanju: ZInfV[2]) sta bila osredotočena na vzpostavitev minimalnih ravni varnosti in obveščanja za izboljšanje kibernetske odpornosti v ključnih sektorjih. NIS 2 širi obseg na več sektorjev, vključuje strožje zahteve glede obvladovanja tveganj in poročanja o incidentih ter uvaja višje kazni za neskladnost.

Države članice morajo sprejeti in objaviti ukrepe, potrebne za uskladitev z direktivo, do 17. oktobra 2024. V obdobju priprave te naloge je že v javni obravnavi osnutek ZInfV-1, ki bo zahteve direktive NIS 2 prenesel v slovensko okolje.

Tematika zaključnega dela obravnava možne izboljšave obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami direktive NIS 2 ter na njej temelječega predloga ZInfV-1. Številne zahteve osnutka ZInfV-1 in Direktive NIS 2 je namreč mogoče razumeti kot zahteve za učinkovitega obvladovanja tveganj na področju kibernetske odpornosti in notranjih kontrol. Organizacije, ki bodo zavezane po direktivi NIS 2 in ZInfV-1 (v nadaljevanju: zavezanci), naj bi a ta način dosegli določeno stopnjo kibernetske odpornosti. Ta je med drugim pomembna za doseganje njihovih strateških ciljev, uspešnost in učinkovitost delovanja informacijskih rešitev ter za varovanje premoženja. Zato naloga obravnava tudi možne izboljšave obvladovanja tveganj in notranjih kontrol v povezavi s širšim področjem kibernetske odpornosti.

1.2 Namen in cilji zaključnega dela

Prenos direktive NIS 2 v slovensko zakonodajo bo za številne organizacije zahteval znatne časovne in finančne vložke. Pri izpolnitvi novih zahtev se organizacije ne bi smele omejiti zgolj na formalno izpolnjevanje. Novi predpisi namreč ponujajo priložnost za bistveno izboljšanje kibernetske odpornosti. V zaključni nalogi želim poudariti ta vidik in se osredotočiti na dva ključna cilja izboljšav v obvladovanju tveganj in notranjih kontrol: doseganje skladnosti z zahtevami osnutka ZInfV-1 in direktive NIS 2 ter širšo krepitev kibernetske odpornosti.

Namen zaključnega dela je predlagati načrt za izvedbo svetovalnega posla, ki temelji na zahtevah osnutka ZInfV-1 in direktive NIS 2 ter bo poleg skladnosti s predpisi obravnaval tudi širše vidike zagotavljanja kibernetske odpornosti. Tako zasnovan svetovalni posel lahko namreč po moji oceni izboljša upravljanje tveganj, dodaja vrednost in doseže boljše delovanje organizacije.

Cilji zaključnega dela so:

- Opredeliti tiste zahteve osnutka ZInfV-1 in direktive NIS 2, ki zahtevajo izboljšanje ali uvedbo novih organizacijskih postopkov ter s tem predstavljajo priložnosti za izboljšave obvladovanja tveganj in notranjih kontrol v organizaciji z vidika notranjega revizorja.

[2] Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23.

- Opredeliti cilje organizacije pri uskladitvi z zahtevami osnutka ZInfV-1 in direktive NIS 2 ter predlagati vsebinski okvir za vzpostavitev robustne kibernetske odpornosti, ki lahko organizaciji služi kot izhodišče.
- Opredeliti cilje in obseg predlaganega svetovalnega posla.
- Izpostaviti možna tveganja pri izvedbi tovrstnega svetovalnega posla in predlagati pristope za njihovo obvladovanje.
- Predlagati možen pristop k začetni oceni tveganj neskladnosti z zahtevami osnutka ZInfV-1 in direktive NIS 2.
- Predlagati možen pristop k začetni oceni tveganj na področju kibernetske odpornosti.
- Predlagati metode za prepoznavanje, proučitev, ovrednotenje in dokumentiranje informacij.
- Predlagati delovne programe za izvedbo svetovalnega posla.

Pri predlaganem svetovalnem poslu je potrebno zagotoviti, da funkcija notranje revizije cilje doseže tako, da ni oslabila nepristranskosti, in da tudi ni ogrožena osebna nepristranskost notranjega revizorja, ki posel izvede.

Zaključno delo je zasnovano tako, da omogoča temeljito spoznavanje zahtev za skladnost z osnutkom ZInfV-1 in direktivo NIS 2 ter predlaga načrt svetovalnega posla kot izhodišče za učinkovito načrtovanje tovrstnega posla .

1.3 Dostop do podatkovnih virov

Predlagani okvir za izvedbo svetovalnega posla je splošen dokument, ki ni zasnovan za konkretno organizacijo, temveč temelji na javno dostopnih virih o obvladovanju tveganj in vzpostavljanju notranjih kontrol na področju kibernetske odpornosti.

1.4 Predpostavke zaključnega dela

Zaključno delo izhaja iz zahtev osnutka ZInfV-1 in direktive NIS 2, ki določata organizacijske aktivnosti, vendar ne ponujata celovitega pristopa za vzpostavitev robustne kibernetske odpornosti. Zaključno delo temelji na predpostavki, da si revidirana organizacija poleg skladnosti z osnutkom ZInfV-1 in direktivo NIS 2 prizadeva tudi za krepitev svoje kibernetske odpornosti.

Predlagani svetovalni posel sem oblikovala tako, da poleg neskladnosti s predpisi izpostavi tudi priložnosti za izboljšanje upravljanja tveganj in vzpostavitve notranjih kontrol pri preprečevanju kibernetskih napadov, odzivanju nanje in drugih vidikih krepitve kibernetske odpornosti.

Pomemben pripomoček, na katerega sem se oprla v tistih delih zaključnega dela, kjer je poleg skladnosti s predpisi treba upoštevati tudi širše vsebinske vidike kibernetske odpornosti, je brezplačni in javno dostopni sistem osnovnega varovanja informacijskih tehnologij[3], ki ga je razvila nemška agencija Zvezni urad za varnost v informacijskih tehnologijah[4] (v nadaljevanju: okvir BSI). Razlog za to izbiro izhaja iz pojasnila k 24. členu osnutka ZInfV-1, ki zavezance usmerja k uporabi standardov, kot so ISO 27001, ISO 27002, NIST Cybersecurity Framework, CIS Controls, ali drugih določil s področja varovanja informacij. (povezava s točko 2.3.6). Ti standardi povzemajo najboljše prakse na področju kibernetske odpornosti, vendar imajo nekaj omejitev:

- standardi družin ISO so plačljivi,
- NIST Cybersecurity Framework izvira iz ZDA in ni v celoti prilagojen malim evropskim podjetjem,
- CIS Controls imajo pomembne pravne omejitve pri uvedbi in uporabi.
- predpisi s področja varovanja informacij ne obravnavajo tveganj z vidika kibernetske odpornosti.

Okvir BSI je po moji oceni ustrezna alternativa naštetim standardom, saj vsebinsko izhaja iz standardov družine ISO 2700x in je z njimi v celoti skladen, hkrati pa ga nadgrajuje z več kot 1.200 stranmi navodil za vzpostavitev celovitega sistema varovanja informacij. Ta navodila pokrivajo tako najvišje ravni etičnih smernic in organizacijskih usmeritev kot tudi podrobnosti, kot so vzpostavitev konkretnih organizacijskih procesov, obvladovanje tveganj v teh procesih ter vzpostavitev učinkovitih notranjih kontrol. Čeprav je njegova uporaba v

[3] Nem. IT-Grundschutz.

[4] Nem. Das Bundesamt für Sicherheit in der Informationstechnik.

Sloveniji razmeroma omejena, je v drugih državah članicah Evropske unije zelo razširjena. Poleg organizacij v Nemčiji ga kot svoj uradni okvir za varovanje informacijskih tehnologij uporabljajo tudi uradi za informacijsko varnost v drugih državah, med drugim v [5] in Estoniji.[6].

Okvir BSI je v osnovi na voljo v nemškem jeziku, vendar se tekoče prevaja in brezplačno objavlja tudi v angleškem jeziku.[7] Podrobneje ga predstavljam v točki 3.2.1 .

Okvir BSI uporabljam v treh točkah zaključnega dela:

- kot predpostavko, da je poslovodstvo revidirane organizacije področje kibernetske odpornosti zasnovala na standardu BSI (povezava s točko 3.2),
- kot izhodišče za začetno oceno tveganj na področju kibernetske odpornosti (povezava s točko 3.8.2) in
- kot vir za oblikovanje predlogov ključnih vprašanj za delovni program posla v delu, ki se nanaša na področje kibernetske odpornosti (povezava s točko 3.9.2).

1.5 Omejitve zaključnega dela

Predlagano zaključno delo ne temelji na konkretni organizaciji in ne vključuje elementov praktičnega primera, kot so predstavitev organizacije, njenega informacijskega okolja, dejanska sodila poslovodstva ali funkcija notranje revizije v organizaciji. Prav tako delo ne obravnava specifik posameznih industrij ali sektorjev, ki bi lahko zahtevali prilagoditve kibernetskih ukrepov, ter ne vključuje ocene stroškov za implementacijo predlaganih izboljšav. Omejeno je tudi na javno dostopne vire in ne zajema morebitnih internih praks, ki jih organizacije že uporabljajo za izboljšanje kibernetske odpornosti.

Osnutek ZInfV-1 in direktiva NIS 2 sta kompleksna predpisa, kar je deloma posledica obsežnega in zahtevnega področja, ki ga obravnavata, deloma pa tudi zaradi njune zasnove s številnimi notranjimi sklici. To otežuje analizo dejanskih zahtev in njihovo oblikovanje v obliki, primerni za pripravo načrta svetovalnega posla. Da bi zaključno delo kar najbolje služilo svojemu namenu, sem v njem povzela in združila ključne zahteve obeh predpisov. Zaradi obsežnosti teh dokumentov je zaključno delo daljše, kot določa šesti odstavek 7. člena Pravilnika o pridobitvi potrdil o strokovnih nazivih preizkušeni davčnik, preizkušeni računovodja, preizkušeni notranji revizor in preizkušeni revizor informacijskih sistemov, vpisu v registre pri Inštitutu ter načinu vodenja seznamov aktivnih imetnikov nazivov.[8]

1.6 Struktura zaključnega dela

Zaključno delo je sestavljeno iz dveh vsebinskih sklopov. V prvem delu povzemam ključne točke osnutka ZInfV-1 in direktive NIS 2, s posebnim poudarkom na določilih, ki predstavljajo temelj za vzpostavitev robustne kibernetske odpornosti. (povezava s točko 2). Drugi vsebinski sklop vključuje predlog načrta svetovalnega posla, ki poleg obveznih vsebin načrtovanja zajema tudi izhodišča za začetno oceno tveganj, dva podrobna delovna programa in priporočila za poročanje (povezava s točko 3).

---

[5] Uporabo BSI standardov povzema spletna stran Urada zveznega kanclerja Avstrije in A-SIT centra za varno informacijsko tehnologijo – Avstrija https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/BSI-IT-Grundschutz-Standards.html.

[6] Uporabo BSI standardov povzema spletna stran Urada za informacijsko varnost Riigi infosüsteemAmet https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its

[7] Tekoči prevodi sistema osnovnega varovanja BSI so na voljo na angleški različici spletne strani BIS: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

[8] Uradni list, št. 93/2011, 107/2011, 5/2018, 45/2019 in 78/2020

2 Pravne podlage svetovalnega posla

V tem poglavju kratko povzemam ključne točke osnutka ZInfV-1 in direktive NIS 2, pri čemer se osredotočam predvsem na določila, ki predstavljajo temelj za vzpostavitev robustne kibernetske odpornosti.

2.1 Kibernetska obramba

Temelj osnutka ZInfV-1 in direktive NIS 2 je koncept kibernetske obrambe. Kibernetska obramba vključuje vse plasti kibernetskega prostora: družbeno, logično-tehnično in fizično.[9]

Pri tem:

- družbena plast zajema uporabnike medsebojno povezanih komunikacij, ki so lahko fizične ali pravne osebe, ter njihove virtualne identitete;
- fizična plast zajema omrežja in naprave, torej vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov;[10]
- logično-tehnična plast zajema digtalne podatke, torej podatke, ki jih družbena in fizična plast shranjujeta, obdelujeta, pridobivata ali prenašata za namene njihovega delovanja, uporabe, varovanja in vzdrževanja.[10]

Opredelitev koncepta kibernetske obrambe je pomembna za načrtovanje politik in postopkov za krepitev kibernetske odpornosti na vseh ravneh informacijske podpore.

2.2 Deležniki

Pri izvajanju osnutka ZInfV-1 in direktive NIS 2 sodeluje več deležnikov, ki imajo pri uresničevanju predpisov različne vloge in naloge. Razumevanje njihovih nalog in odgovornosti je ključno za celovito razumevanje usmeritve Republike Slovenije na področju kibernetske obrambe ter za načrtovanje notranjih postopkov, ki zahtevajo sodelovanje zunanjih deležnikov, na primer pri obvladovanju incidentov, poročanju pristojnim institucijam in ravnanju ob inšpekcijskih pregledih.

2.2.1 Vlada Republike Slovenije

Poleg prenosa direktive NIS 2 v nacionalno zakonodajo ima Vlada Republike Slovenije (v nadaljevanju: vlada) več konkretnih nalog na področju krepitve kibernetske odpornosti. Sprejeti mora nacionalno strategijo za kibernetsko varnost, v kateri bodo opredeljeni strateški cilji, potrebna sredstva za dosego teh ciljev[11] ter konkretne politike na različnih področjih obvladovanja kibernetskih ranljivosti in zagotavljanja kibernetske odpornosti.[12]

Vlada mora sprejeti tudi načrt odzivanja na kibernetske incidente velikih razsežnosti in kibernetske krize.[13] Nacionalna strategija kibernetske odpornosti s konkretnimi področnimi politikami in načrt odzivanja na kibernetske incidente velikih razsežnosti naj bi opredelila celotno področje kibernetske odpornosti v Republiki Sloveniji.

Zavezanci morajo biti seznanjeni z vsemi vladnimi objavami s področja kibernetske odpornosti, saj bodo pri nekaterih vidikih obvladovanja tveganj in notranjih kontrol lahko izhajali iz vladnih dokumentov.

---

9 Prvi odstavek 34. člena osnutka ZInfV-1 in člen 7 direktive NIS 2.

10 Sedemindvajseta točka 5. člena osnutka ZInfV-1 in člen 6 direktive NIS 2.

11 Prvi odstavek 8. člena in tretji odstavek 60. člena ZInfV-1 ter prvi odstavek člena 7 direktive NIS 2.

12 Drugi odstavek 8. člena osnutka ZInfV-1 in drugi odstavek člena 7 direktive NIS 2.

13 Tretji odstavek 11. člena in tretji odstavek 60. člena ZInfV-1 ter četrti odstavek člena 9 direktive NIS 2.

2.2.2 Urad Republike Slovenije za informacijsko varnost

Pristojni nacionalni organ za področje kibernetske odpornosti v Republiki Sloveniji je Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV),[14] ki poleg nalog, predpisanih državam članicam z direktivo NIS 2, opravlja tudi funkcijo mednarodne in nacionalne enotne kontaktne točke.[15] URSIV je pristojen tudi za obvladovanje kibernetskih incidentov velikih razsežnosti in kibernetskih kriz[16] ter naj bi vzpostavil mehanizem za samoregistracijo zavezancev[17],vodil in objavljal seznam zavezancev[18] in izvajal številne druge naloge na nacionalni ter mednarodni ravni.

2.2.3 Skupine za odzivanje na incidente na področju računalniške varnosti - skupine CSIRT

Vsaka država članica določi ali vzpostavi eno ali več skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljevanju: skupin CSIRT).[19]

Skupini CSIRT v Republiki Sloveniji sta SI-CERT, ki deluje kot notranja organizacijska enota pri javnem zavodu Akademska in raziskovalna mreža Slovenije in CSIRT državne uprave, ki deluje kot notranja organizacijska enota SIGOV-CERT pri Uradu za informacijsko varnost.[20] SIGOV-CERT je pristojen za obravnavo incidentov subjektov javne uprave na državni in regionalni ravni, ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave in incidentov povezanih subjektov,[21] SI-CERT pa za obravnavo incidentov, ki jih priglasijo ostali zavezanci (vključno z organi lokalne samouprave, če niso povezani subjekti).[22] Skupini CSIRT imata poleg nalog, povezanih z odzivanjem na incidente, tudi vrsto nalog s področij spremljanja ranljivosti, preventive in sodelovanja na nacionalni ravni in koordinacije med deležniki javnega in zasebnega sektorja.

2.2.4 Drugi državni organi

Organizacijske, logično-tehnične, tehnične in administrativne ukrepe kibernetske obrambe na ravni državnih organov pod koordinacijo URSIV usklajujejo in izvajajo URSIV, skupine CSIRT ter Ministrstvo za obrambo, Ministrstvo za digitalno preobrazbo, Ministrstvo za zunanje zadeve, Ministrstvo za notranje zadeve, Policija, Slovenska obveščevalno-varnostna agencija in drugi nacionalni organi v skladu s svojimi pristojnostmi pri zagotavljanju nacionalne varnosti. V ta namen lahko vzpostavijo svoje varnostno-operativne centre, ki stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru na področju njihovega delovanja ter o svojem delu redno poročajo URSIV[23].

2.2.5 Zavezanci po osnutku ZinfV-1 in direktivi NIS 2

Obstajajo tri splošna merila, ki določajo, katere organizacije morajo izpolnjevati zahteve direktive NIS 2:

- Lokacija – organizacije, ki nudijo storitve ali izvajajo dejavnosti v kateri koli državi Evropske unije (ne glede na to, ali imajo sedež v EU ali ne),
- Velikost – organizacije, ki so kategorizirane kot srednje velike ali velike,
- Industrija – organizacije, ki delujejo v katerem koli od 18 sektorjev, navedenih v prilogah 1 in 2 k osnutku ZInfV-1 in direktivi NIS 2.

---

14 Prvi odstavek 9. člena osnutka ZInfV-1.
15 Prvi odstavek 10. člena osnutka ZInfV-1, 38. in 39. člen ZInfV-1 in drugi.
16 Prvi odstavek 11. člena osnutka ZInfV-1 in prvi odstavek člena 9 direktive NIS 2.
17 Prvi odstavek 7. člena osnutka ZInfV-1 in četrti odstavek člena 3 direktive NIS 2.
18 Četrti odstavek 7. člena osnutka ZInfV-1 in četrti odstavek člena 3 direktive NIS 2.
19 Prvi odstavek 10. člena direktive NIS 2.
20 Prvi odstavek 12. člena osnutka ZInfV-1.
21 Drugi odstavek 12. člena osnutka ZInfV-1.
22 Tretji odstavek 12. člena osnutka ZInfV-1.
23 Prvi odstavek 35. člena osnutka ZInfV-1 prvi odstavek člena 20 direktive NIS 2.

Ključni informacijski sistemi so vsi omrežni in informacijski sistemi s pripadajočimi podatki zavezanca, brez katerih ta ne more neprekinjeno izvajati storitev.[24]

Osnutek ZInfV-1 in direktiva NIS 2 predvidevata delitev zavezancev na **bistvene** in **pomembne** subjekte. Ta delitev je pomembna, saj za oba tipa organizacij veljajo nekoliko različne zahteve.

2.2.5.1 Bistveni subjekti

Bistveni subjekti delujejo v sektorjih, ki so ključni za gospodarstvo in družbo. Sem spadajo energetika (elektrika, nafta, plin), transport (zračni, železniški, vodni, cestni), bančništvo, infrastruktura finančnih trgov, zdravstveni sektor (bolnišnice, klinike), oskrba in distribucija pitne vode, digitalna infrastruktura (ponudniki storitev DNS, registri TLD imen[25]), javna uprava in vesolje. Bistveni subjekti so torej organizacije z vsaj 250 zaposlenimi in letnim prometom najmanj 50 milijonov evrov ali letno bilančno vsoto najmanj 42 milijonov evrov, ki delujejo v naštetih sektorjih.

Poleg tega so bistveni subjekti tudi:

- ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS ne glede na njihovo velikost,
- ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev z vsaj 50 zaposlenimi in letnim prometom ali letno bilančno vsoto vsaj 10 milijonov evrov,
- organizacije javne uprave na državni ravni,
- subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo, in
- subjekti, ki so bili prej določeni kot izvajalci bistvenih storitev po prejšnjem ZInfV.[26]

2.2.5.2 Pomembni subjekti

Pomembni subjekti so prav tako ključni, vendar morda manj kritični kot bistveni. Sem spadajo poštne in kurirske storitve, upravljanje z odpadki, proizvodnja, predelava in distribucija kemikalij, proizvodnja, predelava in distribucija hrane ter proizvodnja elektronike, računalnikov, optičnih izdelkov, električne opreme, strojev, motornih vozil, prikolic, polprikolic in drugih prevoznih sredstev, pa tudi digitalni ponudniki (spletne tržnice, spletni iskalniki, družabna omrežja). Pomembni subjekti so organizacije, ki delujejo v teh sektorjih, poleg njih pa tudi organizacije iz sektorjev bistvenih subjektov, ki ne dosegajo njihovega praga velikosti, ter drugi zavezanci po različnih kriterijih.[27]

2.2.5.3 Seznam zavezancev

URSIV vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen, in ga redno, oziroma vsaj na dve leti, posodablja[28]. Prvi seznam naj bi bil vzpostavljen v roku dveh mesecev po sprejemu ZInfV-1.[29]

2.2.6 Odgovornosti poslovodstva po ZInfV-1

Poslovodstva zavezancev so izrecno odgovorna za:

- ukrepe za obvladovanje tveganj na področju kibernetske varnosti in njihovo izvajanje,[30]

---

[24] 5. člen osnutka ZInfV-1 in 6. člen direktive NIS 2.

[25] Registri TLD imen (angl. Top-Level Domain, vrhnje domene) so odgovorni za upravljanje in vzdrževanje specifičnih vrhnjih domen, kot so ".com," ".org," ".gov," ".eu," ali nacionalne domene, kot je ".si" za Slovenijo. Te organizacije zagotavljajo infrastrukturo in postopke, ki omogočajo registracijo domenskih imen pod določeno vrhnjo domeno, ter skrbijo za pravilno delovanje in varnost omrežja v okviru te domene. (OpenAI ChatGPT, 2024, 16. oktober). Za domene, kot je ".si," je na primer odgovoren register Arnes - Akademska in raziskovalna mreža Slovenije.

[26] Drugi odstavek 6. člena osnutka ZInfV-1 in prvi odstavek člena 3 direktive NIS 2.

[27] Tretji odstavek 6. člena osnutka ZInfV-1 in drugi odstavek člena 3 direktive NIS 2

[28] Četrti odstavek 7. člena osnutka ZInfV-1 in tretji odstavek člena 3 direktive NIS 2

[29] Prvi odstavek 56. člena osnutka ZInfV-1.

[30] Prvi in drugi odstavek 19. člena osnutka ZInfV-1 ter prvi odstavek člena 20 direktive NIS 2.

- izobraževanje na področju kibernetske varnosti tako za člane poslovodstva kot tudi za zaposlene, še posebej za skrbnike informacijskih sistemov[31]
- ocene skladnosti pri bistvenih subjektih,[32]
- izvedba ukrepov za odpravo nepravilnosti oziroma pomanjkljivosti, odkritih v inšpekcijskih pregledih.[33]

2.3 Ključne zahteve osnutka ZInfV-1 in direktive NIS 2 za zavezance

V nadaljevanju povzemam zahteve osnutka ZInfV-1 in direktive NIS 2, ki zavezancem predpisujejo vrste in najmanjši sprejemljiv obseg notranjih kontrol, namenjenih obvladovanju tveganj na področju kibernetske odpornosti.

2.3.1 Upravljanje in izobraževanje

Poslovodstvo zavezancev se mora redno izobraževati o kibernetski odpornosti v okviru izobraževalnih programov URSIV[34] in mora poleg tega zagotoviti ustrezna usposabljanja tudi za zaposlene[35]. Prav tako mora zagotoviti, da imajo vsi skrbniki informacijsko-komunikacijskih sistemov obveznost rednega letnega usposabljanja na področju kibernetske odpornosti.[36]

2.3.2 Samoregistracija

Zavezanci se morajo registrirati prek mehanizma za samoregistracijo URSIV in podati vsaj naslednje informacije:

- ime in naslov, kontaktne podatke, matično številko ter elektronski naslov zavezanca za vročanje;
- dodeljene bloke javnih naslovov IP;
- kontaktno osebo za informacijsko varnost in njenega namestnika ter njune kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami;
- sektor in podsektor, v katerem izvajajo storitve;
- seznam držav članic Evropske unije, kjer opravljajo storitve, ter
- registrirane številke avtonomnih sistemov in vsa domenska imena, ki jih zavezanec uporablja pri poslovanju.[37]

Vse spremembe teh podatkov morajo zavezanci URSIV javiti v največ dveh tednih.[38]

Tudi nekatere organizacije, ki imajo sedež v drugi državi članici EU, vendar poslujejo na ozemlju Republike Slovenije, morajo URSIV zaradi olajšanega sodelovanja s pristojnimi organi pri obvladovanju incidentov podati informacije o kontaktnih točkah in o svojem poslovanju.[39]

2.3.3 Varnostna dokumentacija

Zavezanci morajo za zagotavljanje visoke ravni informacijske in kibernetske odpornosti svojih omrežnih in informacijskih sistemov vzpostaviti in vzdrževati dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti in morata obsegati najmanj:

---

31 Tretji, četrti in peti odstavek 19. člena osnutka ZInfV-1 ter drugi odstavek 20. člena direktive NIS 2

32 Prvi odstavek 45. člena osnutka ZInfV-1.

33 Drugi odstavek 42. člena osnutka ZInfV-1

34 Šesti odstavek 19. člena osnutka ZInfV-1.

35 Tretji in četrti odstavek 19. člena osnutka ZInfV-1 ter drugi odstavek 20. člena direktive NIS 2

36 Peti odstavek 19. člena osnutka ZInfV-1.

37 Drugi odstavek 7. člena osnutka ZInfV-1 in četrti odstavek člena 3 direktive NIS 2.

38 Tretji odstavek 7. člena osnutka ZInfV-1 in četrti odstavek člena 3 direktive NIS 2.

39 27 .in 28. člen osnutka ZInfV-1.

- natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter določitev njihovih upravljavcev;
- analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
- politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij ter določitvijo vlog in odgovornosti;
- načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
- načrt odzivanja na incidente s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;
- načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upošteva posebnosti bistvenega ali pomembnega subjekta;
- politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov[40]

Že izdelano varnostno dokumentacijo na podlagi drugih predpisov morajo za skladnost z ZInfV-1 ustrezno dopolniti.[41]

Zavezanci določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, ki mora obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke ter procese, ki so potrebni za njihovo delovanje ali opravljanje storitev.[42]

2.3.4 Ukrepi za obvladovanje tveganj za kibernetsko varnost

Zavezanci morajo sprejeti ustrezne, učinkovite in sorazmerne tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve.[43] Sorazmernost se nanaša na stopnjo, do katere je zavezanec izpostavljen tveganjem, njegovo velikost, verjetnost pojava incidentov ter resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom.[44]

Varnostni ukrepi zavezancev morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti, in morajo obsegati najmanj:

- podporo poslovodstva pri zagotavljanju informacijske varnosti in kibernetske odpornosti,
- vključitev področja informacijske varnosti v letni načrt dela,
- zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve,
- osnovne prakse kibernetske higiene[45] in usposabljanje na področju kibernetske odpornosti,
- varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop,

---

[40] Prvi odstavek 20. člena osnutka ZInfV-1.

[41] Tretji odstavek 20. člena osnutka ZInfV-1.

[42] Drugi odstavek 20. člena osnutka ZInfV-1.

[43] Prvi odstavek 21. člena osnutka ZInfV-1 in prvi odstavek člena 21 direktive NIS 2.

[44] Tretji odstavek 21. člena osnutka ZInfV-1.

[45] V skladu s 5. členom ZInfV-1 izraz kibernetska higiena pomeni dobro prakso ohranjanja varnosti in zaščite informacij v digitalnem okolju. To vključuje različne ukrepe in postopke, namenjene zaščiti računalniških sistemov, omrežij in podatkov pred različnimi varnostnimi grožnjami.

- izvajanje in upravljanje varnostnih kopij podatkov,
- zagotavljanje in ohranjanje dnevniških zapisov,
- upravljanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito,
- politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem,
- upravljanje prometa in komunikacij,
- obvladovanje incidentov,
- varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim zavezancem in njegovimi neposrednimi dobavitelji ali ponudniki storitev,
- fizično in tehnično varovanje prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev,[46]
- varnostne mehanizme v posamezni informacijski rešitvi za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter obravnavanjem in razkrivanjem ranljivosti,
- upravljanje in preprečevanje izrab tehničnih ranljivosti,
- zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov,
- uporabo večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost, in
- kadar je primerno, uporabo varovanih glasovnih, video in besedilnih komunikacij ter varnih sistemov za komunikacije v sili znotraj zavezanca.[47]

Zavezanci morajo vzpostavljene ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov najmanj enkrat letno preverjati ter brez nepotrebnega odlašanja sprejeti njihove morebitne korekcije.[48]

Zavezanci ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti, brez dodatne izvedbe ocene tveganja in, kjer je to glede na oceno tveganja primerno, uvedbe ustreznih popravljalnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven.[49]

2.3.5 Uporaba certificiranih proizvodov in postopkov

Zavezanci naj bi pri izboru tehnologij in postopkov za svoja informacijska okolja prednostno izbirali proizvode, storitve in postopke, ki so jih razvili drugi zavezanci, skladni z direktivo NIS 2, ali pa izdelke, ki so bili kupljeni pri tretjih straneh in certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi 49. člena Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske odpornosti ter razveljavitvi Uredbe (EU) št. 526/2013 (v nadaljevanju: Akt o kibernetski odpornosti)[50]. Kjer je le mogoče, naj bi uporabljali tudi kvalificirane storitve zaupanja.[51]

---

[46] Pri tem morajo v skladu s petim odstavkom 21. člena osnutka ZInfV-1 in tretjim odstavkom 21. člena direktive NIS 2 upoštevati ranljivosti, 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.

[47] Drugi odstavek 21. člena osnutka ZInfV-1 in drugi odstavek člena 21 direktive NIS 2.

[48] Šesti odstavek 21. člena osnutka ZInfV-1 in četrti odstavek člena 21 direktive NIS 2.

[49] Deveti odstavek 21. člena osnutka ZInfV-1.

[50] Prvi odstavek 23. člena osnutka ZInfV-1 in prvi odstavek člena 24 direktive NIS 2.

[51] Drugi odstavek 23. člena osnutka ZInfV-1 in prvi odstavek člena 24 direktive NIS 2. Temeljne storitve zaupanja vključujejo digitalne certifikate, ki omogočajo preverjanje identitete posameznikov in organizacij v digitalnem okolju, ter elektronske podpise, ki omogočajo pravno zavezujoče podpisovanje dokumentov v elektronski obliki. Vključujejo tudi elektronske žige, ki so namenjeni potrjevanju pristnosti in celovitosti dokumentov za pravne osebe, ter časovne žige, ki omogočajo dokazljivost časa nastanka ali spremembe digitalnih dokumentov. Poleg tega so pomembne elektronske storitve priporočene dostave, ki omogočajo varno pošiljanje elektronskih sporočil s potrditvijo prejema in celovitostjo vsebine, ter potrdila za spletna mesta (TLS/SSL certifikati), ki zagotavljajo šifrirano povezavo med spletnimi stranmi in uporabniki za zaščito pred prestrezanjem ali spremembami komunikacije.

2.3.6 Standardizacija

Zavezanci naj bi v čim večji meri uporabljali evropske in mednarodne standarde ter tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. Pri tem naj bi upoštevali tudi nasvete in smernice ENISA.[52].

Pojasnilo k temu določilu v osnutku ZInfV-1 izpostavlja standarde ISO/IEC 27001 in ISO/IEC 27002, ki ju je izdala Mednarodna organizacija za standardizacijo, NIST Cybersecurity Framework, ki ga je izdal Nacionalni inštitut za standarde in tehnologijo ZDA, CIS Controls, ki jih je izdala zasebna organizacija Center for Internet Security, ter Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Kot sem pojasnila v točki 3.2, sem za namene zaključnega dela predpostavila, da revidirana organizacija za oblikovanje procesov, in obvladovanje tveganj na področju kibernetske odpornosti uporablja Sistem osnovnega varovanja BSI.

2.3.7 Vrednotenje incidentov in ocena ogroženosti

Pri določitvi pomembnosti incidenta se praviloma[53] upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja.[54]

V praksi priglašene incidente pri njihovem reševanju vrednoti pristojna skupina CSIRT po lestvici od C6 – varnostni dogodek, do C1 – kritični incident,[55] URSIV pa izdela oceno ogroženosti.[56]

2.3.8 Obvezno posredovanja podatkov in informacij

URSIV lahko od zavezancev kadarkoli pisno zahteva podatke in informacije, pri čemer mora biti njihov obseg sorazmeren namenu, za katerega bodo uporabljeni, URSIV pa mora namen zahteve tudi razkriti.[57]

2.3.9 Obvezno priglašanje incidentov skupinam CSIRT

Zavezanci morajo pristojno skupino CSIRT brez odlašanja obvestiti o vseh incidentih, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Incident se šteje za pomembnega, če:

- je zavezancu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;
- je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.[58]

Pri tem morajo

- brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po zaznavi incidenta, pripraviti zgodnje opozorilo, iz katerega je po potrebi razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali bi lahko imel čezmejni vpliv;
- brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po zaznavi pomembnega incidenta, priglasiti incident, pri čemer se po potrebi posodobijo informacije in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter, kadar so na voljo, kazalniki ogroženosti;
- na zahtevo skupine CSIRT pripraviti vmesno poročilo o ustreznih posodobitvah stanja in
- predložiti končno poročilo najpozneje v enem mesecu po predložitvi priglasitve incidenta, ki vključuje naslednje:

---

52 Prvi odstavek 24. člena osnutka ZInfV-1 in prvi odstavek člena 25 direktive NIS 2.

53 Kadar za posamezno vrsto zavezanca ne obstajajo ločeni izvedbeni akti Evropske komisije ali drugi predpisi.

54 Četrti odstavek 26. člena osnutka ZINfV-1.

55 Prvi odstavek 32. člena osnutka ZInfV-1 in drugi odstavek člena 23 direktive NIS 2.

56 Prvi odstavek 33. člena osnutka ZInfV-1 in enajsti odstavek člena 23 direktive NIS 2

57 22.člen osnutka ZInfV-1.

58 Prvi odstavek 25. člena osnutka ZInfV-1 in drugi odstavek člena 23 direktive NIS 2.

- podroben opis incidenta, vključno z njegovo resnostjo in vplivom;
- vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;
- izvedene blažilne ukrepe in ukrepe v teku;
- po potrebi čezmejni vpliv incidenta;
- v primeru incidenta, ki je dva meseca po priglasitvi še vedno v teku, priglasitveni subjekt predloži poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta.[59]

2.3.10 Sodelovanje s pristojno skupino CSIRT in URSIV pri obvladovanju incidenta

Pristojna skupina CSIRT naj bi brez nepotrebnega odlašanja in po možnosti v 24 urah zavezancu posredovala povratne informacije ter na zahtevo zagotovila tehnično podporo.[60]

URSIV, ki od pristojne skupine CSIRT prejema podatke o incidentu, lahko v primeru z višjo stopnjo kritičnosti s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot so potrebni za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic.[61] Zoper odločbo ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu Upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.[62]

Direktor URSIV lahko z namenom preprečitve nastanka krize ali njenega obvladovanja oziroma zaradi hitrejšega obvladovanja razmer in omejevanja nadaljnjih škodljivih posledic incidenta izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih. Odredba se izda pisno, izjemoma, če razmere to onemogočajo, pa ustno in naknadno tudi pisno, takoj ko je to mogoče. V odredbi se določita zlasti vrsta in obseg del, ki jih je treba opraviti, ter rok.

Kadar URSIV za odločanje potrebuje dodatne informacije, lahko s pisno odločbo, v nujnih primerih pa tudi ustno, od zavezanca zahteva posredovanje dodatnih podatkov in pojasnil ter določi rok za njihovo posredovanje.[63]

2.3.11 Pomoč na področju kibernetske obrambe

URSIV lahko v primeru kibernetskih groženj in incidentov na prošnjo zavezancev ali pristojne skupine CSIRT nudi zavezancem dodatno pomoč na področju kibernetske obrambe.[64]

2.3.12 Prostovoljno priglaševanje incidentov skupinam CSIRT

Zavezanci lahko skupinam CSIRT prostovoljno priglasijo tudi druge incidente.[65]

Tudi fizične in pravne osebe, ki niso zavezanci po ZInfV-1 in NIS 2, lahko skupinam CSIRT prostovoljno priglasijo incidente, pri čemer zanje iz tega ne izhajajo dodatne obveznosti.[66] Pristojni skupini CSIRT lahko pred prostovoljnimi priglasitvami prednostno obravnavata obvezne priglasitve.[67] Prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev zavezancev ter imajo zanemarljiv čezmejni vpliv, se obdelajo le, kadar takšna obdelava za skupini CSIRT ne predstavlja nesorazmernega ali neupravičenega bremena.[68]

---

[59] Prvi odstavek 26. člena osnutka ZInfV-1 in četrti odstavek člena 23 direktive NIS 2.
[60] Tretji odstavek 26. člena osnutka ZInfV-1 in peti odstavek člena 23 direktive NIS 2.
[61] Četrti odstavek 32. člena osnutka ZInfV-1 in peti odstavek člena 23 direktive NIS 2.
[62] Šesti odstavek 32. člena osnutka ZInfV-1 in peti odstavek člena 23 direktive NIS 2.
[63] Peti odstavek 32. člena osnutka ZInfV-1 in peti odstavek člena 23 direktive NIS 2.
[64] 37. člen osnutka ZInfv-1 in člen 7 direktive NIS 2.
[65] Prvi odstavek 31. člena osnutka ZInfV-1 in člen 30 direktive NIS 2.
[66] Drugi odstavek 31. člena osnutka ZInfV-1 in člen 30 direktive NIS 2.
[67] Peti odstavek 31. člena osnutka ZInfV-1 in člen 30 direktive NIS 2.
[68] Šesti odstavek 31. člena osnutka ZInfV-1 in člen 30 direktive NIS 2.

2.3.13 Obveščanje strank zavezancev in javnosti

Zavezanci naj o incidentih kadar je primerno, obvestijo tudi svoje stranke.[69] Kadar bi jih pomembna kibernetska grožnja lahko prizadela, jim morajo sporočiti vse ukrepe ali sredstva, ki jih lahko ti prejemniki sprejmejo v odziv na to grožnjo.[70]

Kadar je to primerno URSIV ali sam zavezanec o grožnji obvestita tudi javnost.[71]

2.3.14 Hramba dnevniških zapisov

Zavezanci morajo zagotoviti ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja za obdobje šestih mesecev ali dlje. Ohranjanje dnevniških zapisov se izvaja na ozemlju Republike Slovenije, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, kjer se lahko zagotavlja na ozemlju EU.[72]

Dnevniški zapisi morajo biti hranjeni na način, ki zagotavlja njihovo avtentičnost, celovitost in razpoložljivost v primeru incidentov.[73]

2.4 Ocena skladnosti

Odgovorne osebe zagotovijo, da bistveni subjekti izvajajo oceno skladnosti sprejetih ukrepov za obvladovanje tveganj kibernetske varnosti, medtem ko pomembni subjekti izvajajo samooceno skladnosti takšnih ukrepov.[74]

2.4.1 Ocena skladnosti pri bistvenih subjektih

Bistveni subjekti morajo opraviti oceno skladnosti najmanj enkrat na dve leti ali, če to zahteva inšpektor na primer v primeru pojava pomembnega incidenta.[75] Ocena skladnosti se izvaja na stroške zavezanca kot revizija informacijske varnosti[76] ali v okviru revizije poslovanja, ki se izvaja na podlagi drugih predpisov in vključuje tudi področje informacijske varnosti iz osnutka ZInfV-1 ter podzakonskih predpisov ali izvedbenih aktov, izdanih na podlagi ZInfV-1, ali izvedbenih aktov Evropske komisije. Rezultat revizije mora biti izdano pisno poročilo o skladnosti,[77] ki ga je potrebno posredovati inšpektorju v osmih dneh po njegovem prejemu.[78].

2.4.2 Samoocena skladnosti pri pomembnih subjektih

Pomembni subjekti morajo opraviti najmanj enkrat na dve leti opraviti samooceno skladnosti[79]. Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt izpolnjuje zahteve ZInfV-1, mora v osmih dneh predložiti inšpektorju izjavo o skladnosti.[80]

---

69 Šesti odstavek 25. člena osnutka ZINfV-1.
70 Sedmi odstavek 25. člena osnutka ZINfV-1.
71 Šesti odstavek 26. člena osnutka ZInfV-1 in sedmi odstavek člena 23 direktive NIS 2.
72 Drugi odstavek 21. člena osnutka ZInfV-1.
73 Četrti odstavek 21. člena osnutka ZInfV-1.
74 Prvi odstavek 45. člena osnutka ZInfV-1.
75 Drugi odstavek 45. člena osnutka ZInfV-1.
76 Sedmi odstavek 45. člena osnutka ZInfV-1.
77 Četrti odstavek 45. člena osnutka ZInfV-1.
78 Peti odstavek 45. člena osnutka ZInfV-1.
79 Prvi odstavek 46. člena osnutka ZinfV-1.
80 Drugi in tretji odstavek 46. člena osnutka ZinfV-1.

2.5 Nadzor

2.5.1 Inšpektorji za informacijsko varnost

Za nadzor nad izvajanjem ZInfV-1 so pristojni inšpektorji za informacijsko varnost URSIV,[81] ki morajo pri svojem delu upoštevati določbe zakona, ki ureja inšpekcijski nadzor.[82]

Inšpektorji nadzirajo, ali zavezanci izpolnjujejo svoje obveznosti, predvsem z:

- neposrednim vpogledom v podatke, dokumentacijo ter v omrežne in informacijske sisteme,
- preverjanjem pogojev in načina izvajanja ukrepov za obvladovanje tveganj na področju kibernetske odpornosti,
- pregledom območij, objektov in prostorov zavezancev, kjer se nahajajo ključni, krmilni in nadzorni informacijski sistemi ter podatki, pregledom dokumentacije o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih in drugih obveznosti na podlagi zahtev pristojnih organov iz osnutka ZInfV-1,
- pregledom poročil o izvedbi revizije informacijskih sistemov in varnostnih pregledov omrežja ter informacijskih sistemov ter pregledom druge dokumentacije, potrebne za izvedbo nadzora.[83]

2.5.2 Izvajanje nadzornih nalog

Inšpektor ima pri izvajanju nadzornih nalog pri bistvenih subjektih poleg pooblastil, ki jih določa zakon o inšpekcijskem nadzoru, tudi pravico:

- opraviti inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi, ki jih lahko izvede skupaj z usposobljenimi strokovnjaki;
- odrediti izvedbo ciljno usmerjene revizije varnosti, pri bistvenih subjektih pa tudi redne revizije varnosti, ki jo izvede preizkušeni revizor informacijskih sistemov;[84] stroške revizije krije zavezanec,[85] če revizorja ne določi zavezanec, pa ga določi inšpektor[86];
- zahtevati izvedbo izredne revizije, tudi ko je to utemeljeno zaradi pomembnega incidenta ali kršitve osnutka ZInfV-1 s strani bistvenega subjekta;
- opraviti varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, pri čemer po potrebi sodeluje z zadevnim subjektom;
- odrediti zavezancu, da obvesti fizične ali pravne osebe, s katerimi opravlja storitve ali izvaja dejavnost, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje ter o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
- odrediti, da zavezanec v razumnem roku izvede priporočila, dana na podlagi izvedene revizije skladnosti;
- odrediti zavezancu, da na določen način objavi kršitve.

Poleg tega lahko inšpektor pri bistvenih subjektih imenuje pooblaščeno osebo z natančno opredeljenimi nalogami za določeno obdobje, ki spremlja izpolnjevanje določb ZInfV-1. [87]

2.5.3 Pravica do pritožbe

Zoper odločbo, izdano v postopkih nadzora, ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu Upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.[88]

---

81 Prvi odstavek 41. člena osnutka ZInfV-1 in drugi odstavek člena 32 direktive NIS 2.

82 Tretji odstavek 41. člena ZInfV-1 in drugi odstavek člena 32 direktive NIS 2.

83 Četrti odstavek 41. člena osnutka ZInfV-1, drugi odstavek člena 32 direktive NIS 2 in drugi odstavek člena 33 direktive NIS 2.

84 Prvi odstavek 47. osnutka člena ZInfV-1.

85 Četrti odstavek 41. in 43. člena osnutka ZInfV-1 drugi odstavek členov 32 in 33 direktive NIS 2.

86 Prvi in drugi odstavek 47. osnutka člena ZInfV-1.

87 Prva odstavka 42. in 44. člena osnutka ZInfV-1, druga odstavka členov 32 in 33 direktive NIS 2.

88 Šesti odstavek 40. člena ZInfV-1 in drugi odstavek člena 32 direktive NIS 2.

2.5.4 Podaljšanje rokov za odpravo nepravilnosti

Inšpektor lahko v inšpekcijskem postopku na podlagi obrazloženega predloga zavezanca za podaljšanje rokov za odpravo nepravilnosti in pomanjkljivosti, ki je podan pred potekom roka za izvedbo odrejenih ukrepov, podaljša roke za odpravo nepravilnosti in pomanjkljivosti oziroma izvedbo odrejenih ukrepov. Pri tem upošteva že izvedene aktivnosti zavezanca za odpravo nepravilnosti in pomanjkljivosti, objektivne okoliščine za zamudo in posledice za javni interes.[89]

2.5.5 Kršitve, ki pomenijo kršitev varstva osebnih podatkov

Inšpektor o kršitvah, katerih posledica je kršitev varstva osebnih podatkov, in tudi že o samih sumih kršitev obvešča Informacijskega pooblaščenca.[90] Kadar Informacijski pooblaščenec zaradi kršitve varstva osebnih podatkov zavezancu naloži globo, inšpektor za informacijsko varnost zavezancu za isto kršitev ne naloži dodatne globe.[91]

2.6 Globe

2.6.1 Globe za zavezance

Direktiva NIS 2 prepušča določitev podrobnosti sankcioniranja nacionalnim državam in predpisuje le, da morajo biti sankcije učinkovite, sorazmerne in odvračilne. Globe so predpisane, če zavezanec:

- ne izpolni obveznosti samoregistracije ali naknadne spremembe podatkov iz drugega in tretjega odstavka 7. člena osnutka ZInfV-1,[92]
- odgovorne osebe zavezancev ne odobrijo ukrepov za obvladovanje tveganj na področju kibernetske odpornosti ali ne nadzirajo njihovega izvajanja, kot to zahteva drugi odstavek 19. člena osnutka ZInfV-1,[92]
- odgovorne osebe zavezanca ne opravijo izobraževanja o področju obvladovanja tveganj na področju kibernetske odpornosti in vpliva teh tveganj na dejavnosti oziroma storitve, ki jih izvaja zavezanec, kot to zahteva tretji odstavek 19. člena osnutka ZInfV-1, [92]
- na podlagi pisne zahteve pristojnemu organu ne posreduje obveznih informacij iz prvega odstavka 22. člena osnutka ZInfV-1, [92]
- ne upošteva delegiranih aktov Evropske komisije o uporabi določenih certificiranih proizvodov , storitve in procese ali o pridobitvi certifikata na podlagi evropske certifikacijske sheme za kibernetsko varnostne iz štirinajstega odstavka 23. člena osnutka ZInfV-1, [92]
- ne uporablja evropskih in mednarodnih standardov in tehničnih specifikacij, ki obravnavajo varnost omrežnih in informacijskih sistemov iz prvega odstavka 24. člena osnutka ZInfV-1, [92]
- ne posreduje informacij za register ponudnikov storitev pri ENISA, kot zahtevajo prvi, drugo ali tretji odstavek 28. člena osnutka ZInfV-1,[92]
- kot register TLD imen ali subjekt, ki opravlja storitve registracije domenskih imen ne izpolni dodatnih obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 29. člena osnutka ZInfV-1, [92]
- kot bistveni subjekt ne izvaja ocen skladnosti iz prvega, drugega, tretjega, petega ali šestega odstavka 45. člena osnutka ZInfV-1, [92]
- kot pomemben subjekt ne izvaja samoocen skladnosti iz tretjega odstavka 46. člena osnutka ZInfV-1,[92]
- ne pripravi varnostne dokumentacije iz 20. člena osnutka ZInfV-1,[93]
- ne uvede in ne izvaja ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, kot jih predpisuje 21. člen osnutka ZInfV-1[93] ali

---

89 Sedmi odstavek 40. člena ZInfV-1 in drugi odstavek člena 32 direktive NIS 2.

90 Prvi odstavek 48. člena ZInfV-1 prvi odstavek člena 35 direktive NIS 2.

l91 Drugi odstavek 48. člena ZInfV-1 drugi odstavek člena 35 direktive NIS 2.

92 Četrta odstavka 53. člena in 54. člena ZInfV-1. Predvidene globe se gibljejo med 1.000 in 15.000 EUR.

93 Prva odstavka 53. člena in 54. člena ZInfV-1. Predvidene globe se gibljejo med 7.000 in 10.000.000 EUR.

- ne izpolni obveznosti preglašanja in obveščanja o incidentih, kot jih predpisuje 25. člen osnutka ZInfV-1 oziroma če pri priglasitvi incidentov ne ravna v skladu z zahtevami 26. člena ZInfV-1. [93]

Globe, predpisane v osnutku ZInfV-1 za kršitve, se razlikujejo glede na resnost prekrška in status zavezanca. Za srednja in velika podjetja se globe gibljejo od nekaj tisoč evrov do največ 10 milijonov evrov. Najvišja globa za naklepne ali iz malomarnosti storjene prekrške bistvenih subjektov lahko znaša do 2 % letnega prometa podjetja, vendar ne več kot 10 milijonov evrov[94]. Za pomembne subjekte, ki so prav tako srednja ali velika podjetja, lahko globa doseže do 1,4 % letnega prometa, vendar ne več kot 7 milijonov evrov za naklepne ali iz malomarnosti storjene prekrške.[95] Globe, izrečene v hitrem prekrškovnem postopku, so lahko tudi nižje.[96]

Višina globe je torej odvisna od več dejavnikov, vključno z:

- velikostjo podjetja: globe so višje za srednja in velika podjetja,
- letnim prometom: odstotek globe se izračuna na podlagi letnega prometa podjetja,
- naravo prekrška: višje globe so predvidene za prekrške, storjene naklepno ali iz malomarnosti.

Poleg tega se pri odločanju o višini globe upoštevajo tudi okoliščine posameznega primera, kot so prejšnje kršitve, narava kršitve in potencialni vpliv kršitve na varnost podatkov ali sistemov.[97]

2.6.2 Globe za odgovorne osebe zavezancev

Osnutek ZInfV-1 ob globah za zavezance, ki jih naštevam v točki 2.6.1 predvideva tudi nekatere globe za odgovorne osebe zavezancev[98]. Globe se, glede na vrsto zavezanca,[99]resnost prekrška, okoliščine prekrška[100] in različne druge dejavnike gibljejo od 200,00 eurov do 20.000,00 eurov.[101]

2.7 Dodatni ukrepi nadzora pri bistvenih subjektih

Če inšpektor ugotovi, da ukrepi, ki jih je naložil bistvenemu subjektu, niso bili učinkoviti, določi rok, v katerem mora subjekt sprejeti potrebne ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev inšpektorja. Če subjekt teh ukrepov ne sprejme v določenem roku, lahko inšpektor z odločbo:

- začasno prekliče certifikat ali dovoljenje za del ustreznih storitev ali začasno prepove izvajanje dejavnosti oziroma vse storitve ali dejavnosti, ki jih opravlja bistveni subjekt;
- zahteva začasno prepoved opravljanja vodstvenih funkcij vsem osebam, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika.[102]

Začasni preklic ali prepoved se uporabljata le, dokler zadevni bistveni subjekt ne sprejme ukrepov za odpravo pomanjkljivosti ali ne izpolni zahtev inšpektorja, zaradi katerih je bil ukrep uporabljen,[103] in se ne uporabljata za zavezance v javni upravi[104].

Inšpektor pri sprejemanju ukrepov za bistvene in pomembne subjekte upošteva okoliščine vsakega posameznega primera, pri čemer ustrezno upošteva vsaj naslednje dejavnike:

- resnost kršitve in pomembnost kršenih določb, pri čemer se med resne kršitve v vsakem primeru štejejo:

---

94 Prvi odstavek 53. člena ZInfV-1 in prvi, drugi ter četrti odstavek 50. člena ZInfV-1.

95 Prvi odstavek 54. člena ZInfV-1. in prvi, tretji ter četrti odstavek 50. člena ZInfV-1.

96 51. člen osnutka ZInfV-1.

97 Četrti odstavek 50. člena osnutka ZInfV-1.

98 V skladu s 53. in 54. člen ZInfV-1 je lahko to odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, če stori prekršek iz prvega odstavka tega člena.

99 Torej ali gre za bistven ali za pomemben subjekt,

100 42. člen in 45. člen ZInfV-1 predvidevata nekatere omejitve pri izrekanju denarnih kazni, ki izhajajo iz izvršbe izvršljivih odločb, ki jih je inšpektor izdal v postopku nadzora bistvenih subjektov.

101 Tretji in šesti odstavek 53. člena ter tretji in šesti odstavek 54. člena.

102 Drugi odstavek 42. člena osnutka ZInfV-1 in peti odstavek člena 32 direktive NIS 2.

103 Tretji odstavek 42. člena osnutka ZInfV-1 in peti odstavek člena 32 direktive NIS 2.

104 Četrti odstavek 42. člena osnutka ZInfV-1 in peti odstavek člena 32 direktive NIS 2.

  - ponavljajoče se kršitve,
  - nepriglasitev ali neodprava pomembnih incidentov,
  - neodprava pomanjkljivosti v skladu z zavezujočimi navodili inšpektorja,
  - oviranje revizij ali dejavnosti spremljanja, ki jih je odredil inšpektor po ugotovitvi kršitve,
  - predložitev napačnih ali zelo netočnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja;

- trajanje kršitve;
- vse relevantne prejšnje kršitve;
- morebitno povzročeno premoženjsko ali nepremoženjsko škodo, vključno s finančnimi ali gospodarskimi izgubami, učinki na druge storitve in številom prizadetih uporabnikov;
- morebitni naklep ali malomarnost storilca kršitve;
- morebitne ukrepe, ki jih je zavezanec sprejel za preprečevanje ali zmanjšanje premoženjske ali nepremoženjske škode;
- morebitno upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;
- raven sodelovanja odgovornih fizičnih ali pravnih oseb z inšpektorjem.[105]

[105] Šesti odstavek 42. in drugi odstavek 44. člena osnutka ZInfV-1.

3 Načrt svetovalnega posla

3.1 Pristop k načrtovanju

Pri načrtovanju svetovalnega posla sem smiselno izhajala iz zahtev standardov. Poleg standardov, ki se izrecno nanašajo na svetovalne posle, sem upoštevala tudi zahteve standardov za dajanje zagotovil.

V skladu s standardom 2201 sem pri načrtovanju svetovalnega posla upoštevala naslednje vidike:

- strategije in cilje, ki jih revidirana organizacija zasleduje z uporabo spletnih tehnologij in orodij, storitve, ki jih z njimi nudi, njene prihodnje cilje na tem področju, njen status bistvenega ali pomembnega subjekta ter cilje na področju uskladitve z zahtevami direktive NIS 2 in osnutka ZInfV-1;
- pomembna tveganja neskladij s predpisi za cilje, vire in delovanje organizacije;
- pomembna tveganja na področju kibernetske odpornosti, ki vplivajo na cilje, vire in delovanje organizacije;
- načine, s katerimi se vpliv tveganj ohranja na sprejemljivi ravni;
- ustreznost in uspešnost upravljanja področja skladnosti, upravljanja tveganj in kontrolnih postopkov glede na zahteve direktive NIS 2 in osnutka ZInfV-1;
- ustreznost in uspešnost upravljanja področja kibernetske odpornosti, upravljanja tveganj in kontrolnih postopkov glede na sodila poslovodstva organizacije;
- priložnosti za izboljšave pri upravljanju dejavnosti, upravljanju tveganj in kontrolnih postopkih.

Standard 2110.A določa, da mora funkcija notranje revizije presoditi, ali upravljanje informacijske tehnologije v organizaciji podpira strategije in cilje organizacije. Standard 2120.A1 pa zahteva, da notranja revizija oceni izpostavljenost tveganjem, povezanim z upravljanjem, delovanjem in informacijskimi sistemi organizacije, pri čemer upošteva doseganje strateških ciljev, zanesljivost in neoporečnost računovodskih ter poslovnih informacij, uspešnost in učinkovitost delovanja in programov, varovanje premoženja ter skladnost z zakoni, predpisi, usmeritvami, postopki in pogodbami. Čeprav se ta standarda nanašata na posle dajanja zagotovil, sem ju smiselno vključila v načrt svetovalnega posla.

3.2 Cilji organizacije pri uskladitvi z zahtevami osnutka ZInfV-1 in direktive NIS 2

Cilj organizacij pri vzpostavitvi postopkov za obvladovanje tveganj in notranjih kontrol je doseganje skladnosti s predpisi. Ker pa ti predpisi urejajo področje kibernetske odpornosti, ki je bistvenega pomena za sodobno poslovanje, se organizacije ne bi smele omejiti zgolj na formalno usklajevanje z zahtevami osnutka ZInfV-1 in direktive NIS 2. Njihova prizadevanja bi morala preseči zakonske zahteve ter se osredotočiti na krepitev odpornosti proti kibernetskim napadom in izboljšanje učinkovitosti odzivanja nanje. S tem organizacije ne samo izpolnjujejo regulatornih zahtev, temveč tudi proaktivno zmanjšujejo tveganja in izboljšujejo svoje notranje kontrolno okolje.

Za uskladitev z zahtevami osnutka ZInfV-1 in direktive NIS 2 ter vzpostavitev kibernetske odpornosti morajo poslovodstva organizacij oblikovati jasno strategijo. To vključuje opredelitev izvedbenih postopkov, vzpostavitev sistemov za obvladovanje tveganj, zasnovo učinkovitih notranjih kontrol, določitev kazalnikov za oceno učinkovitosti, vzpostavitev postopkov spremljanja izvedbenih ukrepov ter strukturiranje poročanja. V okviru tega zaključnega dela predpostavljam, da se je poslovodstvo organizacije pri načrtovanju teh ukrepov oprlo na okvir BSI. V nadaljevanju bo podrobneje predstavljena možna uporaba okvira BSI za vzpostavitev kibernetske odpornosti in zagotavljanje skladnosti z osnutkom ZInfV-1 in direktivo NIS 2..

3.2.1 Okvir BSI

Okvir BSI izhaja iz standardov informacijske varnosti družine ISO 2700x in jih v veliki meri nadgrajuje. Združuje priporočila za poslovodstva organizacij o metodah, procesih, postopkih, pristopih in ukrepih za različne vidike varnosti informacij. To vključuje krepitev odpornosti proti kibernetskim napadom in izboljšanje učinkovitosti odzivanja nanje, kar so področja, ki jih urejata osnutek ZInfV-1 in direktiva NIS 2.

Sistem osnovnega varovanja informacijskih tehnologij BSI je sestavljen iz štirih standardov in ene zbirke znanja. Standardi BSI so:

- BSI 200-1 - Sistemi za upravljanje varnosti informacij[106] [107], ki opredeljuje splošne zahteve za sistem upravljanja informacijske varnosti in je združljiv z ISO/IEC 27001;
- BSI 200-2 - Metodologija osnovnega varovanja informacijskih tehnologij,[108] ki opisuje vzpostavitev in delovanje sistema upravljanja informacijske varnosti v praksi;
- BSI 200-3 - Upravljanje tveganj,[109] ki opisuje postopek analize tveganj po uvedbi sistema upravljanja informacijske varnosti na podlagi metodologije osnovnega varovanja informacijskih tehnologij in
- BSI 200-4 - Upravljanje neprekinjenosti poslovanja[110], obravnava sistematičen pristop k vzpostavitvi in uvedbi sistema za upravljanje neprekinjenosti poslovanja.

Zbirka znanja o osnovnem varovanju informacijskih tehnologij[111] je poslovodstvu organizacij namenjeno orodje za praktično uporabo načel sistema osnovnega varovanja BSI. Orodje izhaja iz 47. *elementarnih grožnj*[112], ki jih naslovi z 111 organizacijskimi procesi, ki predstavljajo *gradnike osnovnega varovanja* (BSI, 2021). Gradniki osnovnega varovanja v Zbirki znanja o osnovnem varovanju informacijskih tehnologij so: ISMS.1 Upravljanje varnosti informacij, ORP.1 Organizacija, ORP.2 Osebje, ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost, ORP.4 Upravljanje identitet in pravic, ORP.5 Upravljanje skladnosti (upravljanje zahtev), CON.1 Kriptokoncept, CON.2 Varstvo podatkov, CON.3 Koncept varnostnega kopiranja podatkov, CON.6 Brisanje in uničenje, CON.7 Informacijska varnost pri potovanjih v tujino, CON.8 Razvoj programske opreme, CON.9 Izmenjava informacij, CON.10 Razvoj spletnih aplikacij, CON.11.1 Varovanje tajnosti, OPS.1.1.1 Splošno delovanje informacijskih tehnologij, OPS.1.1.2 Pravilna administracija informacijskih tehnologij, OPS.1.1.3 Upravljanje popravkov in sprememb, OPS.1.1.4 Zaščita pred zlonamerno programsko opremo, OPS.1.1.5 Beleženje, OPS.1.1.6 Testiranje in odobritve programske opreme, OPS.1.1.7 Upravljanje sistemov, OPS.1.2.2 Arhiviranje, OPS.1.2.4 Delo na daljavo, OPS.1.2.5 Oddaljena podpora, OPS.1.2.6 Sinhronizacija časa z omrežnim časovnim protokolom (angl. Network Time Protocol, krat. NTP), OPS.2.2 Uporaba oblaka, OPS.2.3 Uporaba zunanjih izvajalcev, OPS.3.2 Izvajanje storitev za zunanje stranke, DER.1 Zaznavanje varnostno pomembnih dogodkov, DER.2.1 Obdelava varnostnih incidentov, DER.2.2 Priprava na forenzično preiskovanje informacijskih tehnologij, DER.2.3 Vzpostavitev delovanja po obsežnih varnostnih incidentih, DER.3.1 Revizije in pregledi, DER.3.2 Pregledi na podlagi vodnika Revizija informacijske varnosti, ki jo je izdal BSI, DER.4 Upravljanje v izrednih okoliščinah, APP.1.1 Informacijske rešitve za podporo pisarniškemu delu, APP.1.2 Spletni brskalniki, APP.1.4 Mobilne aplikacije, APP.2.1 Imeniki storitev, APP.2.2 Imeniške domenske storitve Active Directory, APP.2.3 Imeniške storitve OpenLDAP, APP.3.1 Spletne informacijske storitve in spletne storitve, APP.3.2 Spletni strežnik, APP.3.3 Datotečni strežnik, APP.3.4 Samba, APP.3.6 DNS-strežnik, APP.4.2 SAP ERP-sistem, APP.4.3 Relacijski podatkovni sistemi, APP.4.4 Kubernetes, APP.4.6 SAP ABAP-programiranje, APP.5.2 Microsoft Exchange in Outlook, APP.5.3 Splošni e-poštni odjemalec in strežnik, APP.5.4 Enotne komunikacije in sodelovanje, APP.6 Splošna programska oprema, APP.7 Razvoj individualne programske opreme, SYS.1.1 Splošni strežnik, SYS.1.2.2 Windows Server 2012, SYS.1.2.3 Windows Server, SYS.1.3 Strežniki na Linux in Unix, SYS.1.5 Virtualizacija, SYS.1.6 Kontejnerizacija, SYS.1.7 IBM Z, SYS.1.8 Rešitve za shranjevanje, SYS.1.9 Terminalski strežniki, SYS.2.1 Splošni odjemalec, SYS.2.2.3 Odjemalci na Windows, SYS.2.3 Odjemalci na Linux in Unix, SYS.2.4 Odjemalci na macOS, SYS.2.5 Virtualizacija odjemalcev, SYS.2.6 Virtualna namizna infrastruktura, SYS.3.1 Prenosniki, SYS.3.2.1 Splošni pametni telefoni in tablice, SYS.3.2.2 Upravljanje mobilnih naprav (MDM), SYS.3.2.3 iOS (za podjetja), SYS.3.2.4 Android, SYS.3.3 Mobilni telefoni, SYS.4.1 Tiskalniki, kopirni stroji in večfunkcijske naprave, SYS.4.3 Vgrajeni sistemi, SYS.4.4 Splošna IoT-naprava, SYS.4.5 Zamenljivi nosilci podatkov, IND.1 Procesno vodenje in avtomatizacijska tehnologija, IND.2.1 Komponente industrijskih kontrolnih sistemov (angl. Industrial Control Systems, krat. ICS),

---

[106] Angl. Information Security Management System.

[107] Nem. BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS).

[108] Nem. BSI-Standard 200-2: IT-Grundschutz-Methodik.

[109] Nem BSI-Standard 200-3: Risikomanagement

[110] Nem. BSI-Standard 200-4 Business Continuity Management.

[111] Nem. IT-Grundschutz-Kompendium.

[112] Nem. Elementare Gefährdungen.

IND.2.2 Programabilni logični krmilnik (PLC), IND.2.3 Senzorji in aktuatorji, IND.2.4 Stroji, IND.2.7 Sistemi z varnostnimi instrumenti, IND.3.2 Oddaljeno vzdrževanje v industrijskem okolju, NET.1.1 Mrežna arhitektura in zasnova, NET.1.2 Upravljanje omrežij, NET.2.1 Delovanje WLAN, NET.2.2 Uporaba WLAN, NET.3.1 Usmerjevalniki in stikala, NET.3.2 Požarni zid, NET.3.3 VPN, NET.3.4 Nadzor dostopa do omrežja, NET.4.1 Telekomunikacijski sistemi, NET.4.2 VoIP, NET.4.3 Faksi in faks strežniki, INF.1 Zgradbe, INF.2 Podatkovni center in strežniška soba, INF.5 Soba ali omara za tehnično infrastrukturo, INF.6 Arhiviranje nosilcev podatkov, INF.7 Pisarniško delovno mesto, INF.8 Domače delovno mesto, INF.9 Mobilno delovno mesto, INF.10 Soba za sestanke, dogodke in usposabljanje, INF.11 Splošno vozilo, INF.12 Ožičenje, INF.13 Upravljanje tehnične zgradbe in INF.14 Avtomatizacija stavb.

Vsak gradnik osnovnega varovanja vključuje podrobne opise:

- pomena posameznega procesa oziroma gradnika osnovnega varovanja pri izvajanju informacijske podpore organizacije,
- ciljev, ki jih organizacija doseže z uvedbo ustreznih notranjih kontrol v okviru tega procesa,
- obsega in omejitev procesa,
- groženj in tveganj, povezanih s procesom,
- natančnih zahtev za osnovne notranje kontrole, ki jih mora proces nujno vključevati,
- natančnih zahtev za standardne notranje kontrole, ki naj bi jih proces vključeval ob upoštevanju uporabljenih tehnoloških rešitev v organizaciji, ter
- natančnih predlogov za notranje kontrole v primerih, kjer je proces potrebno dodatno zaščititi.

Zahteve za notranje kontrole vključujejo tudi sodila, namenjena poslovodstvu za ugotavljanje, ali so naloge in cilji procesa uresničeni. V nekaterih primerih so sodila zasnovana kot obstoj/neobstoj notranje kontrole, v drugih primerih pa Zbirka znanja o osnovnem varovanju informacijskih tehnologij vključuje tudi ključne indikatorje učinkovitosti kontrole. Čeprav so slovenske organizacije v primerjavi z nemškimi in ameriškimi praviloma manjše in morajo v praksi številna tveganja obravnavati s prilagojenimi notranjimi kontrolami, lahko po moji oceni poslovodstva pri vzpostavitvi sodil vsaj deloma izhajajo iz gradnikov osnovnega varovanja v zbirki znanja. Iz tako opredeljenih sodil lahko izhajajo tudi notranjerevizijski poslo. Okvir BSI je poleg tega pregledno izhodišče pri pripravi notranjerevizijskih delovnih programov in drugih gradiv s področja informacijske varnosti, med drugim tudi za posle na področjih skladnosti z zahtevami osnutka ZInfV-1, direktive NIS 2 in kibernetske odpornosti.

3.3 Cilji svetovalnega posla

Cilj svetovalnega posla je svetovati glede izboljšav upravljanja, obvladovanja tveganj in notranjih kontrol na področjih skladnosti z zahtevami osnutka ZInfV-1, direktive NIS 2 in širše kibernetske odpornosti. Ker mora funkcija notranje revizije, kjer je to smiselno, presoditi tudi, ali upravljanje informacijske tehnologije v organizaciji podpira strategije in cilje organizacije, je cilj svetovalnega posla prepoznati in izpostaviti priložnosti za izboljšanje obvladovanja tveganj in notranjih kontrol pri preprečevanju kibernetskih napadov, odzivanju nanje ter pri drugih vidikih vzpostavljanja robustne kibernetske odpornosti.

3.4 Obseg svetovalnega posla

3.4.1 Naloge, ki jih obsega svetovalni posel

Svetovalni posel zajema prepoznavanje, analizo, ocenjevanje in dokumentiranje informacij, razdeljenih v štiri sklope. Prvi vključuje identifikacijo tveganj neskladnosti z osnutkom ZInfV-1 in direktivo NIS 2 ter tveganj na področju kibernetske odpornosti, kjer se poleg začetne ocene splošnih tveganj področja, upoštevajo dejavniki, kot so panoga, velikost organizacije, geopolitične razmere in informacijsko okolje. Drugi sklop obsega analizo obstoječih notranjih kontrol in varnostnih mehanizmov, njihovo učinkovitost ter ozaveščenost zaposlenih. Tretji sklop vključuje vrednotenje tveganj z uporabo metod za razvrstitev tveganj po vplivu in verjetnosti ter pripravo priporočil za izboljšanje notranjih kontrol in skladnosti. Četrti sklop se osredotoča na sistematično dokumentiranje in strukturirano poročanje, kar zagotavlja preglednost, sledljivost ter jasen prikaz ključnih ugotovitev in predlaganih izboljšav.

3.4.2 Obseg v svetovalni posel vključenih elementov informacijskega okolja

Opredelitev obsega notranjerevizijskega posla na področju informacijskih tehnologij zahteva posebno pozornost glede na informacijsko okolje organizacije. Organizacije uporabljajo raznovrstne informacijske tehnologije, katerih tveganja zahtevajo specifične notranje kontrole. Za potrebe načrtovanja lahko informacijske tehnologije organizacije primeroma[113] razvrstimo v naslednje skupine:

- poslovne informacijske rešitve, s katerimi organizacija podpira svoje poslovanje,
- informacijske rešitve, ki omogočajo delovanje poslovnih informacijskih rešitev, kamor sodijo na primer orodja za upravljanje zbirk podatkov,
- strojno oprema in drugo infrastrukturo,
- elemente hibridnega procesnega okolja, predvsem najete zmogljivosti in informacijske rešitve v oblaku,
- rešitve za upravljane strojne opreme, torej operacijski sistemi, orodja za virtualizacijo in konteinerizacijo[114], platforma kubernetes[115] in druge,
- podporne informacijske rešitve, s katerimi organizacija organizira in varuje svoje informacijske tehnologije, kamor sodijo med drugim:
    - imeniške rešitve, ki omogočajo organizacijo informacijskih tehnologij in drugih virov, na primer rešitve Aktivnega direktorija,[116] OpenLDAP rešitve,[117] in SAMBA,[118]
    - informacijske rešitve za nadzor dostopa, avtorizacijo in avtentičnost uporabnikov, kot so sistemi za enotno prijavo (angl. Single Sign-On, krat. SSO), sistemi za večfaktorsko avtentikacijo (angl. Multi-Factor Authentication, krat. MFA) ter rešitve za upravljanje identitete in dostopa (angl. Identity and Access Management, krat. IAM),
    - datotečni strežniki,
    - informacijske rešitve za šifriranje in varno posredovanje podatkov,
    - navidezna zasebna omrežja,
    - informacijske rešitve za izvajanje varnostnih kopij,
    - informacijske rešitve za uničevanje podatkov iz elektronskih nosilcev,
    - protivirusne informacijske rešitve,
    - sistemi za zaznavanje in preprečevanje vdorov ,
    - informacijske rešitve za upravljanje varnostnih dogodkov,
- operativne tehnologije, ki jih organizacija uporablja za upravljanje naprav, s katerimi izvaja svoje storitve ali drugače podpira svoje delo,
- spletne informacijske rešitve in spletne strani, s katerimi organizacija ponuja storitve,
- sisteme za poslovno analitiko (angl. Business Intelligence, krat. BI), ki zagotavljajo analizo in vizualizacijo podatkov,
- platforme za izvajanje mobilnih storitev za stranke,
- pametne naprave, njihovi operacijski sistemi in njihove informacijske rešitve,
- komunikacijske informacijske tehnologije, kamor sodi strojna in programska oprema, s katero organizacije upravljajo svoja notranja omrežja in se povezujejo v zunanja omrežja,

---

[113] Mogoče to tudi različne druge delitve informaicjskih tehnologij v organizaciji.

[114] Kontejnerizacija je proces zgostitve informacijske rešitve skupaj z vsemi njenimi odvisnostmi (knjižnice, konfiguracije, orodja) v kontejner, ki je lahka in izolirana enota. S tem pristopom se zagotovi, da rešitev deluje enako ne glede na okolje, v katerem je nameščena.

[115] Platforma za upravljanje (orkestracijo) kontejnerjev z informacijskimi rešitvami,

[116] Active Directory je Microsoftova informacijska rešitev ki omogoča centralizirano upravljanje uporabnikov, računalnikov in omrežnih virov ter zagotavlja avtentikacijo in avtorizacijo dostopa v omrežjih z operacijskim sistemom Windows.

[117] OpenLDAP je odprtokodna rešitev za katalogizacijo in upravljanje uporabniških podatkov ter avtentikacijskih informacij, ki uporablja odprti lahko protokol za dostop do imenikov (angl. Lightweight Directory Access Protocol, krat. LDAP) za dostop in organizacijo teh podatkov v omrežjih.

[118] Samba je protokol, ki omogoča deljenje datotek in tiskalnikov med različnimi operacijskimi sistemi, kot sta Linux in Windows, v omrežju.

- nadzorne informacijske sisteme, preko katerih se izvaja upravljanje in nadzor delovanja omrežij in informacijskih sistemov, vključno z zaznavanjem in odzivanjem na varnostne dogodke, anomalije in grožnje,[119]
- krmilne informacijske sisteme, ki omogočajo nadzor, regulacijo, avtomatizacijo ali optimizacijo delovanja industrijskih, tehnoloških ali infrastrukturnih procesov,[119]
- naprave in informacijske rešitve, ki povezujejo fizične naprave z zunanjimi ormežji (angl. Internet of Things, krat. IoT),
- Informacijske rešitve za upravljanje načrtov neprekinjenega poslovanja (angl. Business Continuity Planning, krat. BCP) in za odzivanje na nesreče (angl. Disaster Recovery Planning, krat. DRP), ki vključujejo redundančne sisteme in avtomatske varnostne kopije.

Poleg informacijskih tehnologij vključuje informacijsko okolje organizacije tudi pravilnike, postopke, politike, organizacijske strukture in, nenazadnje, tudi zaposlene.

Pri načrtovanju kateregakoli notranjerevizijskega posla, ki vključuje elemente informacijskega okolja, je nujno natančno opredeliti, katere elemente bo posel zajel, saj lahko v primeru nejasno določenega obsega pride do nenadzorovanega širjenja posla (povezava s točko 3.4.4).

Kadar funkcija notranje revizije izvaja svetovalni posel brez posebnih strokovnih znanj s področja revidiranja informacijskih sistemov, je smiselno posel zasnovati na najvišji vsebinski ravni. Takšen posel lahko zajema prepoznavanje, analizo, ocenjevanje in dokumentiranje informacij o ključnih informacijskih tehnologijah organizacije. Vključuje pregled upravljanja teh tehnologij, oceno tveganj neskladnosti z zahtevami osnutka ZInfV-1 in direktive NIS 2, analizo tveganj na področju kibernetske varnosti ter pregled informacijskih rešitev in drugih tehnologij, ki organizaciji omogočajo učinkovito obvladovanje teh tveganj. Prav tako lahko obsega preučitev obstoječih notranjih kontrol in organizacijskih ukrepov, katerih namen je obvladovanje tveganj ter krepitev skladnosti in kibernetske odpornosti.

Tako zasnovan svetovalni posel se lahko omeji tako, da ne vključuje podrobnega pregleda obvladovanja tveganj in notranjih kontrol, ki so vgrajene v informacijske tehnologije organizacije. Takšen pregled pogosto presega okvir predlaganega posla in zahteva obsežnejši pristop, ki lahko predstavlja ločen notranjerevizijski posel.

Delovna programa svetovalnega posla (povezava s točko 3.9) smo pripravili ob predpostavki, da bo posel izveden na najvišji vsebinski ravni, brez vključitve podrobnega pregleda informacijskih tehnologij organizacije. Ta pristop omogoča osredotočenost na strateške in organizacijske vidike ter kibernetsko odpornost, skladno s cilji predlaganega posla.

Delavna programa svetovalnega posla (povezava s točko 3.9) posla smo pripravili ob predpostavki, da ga izvajamo na na najvišji vsebinski ravni, brez vključitve podrobnega pregleda informacijskih tehnologij organizacije.

O obsegu posla in vseh omejitvah obsega je potrebno ustrezno poročati (povezava s točko 4).

3.4.3 Obdobje na katero se nanaša svetovalni posel

Pri svetovalnih poslih je nujno jasno opredeliti in razkriti obdobje, na katero se nanašajo izsledki, ter čas izvedbe posla. To zagotavlja preglednost in omogoča pravilno interpretacijo ugotovitev. O obeh obdobjih je treba ustrezno poročati.

Nekatere notranje kontrole za obvladovanje tveganj v informacijskem okolju organizacije so vgrajene v informacijske tehnologije. Njihova učinkovitost ni odvisna le od neposrednih nastavitev, temveč tudi od nastavitev povezanih informacijskih tehnologij, s katerimi so soodvisne. Zato je pri ocenjevanju teh kontrol ključno upoštevati širši kontekst informacijskega okolja in medsebojne povezave njegovih elementov. Učinkovitost takšnih kontrol je mogoče zanesljivo oceniti le za obdobje, v katerem je bilo njihovo delovanje dejansko preizkušeno.

[119] Opredelitev povzeta po 5. členu osnutka ZInfV-1.

Predlagani svetovalni posel se osredotoča na možne izboljšave obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfV-1 in direktive NIS 2. Smiselno je, da posel zajema pregled stanja v določenem presečnem obdobju. Priporočljivo je, da se posel omeji na kratko obdobje, na primer december 2024, kar omogoča jasen vpogled v stanje organizacije na določeni točki v času..

3.4.4 Druge omejitve in predpostavke svetovalnega posla

Ob oddaji zaključnega dela je osnutek ZInfV-1 v javni razpravi. Čeprav zaključno delo temelji na predpostavki, da gre za veljavno različico zakona, je pričakovati, da se bodo nekateri deli predlaganega predpisa do končnega sprejetja še spremenili.

3.5 Človeški in drugi viri za izvedbo svetovalnega posla

Predlagani svetovalni posel zahteva specifična znanja s področja informacijske tehnologije, kibernetske varnosti, upravljanja tveganj, skladnosti z zakonodajo ter notranjega revidiranja, pri čemer je ključna podpora poslovodstva, odgovornih za informacijsko okolje, pravnega področja in skladnost. Za uspešno izvedbo je potrebno zagotoviti ustrezne časovne in finančne vire, programska orodja za analizo in dokumentiranje ter po potrebi dodatna usposabljanja vključenih strokovnjakov. Ob omejitvah virov, kot so pomanjkanje specifičnih znanj ali razpoložljivosti zaposlenih, je smiselno predvideti vključitev zunanjih strokovnjakov ali omejiti obseg posla, pri čemer so redna komunikacija z deležniki, jasno časovno načrtovanje in učinkovito upravljanje virov ključni za dosego ciljev. Hkrati je pomembno glede na razpoložljiva znanja ustrezno omejiti obseg posla (povezava točko 3.4.2) in o tem ustrezno poročati (povezava s točko 4)).

3.6 Metode izvedbe svetovalnega posla

Notranjerevizijske posle, ki se osredotočajo na področje informacijskih tehnologij, je mogoče izvajati na različne načine, odvisno od ciljev posla in specifičnega informacijskega okolja organizacije. Metode za prepoznavanje, proučevanje, ovrednotenje in dokumentiranje informacij pri svetovalnih poslih lahko vključujejo:

- Razgovore in poizvedbe: Izvedba intervjujev s ključnimi deležniki, kot so odgovorne osebe za skladnost, informatiki, strokovnjaki za informacijsko varnost, vodje specifičnih področij organizacije, ki morajo delovati skladno z osnutkom ZInfV-1 in direktivo NIS 2, ter zunanji sodelavci na področju pravnega svetovanja in upravljanja incidentov.
- Pregled dokumentacije: Analiza dokumentacije, povezane z obvladovanjem kibernetskih tveganj, upravljanjem informacijske varnosti, upravljanjem incidentov, skladnostjo, poročanjem nadzornim institucijam in drugih relevantnih virov.
- Opazovanje aktivnosti: Opazovanje izvedbe določenih aktivnosti v organizaciji, na primer dnevnih pregledov varnostnih poročil iz informacijskih rešitev za spremljanje varnostnih dogodkov in odzivanja na incidente.
- Analiza skladnostne in varnostne dokumentacije: Preučevanje dokumentacije, ki se nanaša na skladnost in zagotavljanje informacijske ter kibernetske odpornosti.
- Pregled poročil nadzornih sistemov: Analiza poročil informacijskih rešitev, ki omogočajo zaznavanje in odzivanje na varnostne dogodke, anomalije in grožnje.
- Pregled arhitekture informacijskega okolja: Preverjanje uporabe zastarelih informacijskih rešitev ali prepoznavanje neustrezne pokritosti določenih aktivnosti z ustreznimi informacijskimi rešitvami.
- Pregled konfiguracij in delovanja: Podrobna analiza konfiguracij in delovanja elementov informacijskega okolja, ki so ključni za skladnost z osnutkom ZInfV-1 in direktivo NIS 2 ter za učinkovito obvladovanje tveganj na področju kibernetske odpornosti.

Z uporabo teh metod se zagotovi strukturiran in celovit pregled informacijskega okolja ter podlaga za oblikovanje priporočil, ki prispevajo k skladnosti in krepitvi kibernetske odpornosti organizacije.

Ker je predlagani svetovalni posel zasnovan na najvišji možni vsebinski ravni in se osredotoča predvsem na upravljavsko-organizacijske kontrole (povezava s točko 3.4.2), predvidoma ne bo zajemal pregleda tehničnih konfiguracij ali podrobnega delovanja elementov informacijskega okolja organizacije.

3.7 Tveganja pri izvedbi svetovalnega posla in pristopi k njihovemu obvladovanju

Poleg tveganj, povezanih s predmetom in področjem, ki ga svetovalni posel obravnava, lahko v povezavi s tem konkretnim svetovalnim poslom opredelimo tudi nekaj tveganj, ki se nanašajo na samo izvedbo posla.

3.7.1 Povečevanja obsega posla

Področje, ki ga obravnavata osnutek ZInfV-1 in direktiva NIS 2, je zelo široko in zajema kompleksne vidike obvladovanja tveganj na področju kibernetske odpornosti. Obvladovanje teh tveganj je zahtevno, saj se kibernetske grožnje nenehno razvijajo in pojavljajo nove. Pri svetovalnih poslih, ki vključujejo elemente informacijskega okolja, se med izvajanjem pogosto pokaže potreba po vključitvi dodatnih elementov in procesov zaradi nepredvidenih odvisnosti znotraj informacijskega okolja. Vse navedeno lahko privede do povečanja obsega posla med njegovo izvedbo.

Za obvladovanje tveganja nenadzorovanega povečanja obsega svetovalnega posla je priporočljivo že na začetku jasno opredeliti in dokumentirati vse elemente informacijskega okolja, ki jih posel zajema, ter določiti meje pregleda (povezava s točko 3.4.2).

3.7.2 Pomanjkljiva podpora ali sodelovanje s strani ključnih oddelkov

Pomanjkanje podpore ali sodelovanja s ključnimi deležniki, kot so odgovorni za upravljanje informacijskega okolja, pravna služba, področje skladnosti in poslovodstvo, lahko omeji dostop do ključnih informacij ali povzroči zamude pri njihovem pridobivanju. Za obvladovanje tega tveganja je priporočljivo že v fazi načrtovanja svetovalnega posla natančno določiti obremenitve, ki jih bo posel predstavljal za ključne deležnike, ter jih o tem pravočasno obvestiti. Poleg tega je koristno vzpostaviti redno komunikacijo z deležniki in tako zagotoviti tekoče sodelovanje

3.7.3 Razpoložljivost strokovnega znanja za izvedbo svetovalnega posla

Omejitve pri razpoložljivosti strokovnega znanja za izvedbo svetovalnega posla lahko izhajajo iz pomanjkljivega poznavanja informacijskega okolja organizacije in njegovih elementov, kibernetske odpornosti, predpisov ter njihove praktične uporabe ali specifičnih znanj s področja notranjega revidiranja (povezava s točko 3.5).

3.8 Začetna ocena tveganj področja posla

Čeprav se morajo cilji svetovalnega posla nanašati na upravljanje, upravljanje tveganj in kontrolne postopke v dogovorjenem obsegu, je pri poslih, ki obravnavajo postopke obvladovanja tveganj, smiselno pripraviti začetno oceno tveganj. Pri svetovalnem poslu o možnih izboljšavah obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfV-1 in direktive NIS 2 je priporočljivo začetno oceno tveganj izvesti v dveh korakih: kot oceno tveganj neskladnosti z obema predpisoma in kot oceno tveganj na področju kibernetske odpornosti.

3.8.1 Neskladje z zahtevami osnutka ZInfv-1 in direktive NIS 2

Osnovno tveganje neskladij z osnutkom ZInfV-1 in direktive NIS 2 je povezano s kazenskimi določbami osnutka ZInfv-1, ki smo jih opisali v točkah2.6 in 2.7, torej tveganji da bo revidirani organizaciji zaradi neskladnosti z zahtevami predpisov naložena globa, da bo naložena globa njeni odgovorni osebi, da bo organizaciji v določenem obsegu omejeno poslovanje ali da bo omejeno opravljanje vodstvenih funkcij njenim poslovodnim osebam.

3.8.2 Tveganja na področju kibernetske odpornosti

Organizacije pa zakonodaje s področja varnosti omrežij in informacijskih sistemov ne smejo obravnavati le kot skupek administrativnih bremen. Grožnje na področju kibernetske odpornosti so prisotne v vsaki organizaciji in morajo predstavljati še posebej pomemben vidik obvladovanja tveganj v organizacijah, ki sodijo v skupini bistvenih ali pomembnih subjektov. V začetni oceni tveganj v okviru svetovalnega posla o učinkovitosti obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfv-1 in direktive NIS 2 je torej

potrebno upoštevati tako vidik tveganj neskladnosti s predpisi, kot tudi vidik tveganj s področja kibernetske odpornosti.

Konkretne grožnje na področju kibernetske odpornosti so specifične za vsako organizacijo in jih opredelimo v delovnem programu posla. Pri opredelitvi teh groženj in iz njih izhajajočih tveganj pa je v okviru načrtovanja notranjerevizijskega posla smiselno izhajati iz splošnih in znanih groženj na področju kibernetske odpornosti, ki jih nato med izvajanjem pregleda prilagodimo značilnostim revidirane organizacije in njenega informacijskega okolja. Splošne grožnje na področju kibernetske odpornosti bomo povzeli po dokumentu Zbirka znanja o osnovnem varovanju informacijskih tehnologij, zlasti po seznamu elementarnih groženj. Te grožnje vključujejo naslednje skupine groženj: G 0.1 Požar, G 0.2 Neugodne klimatske razmere, G 0.3 Voda, G 0.4 Onesnaževanje, prah, korozija, G 0.5 Naravne nesreče, G 0.6 Katastrofe v okolici, G 0.7 Veliki dogodki v okolici,[120] G 0.8 Izpad ali motnja v električnem omrežju, G 0.9 Izpad ali motnja v komunikacijskih omrežjih, G 0.10 Izpad ali motnja v oskrbovalnih omrežjih[121], G 0.11 Izpad ali motnja pri zunanjih izvajalcih storitev, G 0.12 Elektromagnetno motenje, G 0.13 Zajem kompromitirajočega sevanja, G 0.14 Vohunjenje za informacijami, G 0.15 Prisluškovanje, G 0.16 Kraja naprav, nosilcev podatkov ali dokumentov, G 0.17 Izguba naprav, nosilcev podatkov ali dokumentov, G 0.18 Slabo načrtovanje ali pomanjkanje prilagoditev[122], G 0.19 Razkritje zaščitenih informacij, G 0.20 Informacije ali izdelki iz nezanesljivega vira, G 0.21 Manipulacija strojne ali programske opreme, G 0.22 Manipulacija informacij, G 0.23 Nepooblaščen vdor v informacijske sisteme, G 0.24 Uničenje naprav ali nosilcev podatkov, G 0.25 Izpad naprav ali sistemov, G 0.26 Okvara naprav ali sistemov, G 0.27 Pomanjkanje virov, G 0.28 Programske ranljivosti ali napake, G 0.29 Kršitve zakonov ali predpisov, G 0.30 Neupravičena uporaba ali administracija naprav in sistemov, G 0.31 Nepravilna uporaba ali upravljanje naprav in sistemov, G 0.32 Zloraba pooblastil, G 0.33 Odsotnost osebja, G 0.34 Napad[123], G 0.35 Prisila, izsiljevanje ali korupcija, G 0.36 Kraja identitete, G 0.37 Zanikanje dejanj[124], G 0.38 Zloraba osebnih podatkov, G 0.39 Zlonamerna programska oprema, G 0.40 Preprečevanje storitev (angl. Denial of Service), G 0.41 Sabotaža, G 0.42 Socialni inženiring, G 0.43 Vnos sporočil, G 0.44 Nepooblaščen vdor v prostore, G 0.45 Izguba podatkov, G 0.46 Izguba integritete zaščitenih informacij in G 0.47 Škodljivi stranski učinki Iz informacijskimi tehnologijami podprtih napadov.

Za obvladovanje tveganj na področju kibernetske odpornosti in za skladnost z osnutkom ZInfV-1 in NIS 2 so po moji začetni oceni posebej pomembne elementarne grožnje, ki jih po Zbirki znanj o osnovnem varovanju informaicjskih tehnologij, povzemam v nadaljevanju. Ob vsaki grožnji izpostavljam tudi tveganja, ki jih opisana grožnja predstavlja ciljem, virom in delovanju organizacije.

3.8.2.1 G 0.9 Izpad ali motnja v komunikacijskih omrežjih

Organizacije, ki spadajo med bistvene ali pomembne subjekte, so praviloma močno odvisne od delujočih komunikacijskih povezav. Če te povezave dlje časa ne delujejo ali celo popolnoma odpovedo, lahko zastanejo ključni procesi, zaradi česar organizacija ne more več izvajati bistvenih ali pomembnih storitev.

3.8.2.2 G 0.11 Izpad ali motnja pri zunanjih izvajalcih storitev

Vzroki za izpade ali motnje pri storitvah, ki jih kupuje ali najema revidirana organizacija, so lahko tehnične težave na strani izvajalca storitev, lahko pa do izpadov prihaja tudi zaradi različnih organizacijskih razlogov, na primer

---

[120] V skladu z Zbirko znanja o osnovnem varovanju informacijskih tehnologij sem spadajo med drugim ulične prireditve, koncerti, športni dogodki, delovni spori ali demonstracije. Izgredi v povezavi s takšnimi dogodki lahko prinesejo dodatne posledice, kot so zastraševanje zaposlenih, pa vse do uporabe nasilja proti osebju ali stavbi.

[121] V skladu z Zbirko znanja o osnovnem varovanju informacijskih tehnologij sem spadajo električna, plinska, vodovodna in druga omrežja, ki so namenjena oskrbi zgradb, v katerih delujejo informacijske tehnologije.

[122] V skladu z Zbirko znanja o osnovnem varovanju informacijskih tehnologij nepravilni organizacijski postopki pri obdelavi informacij lahko povzročijo varnostne težave, tudi če so posamezni koraki pravilno izvedeni. Odvisnosti med procesi, ki niso očitno povezani z obdelavo informacij, so pogosto prezrte in lahko povzročijo motnje. Nejasne odgovornosti lahko privedejo do zamud, zanemarjanja varnostnih ukrepov in kršitev pravil. Tveganja nastanejo tudi, če so naprave, izdelki ali postopki nepravilno uporabljeni ali če obstajajo pomanjkljivosti v sistemski arhitekturi.

[123] V skladu z Zbirko znanja o osnovnem varovanju informacijskih tehnologij sem spadajo fizični napadi na zgradbe in zaposlene.

[124] Ljudje lahko iz različnih razlogov zanikajo, da so storili določena dejanja, na primer zato, ker ta dejanja kršijo navodila, varnostne predpise ali celo zakone. Prav tako lahko zanikajo, da so prejeli obvestilo, na primer ker so pozabili na dogodek. Na področju informacijske varnosti se zato pogosto poudarja zavezujočnost, lastnost, ki naj bi zagotovila, da storjenih dejanj ni mogoče neupravičeno zanikati. V angleščini se za to uporablja izraz Non-Repudiation (nezanikljivost).

insolventnosti, odpovedi pogodbe, naravnih nesreč ali pomanjkanja osebja. Izpad ali motnja pri delovanju zunanjih izvajalcih storitev lahko pomembno vpliva na poslovno kontinuiteto organizacije, še posebej pri procesih, s katerimi organizacija izvaja bistvene ali pomembne storitve.

3.8.2.3 G 0.14 Vohunjenje za informacijami

V skladu z Zbirko znanja o osnovnem varovanju informacijskih tehnologij so z vohunjenjem mišljeni napadi, katerih cilj je zbiranje, analiziranje in priprava informacij o organizacijah, osebah, izdelkih ali drugih ciljnih objektih. Tako obdelane informacije se lahko uporabijo, na primer, za pridobitev konkurenčnih prednosti za drugo organizacijo, izsiljevanje oseb ali kopiranje izdelkov. Poleg številnih tehnično zapletenih napadov obstajajo pogosto tudi enostavnejše metode za pridobivanje dragocenih informacij, na primer z združevanjem podatkov iz več javno dostopnih virov, ki posamezno izgledajo neškodljivo, a v drugih kontekstih lahko predstavljajo tveganje.

3.8.2.4 G 0.16 Kraja naprav, nosilcev podatkov ali dokumentov in G 0.17 Izguba naprav, nosilcev podatkov ali dokumentov

Kraja naprav, nosilcev podatkov in dokumentov povzroča materialno škodo, v določenih primerih pa lahko vodi tudi do izgube zaupnih podatkov in omogoči izvedbo kibernetskega napada. Tudi izguba naprav, nosilcev podatkov in dokumentov lahko predstavlja varnostna tveganja, pri čemer pa v večini okoliščin ne predstavlja tveganja kibernetskega napada.

3.8.2.5 G 0.19 Razkritje zaščitenih informacij

Zaupni podatki in informacije smejo biti dostopni samo pooblaščenim osebam. Do razkritja lahko pride zaradi tehnične napake, nepazljivosti ali celo namernih dejanj. Napadalci lahko pridobijo dostop do zaupnih informacij na različne načine, na primer z dostopom do pomnilniških medijev v računalnikih (trdi diski), prenosnih ali izmenljivih pomnilniških medijev (USB-ključi, CD-ji ali DVD-ji), med prenosom podatkov po komunikacijskih kanalih ali v nekaterih primerih celo v tiskani obliki na papirju. Metode, ki jih pri tem uporabljajo, vključujejo različne oblike socialnega inženiringa, okužbo informacijskih sistemov s škodljivo kodo, vohunjenje, krajo naprav, nosilcev podatkov ali dokumentov in druge tehnike.

3.8.2.6 G 0.20 Informacije ali izdelki iz nezanesljivega vira, G 0.21 Manipulacija strojne ali programske opreme in G 0.41 Sabotaža

Če organizacije uporabljajo informacije, programsko opremo ali naprave iz nezanesljivih virov, ali če izvor in pravilnost teh virov niso ustrezno preverjeni, lahko ti postanejo vstopna točka za kibernetske napade. Nepreverjene informacijske rešitve in naprave so med drugim povezane z grožnjo manipulacije, ki jo Zbirka znanja o varovanju informacijskih tehnologij opredeljuje kot namerne, a prikrite posege z namenom neopaženega spreminjanja programske ali strojne opreme. Nepreverjena programska oprema, zlasti različne odprtokodne rešitve, ki so brezplačno dostopne na svetovnem spletu, lahko vsebujejo namerno vgrajene varnostne ranljivosti. Prav tako lahko strojna oprema, razvita in izdelana v državah z močnimi paradržavnimi hekerskimi skupinami, vsebuje skrite dostopne točke, ki omogočajo dolgotrajno prikrito zbiranje informacij, vohunjenje in sabotažo – namerno manipulacijo ali poškodovanje stvari ali procesov z namenom povzročiti škodo. Podatkovni centri ali komunikacijske povezave vladnih organov ali organizacij so posebej privlačne tarče, saj lahko z razmeroma majhnimi sredstvi dosežemo velik učinek.

Nepreverjene informacije in izdelki iz nezanesljivih virov poleg tega, da predstavljajo vstopno točko za kibernetski kriminal, lahko povzročijo tudi težave v operativnem poslovanju. Posledica tega je lahko, da poslovno pomembne informacije temeljijo na napačnih podatkih, izračuni pa dajejo nepravilne rezultate ipd.

3.8.2.7 G 0.23 Nepooblaščen vdor v informacijske sisteme

Vsak element informacijskega okolja lahko v določenih okoliščinah predstavlja možnost nepooblaščenega dostopa in uporabe. Ta elementarna grožnja je povezana s številnimi drugimi elementarnimi grožnjami, saj je nepooblaščeni dostop pogost vstopni vektor za kibernetske napade.

3.8.2.8 G 0.27 Pomanjkanje virov in G 0.40 Preprečevanje storitev

Zahteve osnutka ZInfV-1 in direktive NIS 2 bodo za bistvene in pomembne subjekte zahtevale znatne kadrovske vire, kar zaradi splošnega pomanjkanja strokovnjakov na področju obvladovanja tveganj na področju kibernetske odpornosti predstavlja pomembno temeljno grožnjo.

Pomanjkanje virov se lahko pojavi tudi v drugih oblikah, kot na primer pomanjkanje procesnih virov pri obdelavi ali pomanjkanje komunikacijskih zmogljivosti. Obstaja več vrst napadov, ki z obremenjevanjem virov poskušajo preprečiti uporabo storitev, funkcij ali naprav. Ti napadi se imenujejo "onemogočanje storitev" (angleško: "Denial of Service" ali DoS). Primeri DoS-napadov vključujejo motnje poslovnih procesov (npr. z napačnimi naročili), blokiranje infrastrukture (npr. zaprtje komunikacijskih kanalov) in preobremenitev komponent informacijskih sistemov (npr. strežnikov). Ti napadi izčrpajo vire, kot so procesor, pomnilnik, diskovni prostor ali prenosne zmogljivosti, zaradi česar ti viri niso več dostopni dejanskim uporabnikom.

Pomanjkanje kadrovskih, časovnih, finančnih, tehničnih ali drugih virov je v rednem poslovanju pogosto še obvladljivo za omejeno obdobje, vendar se te pomanjkljivosti pod velikim časovnim pritiskom, na primer v izrednih situacijah, še bolj izrazito pokažejo.

3.8.2.9 G 0.28 Programske ranljivosti ali napake

Bolj kot je določena informacijska rešitev kompleksna, pogosteje se pojavijo napake. Te pogosto niso odkrite kljub intenzivnemu in obsežnemu testiranju. Neodkrite ranljivosti informacijskih rešitev lahko predstavljajo vstopni vektor za kibernetske napade in imajo zato na temnem spletu visoko ceno. Napake v informacijskih rešitvah so povezane tudi z drugimi tveganji, kot so težave pri delovanju informacijskih rešitev, napačni izračuni in podobno.

3.8.2.10 G 0.30 Neupravičena uporaba ali administracija naprav in sistemov

Nepooblaščeni uporabniki, na primer kibernetski napadalci, lahko z nepooblaščeno uporabo naprav in sistemov pridobijo dostop do zaupnih informacij, izvedejo manipulacije ali povzročijo motnje v delovanju. Posebej pomemben primer nepooblaščene uporabe je nepooblaščena administracija. Če kibernetski napadalci z nepooblaščeno uporabo administratorskih in drugih računov z močnimi pravicami spremenijo konfiguracije informaicjskih rešitev ali operativne parametre strojnih ali programskih komponent, lahko to povzroči resno škodo.

3.8.2.11 G 0.31 Napačna uporaba ali administracija naprav in sistemov

Napake pri namestitvi, konfiguraciji, vzdrževanju in upravljanju strojnih ali programskih komponent lahko omogočijo kibernetske napade in povzročijo resno škodo. Primeri napak v konfiguraciji strojnih in programskih komponent, ki lahko prispevajo k uspešnim kibernetskim napadom, vključujejo preveč široka uporabniška dovoljenja, enostavno uganljiva gesla, prenašanje podatkov v nešifrirani obliki in druge napake.

3.8.2.12 G 0.32 Zloraba pravic

Zloraba pravic se zgodi, ko se namerno, zakonito ali nezakonito pridobljene uporabniške pravice uporabljajo izven predvidenega okvira. Cilj tega je pogosto pridobiti osebno korist ali škodovati instituciji ali določenim osebam, zloraba pravic pa je lahko tudi del kibernetskega napada.

3.8.2.13 G 0.35 Prisila, izsiljevanje ali korupcija

Z grožnjo nasilja ali drugih negativnih posledic lahko kibernetski napadalci poskušajo zaposlene prisiliti, da kršijo varnostne politike ali zaobidejo varnostne ukrepe ter tako služijo kot vstopni vektor v informacijska okolje organizacije. Namesto groženj lahko napadalci zaposlenim ponujajo tudi denar ali druge ugodnosti. Ti napadi so praviloma usmerjeni proti visokim vodstvenim kadrom ali osebam na položajih posebnega zaupanja, na primer administratorjem informacijskih sistemov.

3.8.2.14 G 0.39 Zlonamerna programska oprema

Zlonamerna programska oprema je namenjena izvajanju nezaželenih in škodljivih funkcij. Primeri zlonamerne programske opreme so virusi, črvi in trojanski konji. Takšna programska oprema deluje prikrito, brez vednosti

administratorjev in uporabnikov, ter lahko napadalcem omogoči šifriranje uporabniških podatkov, pridobivanje gesel, nadzor sistemov na daljavo, onemogočanje varnostnih programov in vohunjenje za podatki ali celo njihovo krajo. Posledice zlonamerne programske kode so lahko onemogočanje delovanja informacijskih sistemov napadenih organizacij, kar omejuje njihovo poslovanje, nepooblaščeno spreminjanje ali kraja podatkov, okužbe strank in poslovnih partnerjev ter druge resne posledice.

3.8.2.15 G 0.42 Socialni inženiring

Socialni inženiring je pristop, s katerim napadalci prek manipulacije ljudi pridobijo nepooblaščen dostop do informacij ali informaicjskih sistemov. Včasih napadalci vzpostavijo daljši stik z žrtvijo, da pridobijo zaupanje in kasneje dostop. Takšni napadi so lahko večstopenjski, kjer napadalec postopoma uporablja pridobljene informacije za nadaljnje manipulacije.

3.8.2.16 G 0.43 Vnos sporočil

Pri vnosu poročil re za obliko napada, kjer napadalci pošiljajo posebej pripravljena sporočila sistemom ali osebam z namenom, da pridobijo korist zase ali povzročijo škodo žrtvi. Za ustrezno oblikovanje sporočil napadalci uporabljajo na primer opise vmesnikov, specifikacije protokolov ali zapise o preteklem komunikacijskem vedenju.

3.8.2.17 G 0.47 Škodljivi stranski učinki Iz informacijskimi tehnologijami podprtih napadov

Kibernetski napadi lahko povzročijo nepredvidene posledice, ki ne vplivajo neposredno na ciljne objekte, ki so bili napadeni ali ki škodijo neudeleženi tretji osebi. Vzrok za to sta visoka kompleksnost in povezanost sodobnih informacijskih tehnologij ter dejstvo, da so soodvisnosti napadenih ciljnih objektov in pripadajočih procesov lahko nedokumentirane ali celo povsem neznane. Zato lahko pride do napačne ocene dejanske potrebe po zaščiti različnih komponent informacijskih tehnologij ali celo do tega, da odgovorni za posamezne komponente nimajo interesa za odpravo njihovih pomanjkljivosti.

3.9 Delovni program svetovalnega posla

Delovni program svetovalnega posla je zasnovan na predpostavki, da bo posel izveden na najvišji vsebinski ravni, brez podrobnega pregleda informacijskih tehnologij organizacije (povezava s točko 3.4.2). Takšen pristop omogoča osredotočenost na strateške in organizacijske vidike ter krepitev kibernetske odpornosti, skladno s cilji predlaganega posla.

V izvedbenem delu svetovalnega posla je smiselno postopke za prepoznavanje, proučitev, ovrednotenje in dokumentiranje informacij organizirati tako, da zagotovijo kar največjo učinkovitost in hkrati čim manj obremenjujejo revidirane organizacijske funkcije. Postopki se lahko razvrstijo po vsebinskih sklopih, pregledovanih informacijskih tehnologijah ali drugih smiselnih kriterijih, ki olajšajo delo notranjega revizorja. Metode izvedbe svetovalnega posla so opisane v točki 3.6, v nadaljevanju pa so vključeni vsebinski vprašalniki, ki služijo kot podlaga za spoznavanje področja ter odločitev o izbiri konkretnih metod dela.

Ker predlagani svetovalni posel zajema tako skladnost z zahtevami osnutka ZInfV-1 in direktive NIS 2 kot tudi obvladovanje tveganj na področju kibernetske odpornosti, je smiselno pripraviti dva ločena vprašalnika, enega za področje skladnosti s predpisoma in enega s področja splošnega pristopa h kibernetski odpornosti. Tako zbrane informacije bodo omogočile strukturirano in ciljno usmerjeno izvedbo posla, skladno z metodami iz točke 3.6.

3.9.1 Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje neskladij z osnutkom ZInfV-1 in NIS 2

Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje neskladij z osnutkom ZInfV-1 in direktivo NIS 2 je zasnovan tako, da naslavlja ključne zahteve obeh predpisov in se povezuje z njihovimi vsebinskimi povzetki, predstavljenimi v točki 2.3. Namen vprašalnika je prevesti zahteve obeh predpisov v jasna, pregledna in praktično uporabna vprašanja, ki omogočajo učinkovito prepoznavanje morebitnih neskladij ter podajo temelja za oceno in izboljšanje skladnosti organizacije.

Tabela 1: Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje neskladij z osnutkom ZInfV-1 in direktivo NIS 2

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.3.1 Upravljanje in izobraževanje	Za področje kibernetske odpornosti je izrecno odgovorno poslovodstvo, ki se mora redno izobraževati in zagotoviti izobraževanje tudi skrbnikom ključnih IKT in vsem drugim zaposlenim.	Ali ima organizacija ažurno krovno varnostno politiko, ki jo je potrdilo poslovodstvo? Je poslovodstvo v krovni varnostni politiki in drugih dokumentih izrecno navedeno kot odgovorno za področje kibernetske odpornosti? Ali izvršno poslovodstvo o področju kibernetske odpornosti periodično nadzornemu svetu? Kako pogosto se poslovodstvo in zaposleni udeležujejo usposabljanj na temo kibernetske odpornosti, in kako se zagotavlja, da so ti programi skladni z zahtevami URSIV? Kakšni so postopki za spremljanje in evidentiranje usposobljenosti skrbnikov informacijskih sistemov glede kibernetske odpornosti? Kako organizacija preverja učinkovitost in ažurnost programov usposabljanja za področje kibernetske odpornosti?
2.3.2 Samoregistracija	Zavezanec se mora registrirati preko mehanizma za samoregistracijo URSIV in zagotoviti, da mu redno javljajo vse spremembe ključnih podatkov.	Ali je organizacija izvedla samoregistracijo pri URSIV? Ali je organizacija vzpostavila postopke za redno posodabljanje podatkov?

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.3.3 Varnostna dokumentacija	Zavezanec mora pripraviti in redno vzdrževati dokumentacijo področja informacijske varnosti.	Ali ima organizacija popisano svoje informacijsko okolje[125] in ali s tem popisom razpolaga tudi funkcija notranje revizije? Kako organizacija redno ocenjuje tveganja na področju kibernetske odpornosti in kako se prilagajajo varnostne politike glede na ugotovitve ocene tveganj? Ali organizacija vodi register tveganj in ali so med tveganji, ki jih spremlja, tudi tveganja na področju kibernetske odpornosti? Kako in organizacija določa sprejemljivo raven tveganj? Kako metodologijo za to uporablja? Ali je organizacija izvedla analizo poslovnih učinkov[126] in ali jo redno posodablja? Ali je organizacija vzpostavila in popisala postopke za zagotavljanje neprekinjenega poslovanja in ali ti predvidevajo tudi ravnanja v primeru večjih incidentov na področju kibernetske odpornosti? So v popisanih postopkih jasno določeni nosilci odgovornosti za izvedbo posameznih nalog , predvsem vloge in odgovornosti za obnovitev delovanja omrežnih in informacijskih sistemov po prekinitvah? Ali je organizacija vzpostavila in popisala postopke postopke za okrevanje po večjem škodnem dogodku in ali ti predvidevajo tudi ravnanja v primeru večjih incidentov na področju kibernetske odpornosti? So v popisanih postopkih jasno določeni nosilci odgovornosti za izvedbo posameznih nalog? Ali ima organizacija popisane protokole za varnostno kopiranje podatkov? Ali ima organizacija načrt odzivanja na incidente vključno z opisom sistema za zaznavo in odzivanje na incidente ter opisom vlog in odgovornosti za odzivanje na incidente? Ali načrt vključuje protokol obveščanja pristojnega CSIRT v obliki in v rokih, ki jih določa ZInfV-1? Ali ima organizacija svojim okoliščinam in svojemu informacijskemu okolju prilagojen (ne generičen) načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost? Ali organizacija spremlja in analizira učinkovitost svojih varnostnih ukrepov, in katere kazalnike učinkovitosti uporablja pri tem? Kako pogosto organizacija posodablja ključne dokumente s področja informacijske varnosti? Ali pri tem uporablja ustrezno verzioniranje in ali so spremembe potrjene na ustrezni ravni upravljanja v organizaciji? Kaka je delitev odgovornosti za načrtovanje in izvedbo varnostnih ukrepov med poslovodnimi in izvršnimi funkcijami v organizaciji?

[125] Najmanjši obseg popisa informacijskega okolja se nahaja v točki 3.4.2 Obseg v svetovalni posel vključenih elementov informacijskega okolja.

[126] Analiza poslovnih učinkov (angl. Business Impact Analysis, krat. BIA) je proces, s katerim organizacija oceni, kako kritični poslovni procesi vplivajo na njeno delovanje v primeru motenj ali incidentov. Cilj je določiti, kateri procesi, sistemi, viri in podatki so bistveni za nemoteno poslovanje ter kako hitro jih je treba obnoviti po prekinitvi.

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.3.4 Ukrepi za obvladovanje tveganj za kibernetsko varnost	Zavezanec mora sprejeti ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov.	Ukrepe za obvladovanje tveganj za kibernetsko varnosti je mogoče natančneje preučiti s pomočjo vprašanj v točki 3.9.2 Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje . Splošna vprašanja, ki neposredno izhajajo iz zahtev osnutka ZInfV-1, so: Kako poslovodstvo podpira načelne in praktične izvršne funkcije pri zagotavljanju informacijske in kibernetske odpornosti? Kako je področje informacijske varnosti vključeno v letni načrt dela organizacije, in kako so opredeljene odgovornosti za izvajanje ukrepov na tem področju? Kateri postopki so, ob upoštevanju predpisov s področja delovnih razmerij, vzpostavljeni za preverjanje integritete kadrov pred zaposlitvijo, med zaposlitvijo in ob prenehanju delovnega razmerja? Kako organizacija zagotavlja, da vsi zaposleni upoštevajo osnovne prakse kibernetske higiene, in kakšni so programi usposabljanja na področju kibernetske odpornosti? Kateri so glavni ukrepi za zagotavljanje varnosti človeških virov, in kako organizacija upravlja dostope in pooblastila v informacijskem okolju? Ali organizacija uporablja večfaktorsko avtentikacijo (angl. Multi-Factor Authentication, krat. MFA) ali rešitve neprekinjene avtentikacije, in v katerih primerih so ti postopki obvezni? Ali organizacija uporablja avtomatizirane rešitve za nadzor in zaznavanje morebitnih nepooblaščenih dostopov, in kako so te rešitve vključene v politiko informacijske varnosti? Ali organizacija ohranja in sistematično spremlja ključne dnevniške zapise, ter kako se zagotavljata njihova avtentičnost in celovitost? Ali se dnevniški zapisi redno pregledujejo in analizirajo, da bi identificirali morebitne nepravilnosti ali varnostne grožnje, in kdo je zadolžen za ta proces? Katere politike in postopki so potrebni in vzpostavljeni v zvezi z uporabo kriptografije in šifriranja za zagotavljanje varnosti podatkov? Kako se na ta način ščitijo omrežni promet, strežniki, zbirke podatkov, prenosne naprave in izmenljivi mediji, varnostne kopije podatkov, uporabniška imena in gesla, podatki v informacijskih rešitvah in drugih oblačnih storitvah, v elektronski pošti in drugih poslovnih komunikacijah ter pri upravljanju dnevniških zapisov? Kako organizacija nadzoruje promet in komunikacije znotraj svojih informacijskih sistemov, in kdo je odgovoren za upravljanje tega nadzora? Ali ima organizacija vzpostavljene postopke odzivanja na incidente, vključno z opisom sistema za zaznavo in odzivanje na incidente ter opisom vlog in odgovornosti za odzivanje na incidente? Ali načrt vključuje protokol obveščanja pristojnega CSIRT v obliki in rokih, ki jih določa ZInfV-1? Kako pogosto se ti postopki testirajo?

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
		Ali je organizacija vzpostavila postopke za zagotavljanje neprekinjenega poslovanja in ali ti predvidevajo tudi ravnanja v primeru večjih incidentov na področju kibernetske odpornosti? Je jasno določila odgovornosti za izvedbo posameznih nalog , predvsem vloge in odgovornosti za obnovitev delovanja omrežnih in informacijskih sistemov po prekinitvah? Kako pogosto se testirajo načrti za zagotavljanje neprekinjenega poslovanja, vključno s pripravljenostjo na kibernetske napade, in ali so določeni jasni cilji uspešnosti teh testov? Ali je organizacija vzpostavila postopke za okrevanje po večjem škodnem dogodku in ali ti predvidevajo tudi ravnanja v primeru večjih incidentov na področju kibernetske odpornosti? So v popisanih postopkih jasno določeni nosilci odgovornosti za izvedbo posameznih nalog? Kakšne protokole ima organizacija vzpostavljene za varnostno kopiranje podatkov, in kako pogosto se izvajajo testi obnovite varnostnih kopij? Kako organizacija obvladuje varnost dobavne verige, in kako zagotavlja, da so dobavitelji skladni z njenimi varnostnimi zahtevami? Kako organizacija zagotavlja, da je skladna z varnostnimi zahtevami svojih ključnih dobaviteljev? Kateri so ključni ukrepi za fizično in tehnično varovanje prostorov, kjer se nahajajo ključni deli omrežnih in informacijskih sistemov? Kakšna zagotovila ima organizacija od ponudnikov oblačnih storitev glede fizičnega in tehničnega varovanja njihovih prostorov? Kakšna zagotovila ima organizacija, da se podatki nahajajo na strežnikih, ki se fizično nahajajo znotraj EU ali Slovenije (kjer je to predpisano)? Ali so v organizaciji opredeljeni varnostni mehanizmi za posamezne informacijske rešitve in druge elemente informacijskega okolja, in ali vključujejo postopke za spremljanje in obvladovanje oziroma sanacijo ranljivosti? Kako organizacija upravlja in preprečuje izrabo tehničnih ranljivosti v posameznih elementih njenega informacijskega okolja? Kako organizacija ravna, ko elementov informacijskega okolja, pri katerih so bile zaznane tehnične ranljivosti, ni mogoče posodobiti ali prenehati z njihovo uporabo?, Kateri so glavni ukrepi za zaščito pred zlonamerno programsko kodo? Kako je v organizaciji urejeno tehnično zaznavanje poskusov vdorov in kako se vsebinsko spremlja zaznavanje? Ali organizacija uporablja varne glasovne, video in besedilne komunikacije, kadar je to primerno, in kako se zagotavlja varnost teh sistemov za komunikacijo v sili? Kako pogosto organizacija preverja učinkovitost vzpostavljenih ukrepov za obvladovanje tveganj za kibernetsko varnost, in kdo je odgovoren za spremljanje skladnosti teh ukrepov? Kateri so postopki za hitro implementacijo korektivnih ukrepov v primeru ugotovljenih pomanjkljivosti pri obvladovanju kibernetskih tveganj?

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.3.5 Uporaba certificiranih proizvodov in postopkov	Zavezanec naj bi pri izboru tehnologij in postopkov za svoja informacijska okolja prednostno izbirali proizvode, storitve in postopke ter so jih razvili drugi zavezanci, ki morajo biti skladni z NIS 2 ali ki so bili kupljeni pri tretjih straneh in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost.	Kakšni so kriteriji za izbiro certificiranih proizvodov in storitev, ki jih organizacija uporablja za zagotavljanje skladnosti z ZInfV-1 in NIS 2? Kako organizacija preverja skladnost dobaviteljev IKT produktov s standardi, kot so NIS 2 in ENISA certifikacijske sheme? Ali organizacija uporablja kvalificirane storitve zaupanja, in če jih, na kakšen način so vključene v varnostne postopke, s katerimi obvladuje tveganja kibernetske odpornosti? Kako organizacija varuje digitalne certifikate, elektronske podpise, elektronske žige, časovne žige, elektronske varne poštne predale in potrdila za spletna mesta pred nepooblaščenim dostopom, kopiranjem ali spreminjanjem, ter ali uporablja nadzorne mehanizme za zaznavanje morebitnih nepravilnosti? Ali ima organizacija vzpostavljene postopke za obnovo, preklic ali zamenjavo elementov storitev zaupanja kadar pride do spremembe dostopnih pravic, izteka veljavnosti ali suma na zlorabo?
2.3.6 Standardizacija	Zavezanec naj bi v čim večji meri uporabljal evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov.	Kateri evropski ali mednarodni standardi za kibernetsko varnost se uporabljajo v organizaciji, in kako se zagotavlja njihovo izvajanje? Kakšen je proces za uskladitev praks varovanja osebnih podatkov v skladu z zahtevami področnih predpisov?
2.3.9 Obvezno priglašanje incidentov skupinam CSIRT	Pri določitvi pomembnosti incidenta se upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja po lestvici od C6 – varnostni dogodek, do C1 – kritični incident.	Katera metodologija za oceno pomembnosti incidentov se uporablja, in kako se ocenjuje skladnost z nacionalnim načrtom odzivanja? Kako organizacija dokumentira in spremlja vpliv varnostnih dogodkov glede na lestvico incidentov od C6 do C1?
2.3.8 Obvezno posredovanja podatkov in informacij	URSIV lahko od zavezancev kadarkoli pisno zahteva podatke in informacije, pri čemer pa mora biti njihov obseg sorazmeren namenu, za katerega bodo uporabljeni, URSIV pa mora namen zahteve tudi razkriti.	Kako organizacija zagotavlja pravočasnost posredovanja informacij URSIV v primeru zahteve za obvezno posredovanje podatkov in informacij? Kateri postopki so vzpostavljeni, da organizacija lahko hitro zbere natančne in popolne podatke?
2.3.9 Obvezno priglašanje incidentov skupinam CSIRT	Zavezanec mora pristojni skupini CSIRT brez odlašanja obvestiti o vseh incidentih, ki imajo pomemben vpliv na zagotavljanje njihovih storitev.	Kako organizacija zagotavlja pravočasnost posredovanja informacij URSIV v primeru pomembnega incidenta? Kateri postopki so vzpostavljeni, da organizacija lahko hitro zbere natančne in popolne podatke? Ali so ti postopki natančno popisani in redno posodabljani? Kako so ti postopki povezani s postopki obvladovanja incidentov?

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.3.10 Sodelovanje s pristojno skupino CSIRT in URSIV pri obvladovanju incidenta	Zavezanec mora pri obravnavi incidenta v natančno predpisanih rokih sodelovati s pristojno skupino CSIRT.	Kako organizacija zagotavlja pravočasnost sprotnega poročanja informacij URSIV v primeru pomembnega incidenta?? Ali so ti postopki natančno popisani in redno posodabljani? Kako so ti postopki povezani s postopki obvladovanja incidentov?
2.3.11 Pomoč na področju kibernetske obrambe	URSIV lahko, v primeru kibernetskih groženj in incidentov, na njihovo prošnjo ali na prošnjo pristojne skupine CSIRT, nudi zavezancem dodatno pomoč na področju kibernetske obrambe.	Kakšni so postopki za koordinacijo z URSIV in CSIRT pri obvladovanju varnostnih incidentov? Kako organizacija zagotavlja, da so povratne informacije pristojnih organov upoštevane in implementirane pri obvladovanju incidentov? Kdo je odgovoren za posredovanje dodatnih informacij CSIRT ali URSIV, če to zahtevajo v primeru incidenta?
2.3.12 Prostovoljno priglaševanje incidentov skupinam CSIRT	Zavezanec lahko skupinam CSIRT prostovoljno priglasi tudi manj kritične incidente	Kakšni so postopki za koordinacijo z URSIV in CSIRT pri obvladovanju varnostnih incidentov?
2.3.13 Obveščanje strank zavezancev in javnosti	Zavezanec naj o incidentih kadar je primerno, obvesti tudi stranke. Kadar bi jih pomembna kibernetska grožnja lahko prizadela, jim mora sporočiti vse ukrepe ali sredstva, ki jih lahko ti prejemniki sprejmejo v odziv na to grožnjo. . Kadar je to primerno URSIV ali sam zavezanec o grožnji obvestita tudi javnost.	Kateri so kriteriji za obveščanje strank ali javnosti o pomembnih incidentih, in kdo je odgovoren za to odločitev? Kako organizacija zagotavlja, da so stranke obveščene o potrebnih ukrepih za zaščito pred kibernetskimi grožnjami? Kakšen je postopek za posredovanje informacij javnosti o incidentih, kadar je to primerno?
2.3.14 Hramba dnevniških zapisov	Zavezanci morajo zagotoviti ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja, za obdobje šestih mesecev, lahko pa tudi za dlje	Kateri postopki so vzpostavljeni za zagotavljanje avtentičnosti, celovitosti in razpoložljivosti dnevniških zapisov? Kako organizacija zagotavlja, da so vsi ključni zapisi hranjeni na ozemlju Republike Slovenije ali v EU, kadar je to zahtevano? Kateri protokoli se uporabljajo za arhiviranje dnevniških zapisov, in kako pogosto se preverja skladnost s politiko hrambe?
2.4.1 Ocena skladnosti pri bistvenih subjektih / 2.4.2 Samoocena skladnosti pri pomembnih subjektih	Bistveni subjekti morajo vsaj vsaki dve leti ali po zahtevi inšpektorja ter ob pomembnih incidentih opraviti oceno skladnosti, katere rezultat je pisno poročilo o skladnosti, posredovano inšpektorju v osmih dneh po prejemu. Pomembni subjekti pa morajo vsaj vsaki dve leti izvesti samooceno skladnosti in, če ta pokaže skladnost z ZInfV-1, v osmih dneh posredovati inšpektorju izjavo o skladnosti.	Kako organizacija zagotavlja, da se ocena skladnosti za bistvene subjekte izvede vsaj vsaki dve leti ali ob pojavu pomembnih incidentov, in kdo je odgovoren za sprožitev tega postopka? Kakšen je postopek priprave in posredovanja pisnega poročila o skladnosti inšpektorju, in kako se zagotavlja pravočasnost ter točnost posredovanih informacij? Kako organizacija spremlja rezultate samoocene skladnosti za pomembne subjekte, in kateri so kriteriji za ugotovitev skladnosti z zahtevami ZInfV-1?

Povezava	Kratek povzetek zahteve	Primeri ključnih vprašanj
2.5 Nadzor	Inšpektorji za informacijsko varnost pri URSIV so odgovorni za nadzor nad izvajanjem ZInfV-1, kar vključuje pregled podatkov, dokumentacije in ključnih informacijskih sistemov zavezancev, izvajanje inšpekcijskih pregledov na kraju samem ali na daljavo, odrejanje revizij varnosti, izvajanje varnostnih pregledov in po potrebi odrejanje obvestil o kibernetskih grožnjah ter ukrepov za skladnost.	Kako organizacija zagotavlja, da so vsi podatki, dokumentacija in dostop do informacijskih sistemov pripravljeni za pregled s strani inšpektorjev za informacijsko varnost pri URSIV? Kakšni so postopki organizacije za pravočasno izvajanje in dokumentiranje priporočil, podanih po revizijah skladnosti ali varnostnih pregledih, ki jih odredi inšpektor? Kako organizacija spremlja in zagotavlja, da so ključne osebe usposobljene za sodelovanje pri inšpekcijskih pregledih ter za izpolnjevanje zahtevanih ukrepov v primeru pomembnih incidentov ali kršitev ZInfV-1?

3.9.2 Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje obvladovanja tveganj na področju kibernetske odpornosti

Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje obvladovanja tveganj na področju kibernetske odpornosti je zasnovan na okviru BSI (povezava s točko 3.2.1. Temelji na začetni oceni tveganj oziroma izpostavljenih groženj na področju kibernetske odpornosti (povezava s točko 3.8.2) ter vključuje primer ključnih vprašanj o tveganjih in kontrolah. Vprašanja so povezana z osnovnimi gradniki, ki vsebujejo podrobne opise pomena procesov, njihovih ciljev, obsega, omejitev, povezanih groženj in tveganj ter zahtev in predlogov za osnovne in standardne notranje kontrole, prilagojene uporabljenim tehnološkim rešitvam in potrebam po dodatni zaščiti procesov.

Tabela 2: Vprašalnik za prepoznavanje, proučitev, ovrednotenje in dokumentiranje obvladovanja tveganj na področju kibernetske odpornosti

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.1 G 0.9 Izpad ali motnja v komunikacijskih omrežjih	Dolgotrajni izpadi komunikacijskih omrežij lahko prekinejo ključne procese in preprečijo izvajanje bistvenih ali pomembnih storitev organizacije.	Kako organizacija zagotavlja redundanco in alternativne komunikacijske poti za ključne procese? Ali je organizacija jasno opredelila in preizkusila postopke ob izpadih omrežij?	NET.1.1 Mrežna arhitektura in zasnova NET.3.1 Usmerjevalniki in stikala OPS.1.1.1 Splošno delovanje informacijskih tehnologij

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.2 G 0.11 Izpad ali motnja pri zunanjih izvajalcih storitev	Izpad storitev zunanjih izvajalcev lahko resno vpliva na poslovno kontinuiteto, zlasti pri izvajanju bistvenih storitev.	Ali je organizacija pri poslovanju pomembno odvisna od zunanjih izvajalcev storitev? Kako organizacija ocenjuje in nadzoruje tveganja, povezana z zunanjimi izvajalci? Kakšne pogodbe je organizacija sklenila za zagotavljanje neprekinjenih storitev s strani zunanjih izvajalcev? Kako organizacija zagotavlja usklajevanje in obveščanje s ključnimi zunanjimi izvajalci v primeru izrednih dogodkov?	OPS.2.3 Uporaba zunanjih izvajalcev NET.4.1 Telekomunikacijski sistemi DER.4 Upravljanje v izrednih okoliščinah
3.8.2.3 G 0.14 Vohunjenje za informacijami	Vohunjenje za informacijami vključuje napade za zbiranje, analiziranje in pripravo podatkov o organizacijah ali posameznikih, ki se lahko uporabijo za pridobitev konkurenčne prednosti, izsiljevanje ali kopiranje izdelkov, pogosto pa vključuje tudi združevanje navidez neškodljivih javno dostopnih informacij.	Kako organizacija prepoznava in spremlja poskuse vohunjenja ter nepooblaščeno zbiranje podatkov? Ali organizacija uporablja varnostne rešitve za zaznavanje sumljivih komunikacij in vohunjenja? Kako organizacija usposablja zaposlene za prepoznavanje tveganj vohunjenja in zaščito občutljivih informacij? Ali je organizacija izvedla preizkuse, ki posnemajo socialni inženiring?	ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost NET.3.4 Nadzor dostopa do omrežja DER.1 Zaznavanje varnostno pomembnih dogodkov
3.8.2.4 G 0.16 Kraja naprav, nosilcev podatkov ali dokumentov in G 0.17 Izguba naprav, nosilcev podatkov ali dokumentov	Kraja ali izguba lahko povzroči materialno škodo in izpostavi zaupne podatke, kar omogoča kibernetske napade.	Kakšne ukrepe je organizacija vzpostavila za fizično varovanje naprav in podatkovnih nosilcev? Kako je vzpostavila postopke javljanja njihove morebitne izgube ali kraje? Kako organizacija zagotavlja šifriranje in zaščito podatkov na napravah v primeru izgube ali kraje?	CON.1 Kriptokoncept CON.6 Brisanje in uničenje INF.2 Podatkovni center in strežniška soba
3.8.2.5 G 0.19 Razkritje zaščitenih informacij	Zaupni podatki so lahko izpostavljeni razkritju zaradi tehničnih napak, nepazljivosti ali namernih dejanj, pri čemer napadalci uporabljajo metode, kot so socialni inženiring, okužba s škodljivo kodo, vohunjenje ter kraja naprav ali dokumentov, da pridobijo dostop do teh informacij.	Kakšne politike in postopke je organizacija vzpostavila glede dostopa in avtorizacije do občutljivih informacij? Kako organizacija zagotavlja šifriranje in druge oblike zaščite za občutljive podatke med prenosom? Kako pogosto organizacija izvaja preglede nadzora nad dostopom do zaupnih podatkov?	ORP.4 Upravljanje identitet in pravic CON.1 Kriptokoncept OPS.1.1.5 Beleženje

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.6 G 0.20 Informacije ali izdelki iz nezanesljivega vira, G 0.21 Manipulacija strojne ali programske opreme in G 0.41 Sabotaža	Uporaba informacij, programske opreme ali naprav iz nezanesljivih virov, ki niso ustrezno preverjeni, lahko predstavlja vstopno točko za kibernetske napade, vključno z manipulacijo in prikritimi spremembami. Tveganja so še posebej visoka pri odprtokodnih rešitvah ali strojni opremi iz držav z močnimi hekerskimi skupinami, saj lahko vključujejo skrite dostopne točke za dolgotrajno vohunjenje, sabotažo ali povzročitev poslovnih težav zaradi napačnih informacij in izračunov.	Ali je jasno predpisano, katere vrste informacij, programske opreme ali naprav je dovoljeno uporabljati v informacijskem okolju organizacije? Kako se preprečuje uporaba informacij, programske opreme ali naprav, ki niso iz dovoljenih virov? Kako organizacija preverja zanesljivost dobaviteljev programske opreme in strojne opreme? Kako so zaposleni ozaveščeni o tveganjih uporabe izdelkov iz nezanesljivih virov?	OPS.1.1.6 Testiranje in odobritve programske opreme ORP.5 Upravljanje skladnosti (upravljanje zahtev) OPS.2.3 Uporaba zunanjih izvajalcev
3.8.2.7 G 0.23 Nepooblaščen vdor v informacijske sisteme	Vsak element informacijskega okolja lahko v določenih okoliščinah predstavlja možnost nepooblaščenega dostopa in uporabe	Kako organizacija spremlja in zaznava poskuse nepooblaščenega dostopa do informacijskega okolja? Kako zagotavlja, da so sporočila avtomatiziranih rešitev za spremljanje poskusov vdora analizirana in da so na podlagi analiz sprejeti ustrezni ukrepi? Ali organizacija uporablja večfaktorsko avtentikacijo za dostop do ključnih elementov informacijskega okolja in za vse vrste računov s posebnimi (na primer administratorskimi) pravicami? Katere postopke za upravljanje ranljivosti elementov informacijskega okolja je vzpostavila organizacija? Kako pogosto se izvajajo varnostni pregledi informacijskih sistemov za prepoznavanje ranljivosti?	ORP.4 Upravljanje identitet in pravic NET.3.2 Požarni zid DER.1 Zaznavanje varnostno pomembnih dogodkov

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.8 G 0.27 Pomanjkanje virov in G 0.40 Preprečevanje storitev	Zahteve osnutka ZInfV-1 in direktive NIS 2 bodo za bistvene in pomembne subjekte zahtevale znatne kadrovske vire, kar predstavlja tveganje zaradi pomanjkanja strokovnjakov na področju kibernetske odpornosti. Poleg kadrovskih se lahko pomanjkanje virov pojavi tudi kot pomanjkanje procesnih in komunikacijskih zmogljivosti, zaradi česar so organizacije ranljive za napade, kot so DoS-napadi, ki izčrpavajo sistemske vire in onemogočijo dostop dejanskim uporabnikom, zlasti v izrednih situacijah.	Ali je organizacija vzpostavila postopke za zagotavljanje neprekinjenega poslovanja in ali ti predvidevajo tudi ravnanja v primeru večjih incidentov na področju kibernetske odpornosti? Je jasno določila odgovornosti za izvedbo posameznih nalog , predvsem vloge in odgovornosti za obnovitev delovanja omrežnih in informacijskih sistemov po prekinitvah? Kako pogosto se testirajo načrti za zagotavljanje neprekinjenega poslovanja, vključno s pripravljenostjo na kibernetske napade, in ali so določeni jasni cilji uspešnosti teh testov? Ali ima organizacija popisane elemente informacijskega okolja, ki so posebej izpostavljeni napadom, kot je preprečevanje storitev? Ali so vzpostavljeni postopki specifično za odzivanje na -napade s preprečevanjem storitev in obvladovanje njihovih posledic? Kako organizacija identificira in naslavlja pomanjkanje virov pri zagotavljanju kibernetske odpornosti?	OPS.1.1.1 Splošno delovanje informacijskih tehnologij DER.4 Upravljanje v izrednih okoliščinah DER.2.3 Vzpostavitev delovanja po obsežnih varnostnih incidentih
3.8.2.9 G 0.28 Programske ranljivosti ali napake	Večja kompleksnost informacijskih rešitev povečuje verjetnost napak, ki kljub obsežnemu testiranju ostajajo neodkrite, s čimer postanejo ranljivosti za kibernetske napade, obenem pa lahko povzročijo težave v delovanju, napačne izračune in druge operativne težave.	Kako organizacija prepoznava in odpravlja ranljivosti v programski opremi? Kako hitro uvede objavljene popravke v svoje informacijsko okolje? Ali organizacija uporablja avtomatizirane sisteme za upravljanje popravkov in posodobitev? Kakšne preizkuse programske opreme opravi organizacija pred prenosom popravkov v svoje informacijsko okolje?	OPS.1.1.3 Upravljanje popravkov in sprememb DER.3.1 Revizije in pregledi CON.9 Izmenjava informacij
3.8.2.10 G 0.30 Neupravičena uporaba ali administracija naprav in sistemov	Nepooblaščeni uporabniki, kot so kibernetski napadalci, lahko z nepooblaščeno uporabo naprav in administratorskih računov pridobijo dostop do zaupnih informacij, manipulirajo s konfiguracijami in povzročijo resne motnje ali škodo v delovanju informacijskih rešitev.	Kako organizacija nadzoruje uporabo administrativnih in drugih močnih pravic pri dostopu do občutljivih elementov informacijskega okolja? Ali so administrativne funkcije omejene na pooblaščeno osebje z ustrezno usposobljenostjo? Kako organizacija zaznava in preprečuje neupravičeno uporabo pravic?	ORP.4 Upravljanje identitet in pravic OPS.1.1.2 Pravilna administracija informacijskih tehnologij DER.1 Zaznavanje varnostno pomembnih dogodkov

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.11 G 0.31 Napačna uporaba ali administracija naprav in sistemov	Napake pri namestitvi, konfiguraciji, vzdrževanju ali upravljanju strojne in programske opreme, kot so preširoka dovoljenja, enostavna gesla in nešifriran prenos podatkov, lahko omogočijo kibernetske napade in povzročijo resno škodo.	Kako so opredeljeni postopki za pravilno uporabo in administracijo ključnih elementov informacijskega okolja? Kako organizacija izvaja usposabljanje zaposlenih glede pravilne uporabe informacijskih tehnologij? Ali organizacija uporablja nadzorne sisteme za zaznavanje napačne uporabe ali nepravilne administracije? Ali so administrativne funkcije omejene na pooblaščeno osebje z ustrezno usposobljenostjo? Ali se pri najbolj občutljivih spremembah konfiguracij izvaja kontrola štirih oči?	OPS.1.1.2 Pravilna administracija informacijskih tehnologij ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost OPS.1.1.5 Beleženje
3.8.2.12 G 0.32 Zloraba pravic	Zloraba pravic nastopi, ko se zakonito ali nezakonito pridobljene uporabniške pravice uporabljajo izven predvidenega okvira, pogosto za osebno korist ali škodovanje instituciji, pri čemer je lahko del kibernetskega napada.	Kako organizacija spremlja uporabo pravic dostopa in zaznava morebitne zlorabe? Kako organizacija redno pregleduje in omejuje dostop do ključnih elementov informacijskega okolja za pooblaščene uporabnike? Kako organizacija zagotavlja skladnost z varnostnimi politikami za preprečevanje zlorabe pravic? Kako organizacija upravlja dodeljevanje in preklic pravic dostopa pri spremembah zaposlitvenega statusa ali položaja zaposlenih? Ali organizacija uporablja avtomatizirana orodja za spremljanje uporabe dostopnih pravic in zaznavanje morebitnih neobičajnih aktivnosti? Kako organizacija obravnava ugotovljene primere zlorabe pravic, in kakšni so postopki za takojšnje ukrepanje? Kako pogosto organizacija preverja in posodablja nastavitve dostopnih pravic, da bi zagotovila da so primerne na trenutne potrebe? Ali organizacija vodi evidenco o dodeljevanju, spreminjanju in preklicu dostopnih pravic, in kako dolgo se ti podatki hranijo? Kakšne ukrepe izvaja organizacija za zmanjšanje tveganja zlorabe privilegiranih računov (npr. administrativnih računov)?	ORP.4 Upravljanje identitet in pravic OPS.1.1.5 Beleženje DER.1 Zaznavanje varnostno pomembnih dogodkov

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.13 G 0.35 Prisila, izsiljevanje ali korupcija	Kibernetski napadalci lahko z grožnjami ali podkupovanjem poskušajo prisiliti zaposlene, zlasti tiste na položajih zaupanja, da kršijo varnostne politike in omogočijo dostop do informacijskega okolja organizacije.	Kako organizacija ozavešča zaposlene o prepoznavanju tveganj izsiljevanja in korupcije? Kakšne zaščitne ukrepe je organizacija vzpostavila za varovanje ključnih zaposlenih pred zunanjimi pritiski in korupcijo?	ORP.2 Osebje ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost DER.1 Zaznavanje varnostno pomembnih dogodkov
3.8.2.14 G 0.39 Zlonamerna programska oprema	Zlonamerna programska oprema, kot so virusi, črvi in trojanski konji, izvaja prikrite škodljive funkcije, ki napadalcem omogočajo šifriranje podatkov, krajo gesel, daljinski nadzor sistemov in onemogočanje varnostnih programov, kar lahko povzroči motnje v delovanju organizacij, krajo podatkov ter okužbe strank in partnerjev.	Kakšne ukrepe je organizacija vzpostavila za zaščito pred zlonamerno programsko opremo? Kako pogosto organizacija posodablja in pregleduje protivirusne ter druge varnostne rešitve? Kako organizacija usposablja zaposlene za prepoznavanje in obvladovanje zlonamerne programske opreme?	OPS.1.1.4 Zaščita pred zlonamerno programsko opremo ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost OPS.1.1.3 Upravljanje popravkov in sprememb
3.8.2.15 G 0.42 Socialni inženiring	Socialni inženiring je metoda, pri kateri napadalci z manipulacijo ljudi pridobijo nepooblaščen dostop do informacijskih sistemov, pogosto z vzpostavitvijo zaupanja prek daljšega stika in postopnim izkoriščanjem pridobljenih informacij.	Kako organizacija ozavešča zaposlene o tveganjih socialnega inženiringa? Ali organizacija izvaja simulacije in testiranja socialnega inženiringa za preverjanje pripravljenosti zaposlenih? Kako organizacija zaznava in beleži poskuse socialnega inženiringa?	ORP.3 Ozaveščanje in usposabljanje za informacijsko varnost DER.1 Zaznavanje varnostno pomembnih dogodkov OPS.1.1.5 Beleženje
3.8.2.16 G 0.43 Vnos sporočil	Pri napadu z vnosom poročil napadalci pošiljajo posebej oblikovana sporočila sistemom ali osebam, da pridobijo korist ali škodujejo žrtvi, pri čemer se zanašajo na opise vmesnikov, specifikacije protokolov ali zgodovino komunikacij.	Kako organizacija filtrira in pregleduje vhodna sporočila za zaznavo morebitnih groženj? Kako organizacija usposablja zaposlene za prepoznavanje sumljivih sporočil? Kako organizacija uporablja sisteme za preprečevanje vdora prek lažnih sporočil?	DER.1 Zaznavanje varnostno pomembnih dogodkov OPS.1.1.4 Zaščita pred zlonamerno programsko opremo CON.9 Izmenjava informacij

Povezava	**Kratek povzetek grožnje**	**Primeri ključnih vprašanj o obvladovanju tveganj in kontrolah**	**Povezava na osnovne gradnike**
3.8.2.17 G 0.47 Škodljivi stranski učinki Iz informacijskimi tehnologijami podprtih napadov	Kibernetski napadi lahko povzročijo nepredvidene posledice, ki prizadenejo neciljne objekte ali tretje osebe zaradi kompleksnosti in povezanosti informacijskih tehnologij ter pomanjkanja dokumentiranih soodvisnosti, kar lahko vodi do napačne ocene potreb po zaščiti ali zanemarjanja odprave pomanjkljivosti.	Kako organizacija analizira in zmanjšuje škodljive učinke napadov na tretje osebe? Katere ukrepe je organizacija vzpostavila za omejitev vpliva napadov na povezane sisteme in partnerje? Kako pogosto organizacija izvaja simulacije za preverjanje odpornosti na kompleksne napade?	DER.2.1 Obdelava varnostnih incidentov DER.4 Upravljanje v izrednih okoliščinah OPS.1.1.7 Upravljanje sistemov

4 Poročanje

Cilj svetovalnega posla je podati priporočila za izboljšanje upravljanja, obvladovanja tveganj in notranjih kontrol na področjih skladnosti z zahtevami osnutka ZInfV-1, direktive NIS 2 ter krepitve kibernetske odpornosti. Poročilo, ki izhaja iz takšnega svetovalnega posla, je mogoče oblikovati na različne načine. Čeprav zaključno delo ne temelji na konkretnem primeru, v nadaljevanju podajam splošna priporočila za oblikovanje poročila, ki lahko služijo kot izhodišče za njegovo pripravo.

4.1 Povzetek

Zaključno poročilo svetovalnega posla o možnih izboljšavah obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfV-1 in direktive NIS 2 je zaradi kompleksnosti tematike lahko zelo obsežno, zato je smiselno vanj vključiti povzetek. Povzetek vodstvu in ključnim deležnikom omogoča hiter pregled glavnih ugotovitev in priporočil ter s tem olajša usmeritev in razumevanje brez podrobnega branja celotnega poročila. Na ta način povzetek izpostavi ključna tveganja in priložnosti za izboljšave, kar omogoča hitro in informirano odločanje.

Povzetek naj vsebuje namen svetovalnega posla, obseg pregleda, ključne ugotovitve, glavna priporočila ter morebitne omejitve. Pri tem naj se v največji meri izogiba uporabi tujk in strokovno-tehničnih izrazov.

4.2 Ključne informacije o izvedenem svetovalnem poslu

Pri svetovalnih poslih je priporočljivo v poročilu navesti ključne informacije o izvedbi posla. Poleg opredelitve namena in ciljev svetovalnega posla (povezava s točko 3.3) je pomembno jasno opredeliti obseg posla, vključno z elementi informacijskega okolja, ki jih je posel zajel, ter časovnim obdobjem, na katero se zaključki in priporočila nanašajo (povezava s točko 3.4). Prav tako je smiselno razkriti uporabljene metode izvedbe svetovalnega posla (povezava s točko 3.6). Pri poslih, povezanih z upravljanjem informacijskega okolja organizacije, je koristno izrecno navesti tudi elemente, ki niso bili vključeni v obseg posla, saj to omogoča jasnejše razumevanje omejitev pregleda in in morebitne druge omejitve in predpostavke svetovalnega posla (povezava s točko 3.4.4).

Druge ključne informacije vključujejo obdobje izvajanja posla, uporabljeno metodologijo in sodelujoče zaposlene. Če je poslovodstvo pri uskladitvi z zahtevami osnutka ZInfV-1 in direktive NIS 2 ter pri vzpostavitvi kibernetske odpornosti izhajalo iz okvira BSI, je potrebno pojasniti, kako so bila sodila iz okvira BSI izpeljana in uporabljena za oceno obvladovanja tveganj in notranjih kontrol. Če so bila dogovorjena druga sodila, jih je prav tako potrebno jasno razkriti.

Pomembno je tudi poudariti, da je bil posel izveden v skladu z Mednarodnimi standardi strokovnega ravnanja pri notranjem revidiranju. To zagotavlja, da so bile pri izvedbi upoštevane strokovne smernice ter zahteve po neodvisnosti in objektivnosti, kar povečuje zaupanje v ugotovitve in priporočila.

4.2.1 Zapis omejitev odgovornosti

V poročilu je treba jasno navesti morebitne omejitve odgovornosti. Ena od teh omejitev izhaja iz standarda 2120.C3, ki določa, da lahko notranji revizorji pomagajo vodstvu pri vzpostavljanju ali izboljševanju upravljanja tveganj, vendar ne smejo prevzeti odgovornosti za dejansko upravljanje tveganj. Čeprav gre za določilo dobro znanega standarda, je smiselno to vključiti v poročilo kot vsebinsko omejitev, zlasti kadar poročilo vsebuje priporočila. S tem se poudarijo meje odgovornosti revizijske funkcije in ohrani neodvisnost notranje revizije.

Omejitev odgovornosti je treba vključiti tudi v primeru, ko notranjerevizijska funkcija ni imela dostopa do določenih dokumentov ali elementov informacijskega okolja. Pogosta situacija je omejena odgovornost za informacijska okolja in storitve podizvajalcev, od katerih je organizacija pomembno odvisna. Ti so običajno predmet ločenih notranjerevizijskih poslov ali pa se zagotovila o njihovem delovanju pridobivajo na druge načine.

4.3 Razkritja in priporočila

Rezultat svetovalnega posla morajo biti jasna razkritja in predvsem izvedljiva priporočila za izboljšanje upravljanja, obvladovanja tveganj in notranjih kontrol na področjih skladnosti z zahtevami osnutka ZInfV-1, direktive NIS 2 ter krepitve kibernetske odpornosti.

Priporočila naj vključujejo praktične predloge za izboljšanje strateškega odločanja na področju kibernetske odpornosti in usklajevanja poslovnih procesov z zahtevami obeh predpisov, pri čemer je ključno upoštevati obseg in kompleksnost informacijskega okolja organizacije ter njene strateške cilje. Prav tako naj priporočila izpostavijo priložnosti za optimizacijo procesov upravljanja tveganj, izboljšanje odzivnosti na kibernetske grožnje ter okrepitev sodelovanja in zavedanja med ključnimi deležniki organizacije.

Na področju nadzora tveganj in notranjih kontrol je pomembno, da priporočila poudarijo potrebo po jasno opredeljenih odgovornostih na področju kibernetske odpornosti in informacijske varnosti kot celote in zagotavljanju rednem spremljanju učinkovitosti kontrol ter kjer je tehnično mogoče uvedbi kazalnikov uspešnosti za pravočasno prepoznavanje in obvladovanje odstopanj.

Priložnost za dodatne izboljšave se lahko pojavi tudi na področju etike in vrednot organizacije. Priporočila naj obravnavajo večjo odgovornost poslovodstva za zagotavljanje kibernetske odpornosti, večjo odgovornost zunanjih izvajalcev ter pogostejše izobraževanje zaposlenih, ki so izpostavljena v zahtevah osnutka ZInfV-1 in direktive NIS 2.

Pri zagotavljanju učinkovitega upravljanja kibernetske odpornosti je pogosto smiselno podati predloge za vzpostavitev jasnih politik in postopkov za obvladovanje kibernetskih tveganj, izboljšanje procesov za zaznavanje in odzivanje na incidente ter vzpostavitev meril uspešnosti za kibernetsko varnost. Prav tako naj priporočila obravnavajo krepitev nadzora nad dostopom do kritičnih informacijskih sistemov, optimizacijo procesov za neprekinjeno poslovanje ter zagotavljanje skladnosti pri sodelovanju z zunanjimi izvajalci.

Na področju sporočanja informacij o tveganjih in kontrolah naj priporočila vključujejo predloge za vzpostavitev ali izboljšanje procesov za strukturirano poročanje o ključnih kibernetskih tveganjih, učinkovitosti kontrol in izvedenih ukrepih. Prav tako naj obravnavajo uvedbo standardiziranih predlog za poročila, ki omogočajo enotno razumevanje tveganj med oddelki, ter vzpostavitev jasnih komunikacijskih poti med poslovodstvom, oddelki za skladnost, upravljanjem tveganj in informacijskimi tehnologijami.

Priporočila za izboljšanje sodelovanja med nadzornimi funkcijami, revizorji in poslovodstvom naj se osredotočijo na vzpostavitev jasnih komunikacijskih protokolov, enotnih standardov za poročanje in učinkovite koordinacije pri prepoznavanju ter obravnavi tveganj. Na ta način lahko organizacija poveča učinkovitost obvladovanja tveganj, zmanjša podvajanje dela in okrepi skladnost z regulativnimi zahtevami.

Poleg zahtev obeh predpisov je lahko odlično izhodišče za oblikovanje priporočil tudi okvir BSI (povezava s točko 3.2.1)

5 Sklep

Zaključno delo o možnih izboljšavah obvladovanja tveganj in notranjih kontrol v povezavi z zahtevami osnutka ZInfv-1 in NIS 2 predlaga svetovalni posel, ki presega zgolj formalno skladnost z osnutkom ZInfV-1 in direktivo NIS 2 ter se osredotoča na širšo krepitev kibernetske odpornosti organizacij. Namen predloga je omogočiti notranji reviziji, da s premišljenim in sistematičnim pristopom prispeva k izboljšavam upravljanja, obvladovanja tveganj in notranjih kontrol. Delo združuje ključne zahteve predpisov z metodološkimi okvirji, kot je BSI, ter vključuje praktične pripomočke, kot so delovni programi in vprašalniki, za oceno in dokumentiranje skladnosti ter kibernetske odpornosti.

Pristop je zasnovan na visoki vsebinski ravni, z omejitvijo tehničnih pregledov, kar omogoča osredotočenost na strateške in organizacijske vidike ter prilagoditev virov in zmogljivosti. Začetna ocena tveganj predstavlja vsebinsko izhodišče posla, medtem ko prilagojeni vprašalniki omogočajo globlji vpogled v specifike obravnavanih področij. Tak način dela lahko zagotovi praktične in uporabne rezultate, ki podpirajo dolgoročno skladnost organizacije s predpisi in njeno kibernetsko odpornost .

Zasnova svetovalnega posla, ki izhaja iz tega zaključnega dela, je prilagodljiva in uporabna za širok spekter organizacij, s čimer želi omogočiti učinkovito izvedbo tovrstnega posla tudi ob raznolikih organizacijskih potrebah in omejitvah. Ključna dodana vrednost predlaganega posla je njegova osredotočenost na krepitev kibernetske odpornosti, ki presega minimalne zahteve skladnosti in ponuja praktične rešitve za aktualne izzive na področju informacijske varnosti in upravljanja tveganj.

6 Literatura in viri

A-SIT Zentrum für sichere Informationstechnologie – Austria. (2023). BSI-IT-Grundschutz-Standards. Bundeskanzleramt Österreich. Pridobljeno 20. 6. 2023 iz spletne strani Urada zveznega kanclerja Avstrije in A-SIT centra za varno informacijsko tehnologijo – Avstrija https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/BSI-IT-Grundschutz-Standards.html.

Bundesamt für Sicherheit in der Informationstechnik. (2017). BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Pridobljeno 1. 5. 2024 na spletni strani Zveznega urada za varnost v informacijskih tehnologijah https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578.

Bundesamt für Sicherheit in der Informationstechnik. (2017). Pridobljeno 1. 5. 2024 na spletni strani Zveznega urada za varnost v informacijskih tehnologijah BSI-Standard 200-2: IT-Grundschutz-Methodik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640.

Bundesamt für Sicherheit in der Informationstechnik. (2021). Informationssicherheit mit System - Der IT-Grundschutz des BSI. Pridobljeno 20. 6. 2023 iz https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.html?nn=128656.

Bundesamt für Sicherheit in der Informationstechnik. (2023). BSI-Standard 200-3: Risikomanagement. Pridobljeno 1. 5. 2024 na spletni strani Zveznega urada za varnost v informacijskih tehnologijah https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html.

Bundesamt für Sicherheit in der Informationstechnik. (2023). BSI-Standard 200-4: Business Continuity Management. Pridobljeno 1. 5. 2024 na spletni strani Zveznega urada za varnost v informacijskih tehnologijah https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html.

Evropski parlament in Svet Evropske unije. (2016). Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Uradni list Evropske unije https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=sl.

Evropski parlament in Svet Evropske unije. (2016). Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov). Uradni list Evropske unije. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Evropski parlament in Svet Evropske unije. (2022). Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske odpornosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148. Uradni list Evropske unije https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32022L2555.

IIA – The Institute of Internal Auditors. (2017). Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju (veljavni od 1. 1. 2017 dalje). Pridobljeno 20. 6. 2023 iz https://si-revizija.si/datoteke/notranji-revizorji/134/nr-ssr-2017_0.pdf

Imperva. 2024 Bad Bot Report. Imperva. Pridobljeno 20. 4. 2024 iz spletne strani https://www.imperva.com. 2024.

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). Pridobljeno 1. 5. 2024 iz portala ISO https://www.iso.org/standard/96958.html.

Minimum security measures for operators of essentials services. (2024). ENISA. Pridobljeno 12. 2. 2024 iz https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services.

National Institute of Standards and Technology. (2023). Framework for Improving Critical Infrastructure Cybersecurity (Version 2.0). U.S. Department of Commerce. Pridobljeno 2. 5. 2024 iz portala NIST https://www.nist.gov/cyberframework.

OpenAI ChatGPT. (2024, 16. oktober). [Generirano besedilo na vprašanje kako na preprost način opredeliti izraz register TDL]. https://chat.openai.com/.

Predlog predpisa Zakon o informacijski varnosti (ZInfV-1) Evidenca vladnega akta 2023-1544-0005. Pridobljeno 15. 3. 2024 iz portala eUprava https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290.

Riigi Infosüsteemi Amet. (2024). Eesti infoturbestandard (E-ITS). Majandus- ja Kommunikatsiooniministeerium Pridobljeno 20. 6. 2023 iz spletne strani https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its .

Slovenski inštitut za revizijo. (2013). Pravilnik o izvajanju izpitov (veljaven od 1. 7. 2013 dalje). Pridobljeno 20. 6. 2023 iz https://si-revizija.si/datoteke/izobrazevanje/806/pravilnik-izpiti.pdf

Statistični urad Republike Slovenije. (2023). Podjetja po dejavnosti (SKD 2008) in velikosti glede na število oseb, ki delajo, Slovenija, letno za leto 2021. Pridobljeno 20. 6. 2023 iz https://pxweb.stat.si/SiStatData/pxweb/sl/Data/-/1418801S.px/table/tableViewLayout2/.

Uradni list RS. (2008). Zakon o revidiranju (ZRev-2). Uradni list RS, št. 65/08, 63/13 – ZS-K in 84/18.

Uradni list RS. (2010). Hierarhija pravil notranjega revidiranja. Uradni list RS, št. 31/10. Pridobljeno 20. 6. 2023 iz https://sirevizija.si/notranji-revizorji/pravila-stroke

Uradni list RS. (2019). Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev. Uradni list RS, št. 39/19.

Uradni list RS. (2020). Pravilnika o pridobitvi potrdil o strokovnih nazivih preizkušeni davčnik, preizkušeni računovodja, preizkušeni notranji revizor in preizkušeni revizor informacijskih sistemov, vpisu v registre pri inštitutu ter načinu vodenja seznamov aktivnih imetnikov nazivov. Uradni list RS, št. 93/2011, 107/2011, 5/2018, 45/2019, 78/2020. Pridobljeno 20. 6. 2023 iz www.revizija.si/datoteke/pravilniki/2060/pravilnik-a-d-i-n-2019.pdf

Zdolšek, D. (2023). Gradivo za izobraževanje za pridobitev strokovnega naziva: Preizkušeni notranji revizor. Ljubljana: Slovenski inštitut za revizijo.