SLOVENSKI INŠTITUT ZA REVIZIJO

LJUBLJANA

ZAKLJUČNO DELO

ZA PRIDOBITEV STROKOVNEGA NAZIVA PREIZKUŠENEGA REVIZORJA INFORMACIJSKIH SISTEMOV

POROČILO O PREGLEDU

SKLADNOST NAROČNIKA – IZVAJALCA BISTVENIH STORITEV Z ZAKONOM O INFORMACIJSKI VARNOSTI IN UREDBO O VARNOSTNI DOKUMENTACIJI IN VARNOSTNIH UKREPIH IZVAJALCEV BISTVENIH STORITEV

FEBRUAR, 2024 MATJAŽ MRAVLJAK

IZJAVA

Matjaž Mravljak, vpisan v izobraževalni program za pridobitev strokovnega naziva preizkušeni revizor informacijskih sistemov izjavljam, da sem avtor tega zaključnega dela in skladno s prvim odstavkom 21. člena Zakona o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15, 63/16 – ZKUASP, 59/19 in 130/22) dovoljujem objavo tega zaključnega dela na spletnih straneh Slovenskega inštituta za revizijo.

V Velenju, 15. februarja 2024

Podpis: Matjaž Mravljak

Digitalno podpisal Matjaž Mravljak
Datum: 2024.05.08 10:12:59 +02'00'

Povzetek poročila za poslovodstvo

Preizkušeni revizor informacijskih sistemov Matjaž Mravljak s. p. je na podlagi revizijskega posla, sklenjenega 1. 8. 2023, v času od 4. 9. 2023 do 22. 9. 2023, izvedel pregled skladnosti naročnika – izvajalca bistvenih storitev z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) in Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23).

Cilj revizijskega posla je bil izvedba pregleda in podaja zagotovila, da naročnik – izvajalec bistvenih storitev, v času izvedbe pregleda, izpolnjuje zahteve z Zakona o informacijski varnosti in Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev na način in v obsegu, kot je določeno v listini o poslu, s katero je bil sklenjen in dogovorjen revizijski posel.

Kot sodila so bila uporabljene relevantne določbe Zakona o informacijski varnosti in določbe Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev ter relevantna poglavja standarda ISO/IEC 27002:2013 s kontrolami podpoglavij, v povezavi z zahtevami iz 9. in 11. člena Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev.

Pregled ni obsegal pregleda izvajanja predpisanih ukrepov (kontrol) pri pogodbenih izvajalcih naročnika, licenciranja in doseganja zahtevanih ravni storitev.

Pri pregledu je bilo skupno identificiranih 20 ugotovitev, ki predstavljajo VISOKO tveganje za varnost omrežij in informacijskih sistemov ter 20 ugotovitev, ki predstavljajo SREDNJE tveganje za varnost omrežij in informacijskih sistemov revidiranega podjetja Gavioli d. o. o., ki zagotavlja bistvene storitve na področju oskrbe s pitno vodo in njeno distribucijo. V nadaljevanju navajamo nekaj ključnih poudarkov oziroma strnjenih ugotovitev pregleda, ki za revidiranca pomenijo bistvena visoka tveganja:

- Sistem upravljanja neprekinjenega poslovanja je ključnega pomena za neprekinjeno izvajanje bistvenih storitev. Iz ugotovitev pregleda izhaja, da v 2018 izvedena analiza vpliva na poslovanje revidiranca ni zajela vseh poslovnih in podpornih procesov in nekaterih pomembnih tveganj. Načrt neprekinjenega poslovanja iz 2018, katerega sestavni del je tudi analiza vpliva na poslovanje, ni bil posodobljen kljub več pomembnim spremembam v sistemih in podjetju. Od 2019 pa pri revidirancu tudi ni določenega skrbnika načrta neprekinjenega poslovanja. Pomanjkljiva ocena vpliva na poslovanje v povezavi z neposodobljenim načrtom neprekinjenega poslovanja in posledično pomanjkljiv načrt varnostnih ukrepov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežja in informacijskih sistemov, predstavlja pomembna varnostna tveganja za neprekinjeno izvajanje bistvenih storitev in pomeni neskladje z ZInfV.

- Ustrezno urejeni odnosi z zunanjimi ponudniki storitev, ki zagotavljajo storitve, ki so bistvenega pomena za delovanje bistvenih storitev, so ključne za varno neprekinjeno izvajanje bistvenih storitev. Iz ugotovitev pregleda izhaja, da revidiranec ni imel sklenjenih ustreznih vzdrževalnih pogodb z zunanjimi ponudniki storitev za nekatere ključne informacijske sisteme, ki zagotavljajo delovanje bistvenih storitev. Neurejena pogodbena razmerja z zunanjimi ponudniki storitev, odsotnost ustreznih pogodb, pomanjkljivosti v pogodbah za vzdrževanje ključnih informacijskih sistemov in posledično neustrezna informacijska podpora izvajanju bistvenih storitev, predstavljajo za revidiranca pomembna varnostna tveganja za neprekinjeno izvajanje bistvenih storitev in pomenijo neskladje z ZInfV.

- Redno posodobljenje informacijskih sistemov in izvajanje vdornih testov zagotavlja varno, stabilno in učinkovito delovanje organizacij in je ključno za zmanjševanje informacijskih

tveganj ter zagotavljanje neprekinjenega delovanja podjetij oziroma njihovih storitev. Iz ugotovitev pregleda izhaja, da revidiranec ni redno izvajal posodobitev svojih ključnih informacijskih sistemov, ki zagotavljajo delovanje bistvenih storitev. Pri izvedbi vdornega testa so bili v obseg testiranja vključeni le poslovni informacijski sistemi, ne pa tudi operativni sistemi (npr. SCADA), od katerih je odvisno izvajanje bistvenih storitev, v testiranje pa niso bili vključeni interni pretoki podatkov. Slednje za revidiranca predstavlja pomembna varnostna tveganja za neprekinjeno izvajanje bistvenih storitev in pomeni neskladje z ZInfV.

- Izvajanje ustreznega varnostnega kopiranja in hrambe podatkov je bistvenega pomena za zagotavljanje in ohranjanje neprekinjenega poslovanja in zagotavljanje zaščite pred morebitno izgubo podatkov. Iz ugotovitev pregleda izhaja, da revidiranec nima posebnih tedenskih, mesečnih, niti letnih kopij svojih podatkov, kopiranje pa se je izvajalo inkrementalno. Vsi podatki so hranjeni na diskovju (ni uporabljenih drugih medijev za varnostno kopiranje) že od vzpostavitve informacijske podpore v letu 1992 in so locirani samo na glavni lokaciji, rezervne lokacije za hrambo varnostnih kopij podatkov ni bilo vzpostavljene. Prav tako revidiranec še ni izvedel testa restavriranja podatkov in ne izvaja arhiviranja podatkov. Slednje za revidiranca predstavlja pomembna varnostna tveganja za neprekinjeno poslovanje in pomeni neskladje z ZInfV.

Tako je bilo v okviru izvedbe pregleda skupno ugotovljenih 40 neskladij z Zakonom o informacijski varnosti (in Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev). Ugotovljeno pa je bilo tudi neskladje s predpisi s področja varstva osebnih podatkov in s področja dokumentarnega in arhivskega gradiva, kar lahko predstavlja tveganje za uvedbo prekrškovnega postopka zoper revidiranca in izrek visoke globe.

Na podlagi ugotovitev izvedenega pregleda revizor podaja mnenje, da revidiranec podjetje Gavioli d. o. o., ki je izvajalec bistvenih storitev na področju oskrbe s pitno vodo in njeno distribucijo, v času izvedbe pregleda oziroma revizijskega posla med 4. 9. 2023 in 22. 9. 2023, ni bil skladen z Zakonom o informacijski varnosti.

Revidiranec tako za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov ni vzpostavil in vzdrževal dokumentiranega sistema upravljanja varovanja informacij ter sistema upravljanja neprekinjenega poslovanja in ni izvajal vseh predpisanih oziroma potrebnih organizacijskih, logično-tehničnih in tehničnih varnostnih ukrepov, kot to predpisujeta 11. in 12. člen Zakona o informacijski varnosti ter Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev.

Kazalo vsebine

1. UVOD 1

1.1 Predmet in cilj revizijskega posla 1
1.2 Naročnik revizijskega posla 1
1.3 Izvajalec revizijskega posla 1
1.4 Obseg pregleda in omejitve 2
1.5 Uporabljena sodila 2
1.6 Uporabljene metode in načini pridobivanja revizijskih dokazov 2
1.7 Prejemniki poročila in omejitve posredovanja poročila 3

2. OZADJE REVIZIJSKEGA POSLA 3

2.1 Podatki o naročniku, pomembni za izvedbo pregleda 3
2.2 Obveznosti naročnika v skladu z Zakonom o informacijski varnosti 4

3. METODOLOGIJA ZA DOLOČANJE STOPENJ TVEGANJ 5

4. UGOTOVITVE OPRAVLJENIH POSTOPKOV, TVEGANJA IN PRIPOROČILA 6

4.1 Preverjanje upravljanja prometa in komunikacij, zaznavanja, poskusov vdorov in preprečevanja incidentov 7
4.2 Preverjanje opredelitve varnostnih zahtev za ključne dobavitelje revidiranca 11
4.3 Preverjanje identifikacije, pridobivanja, uvajanja in preverjanja posodobitev programske opreme 14
4.4 Preverjanje izvajanja logično-tehničnih in tehničnih varnostnih ukrepov za zaznavanje poskusov vdorov in preprečevanja incidentov 16
4.5 Preverjanje ustreznosti izvajanja varnostnega kopiranja podatkov in ohranjanja dnevniških zapisov o delovanju ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja 18
4.6 Preverjanje politike neprekinjenega poslovanja in načrta njegovega upravljanja ter načrta obnovitve delovanja informacijskih sistemov 21
4.7 Preverjanje osnovnih nastavitev domenske varnosti in varnostne politike uporabniških računov 23
4.8 Preverjanje zagotavljanja ustreznosti ravni dostopnosti informacij, upravljanja s pooblastil za dostop in integritete kadrov 25
4.9 Povzetek ugotovitev 27

5. MNENJE REVIZORJA 28

Kazalo preglednic

Preglednica 1: stopnje tveganja 5
Preglednica 2: Ocena vpliva 5
Preglednica 3: Ocena verjetnosti nastanka neželenih posledic na območju Evropske unije 6

Priloge

Priloga A: Seznam uporabljenih kratic

Priloga B: Vprašalnik za revidiranca

Priloga C: Načrt testiranja

Priloga D: Listina o poslu

Priloga E: Načrt revizijskega posla

1. Uvod

Mravljak Matjaž s. p., preizkušeni revizor informacijskih sistemov (v nadaljevanju: revizor) je 1. 6. 2023 od podjetja Gavioli d. o. o., Industrijska cesta 10, Izola (v nadaljevanju: podjetje Gavioli), prejel povpraševanje za izvedbo revizijskega posla in sicer izvedbo pregleda skladnosti podjetja Gavioli z zakonom in podzakonskimi akti, ki je zavezanec (izvajalec bistvenih storitev) po Zakonu o informacijski varnosti. Na podlagi podane ponudbe revizorja je podjetje Gavioli z revizorjem 1. 6. 2023 sklenilo oziroma podpisalo listino o poslu.

Predmet listine o poslu je izvedba pregleda kot revizijskega posla dajanja zagotovil, in sicer izvedba pregleda skladnosti podjetja Gavioli, kot izvajalca bistvenih storitev z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23, v nadaljevanju: ZInfV) in Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23, v nadaljevanju: uredba). Naloga revizorja je bila, da na podlagi izvedenega pregleda poda zagotovilo oziroma mnenje o skladnosti oziroma izpolnjevanju zakonskih zahtev podjetja Gavioli z ZInfV in uredbo.

Revizor se je z listino o poslu zavezal, da bo revizijski pregled opravil v skladu z Zakonom o revidiranju (Uradni list RS, št. 65/08, 63/13 – ZS-K, 84/18 in 115/21) ter Okvirjem strokovnega ravnanja za dajanje zagotovil/revidiranja informacijskih sistemov (ITAF, verzija 3), kot neodvisen in nepristranski strokovnjak, osvobojen od okoliščin, ki ogrožajo nepristranskost. Pri izvedbi posla se je revizor ravnal s potrebno poklicno skrbnostjo in z upoštevanjem veljavnih strokovnih, poklicnih in etičnih standardov.

1.1 Predmet in cilj revizijskega posla

Revizijski posel sta izvajalec – revizor in naročnik opredelila kot pregled ustreznosti in izvajanja načrta varnostnih ukrepov in skladnost naročnika - izvajalca bistvenih storitev z ZInfV v obsegu in z omejitvami, ki izhajajo iz listine o poslu.

Cilj revizijskega posla je bil opraviti pregled in podati zagotovilo, da naročnik – izvajalec bistvenih storitev, v času izvajanja pregleda, izpolnjuje zahteve z ZInfV in uredbe na način, v obsegu in z omejitvami, kot je bilo določeno v listini o poslu. V okviru navedenega cilja se je preverila implementacija in učinkovitost izvajanja predpisanih minimalnih varnostnih ukrepov (kontrolnih postopkov), povezanih z izvajanjem bistvenih storitev.

1.2 Naročnik revizijskega posla

Naročnik revizijskega posla – pregleda je podjetje Gavioli d. o. o., Industrijska cesta 10, Izola, matična številka 111111, ki ga zastopa direktor Martin Peter in je zavezanec – izvajalec bistvenih storitev za področje oskrbe s pitno vodo in njene distribucije, določen s sklepom Vlade Republike Slovenije v skladu z ZInfV.

1.3 Izvajalec revizijskega posla

Izvajalec revizijskega posla je Matjaž Mravljak s. p., Obala 10, Koper, matična številka 222222, aktivni preizkušeni revizor informacijskih sistemov.

1.4 Obseg pregleda in omejitve

Pregled je obsegal pregled relevantne dokumentacije naročnika, in sicer: seznama ključnih, krmilnih in nadzornih informacijskih sistemov, analize obvladovanja tveganj, politike neprekinjenega poslovanja z načrtom njenega upravljanja, načrta obnovitve delovanja informacijskih sistemov, načrta odzivanja na incidente in načrta varnostnih ukrepov. Pregled je obsegal tudi pregled minimalnega obsega in vsebine organizacijskih, logično-tehničnih in tehničnih varnostnih ukrepov in njihovo testiranje.

Pregled ni obsegal pregleda izvajanja predpisanih ukrepov (kontrol) pri pogodbenih izvajalcih naročnika, licenciranja in doseganja zahtevanih ravni storitev.

1.5 Uporabljena sodila

Pri izvedbi pregleda so bila uporabljena naslednja sodila:

- Zakon o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23);
- Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23) in
- standard ISO/IEC 27002:2013 in sicer poglavja z relevantnimi kontrolami podpoglavij v povezavi z zahtevami iz 9. in 11. člena uredbe: A.7.1.2, A.7.2, A.7.3, A.8.1, A.9.1, A.9.2, A.9.4, A.11.1, A.11.2, A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6, A.13.1, A.14.1, A.14.2, A.15.1, A.15.2, A.16.1 in A 17.1, ob upoštevanju področnih posebnosti revidiranca.

1.6 Uporabljene metode in načini pridobivanja revizijskih dokazov

Na podlagi listine o poslu je bil pripravljen načrt revizijskega posla, ki je bil usklajen s podjetjem Gavioli d. o. o. Po preliminarnem pregledu dokumentacije in izvedbi ocene tveganj je revizor ustrezno dopolnil Načrt revizijskega posla ustrezno z načrtom pregleda kontrol in ukrepov.

Za izvedbo pregleda so bile uporabljene naslednje metode in načini pridobivanja revizijskih dokazov:

- pridobitev, pregled in presoja dokumentacije – internih dokumentov, ki jih predpisuje zakon in podzakonski predpis;
- razgovori s pristojnimi predstavniki revidiranca in drugimi zaposlenimi;
- obiski in pregledi lokacij, kjer se izvajajo aktivnosti, povezane z izvajanjem bistvenih storitev;
- pisna vprašanja revidirancu;
- pridobitev in presoja dokazil o izvajanju predpisanih ukrepov;
- pregled in/ali testiranje implementiranih varnostih ukrepov (kontrol) in
- analiza pridobljenih podatkov in informacij.

Za potrebe izvedbe testiranj delovanja določenih kontrolnih postopkov in dosego revizijskih ciljev je bilo uporabljeno vzorčenje po ne-statistični metodi vzorčenja po lastni presoji, glede na pridobitev zadostnih, zanesljivih in ustreznih dokazov o delovanju kontrolnih postopkov.

Pri izvedbi pregleda niso sodelovali zunanji strokovnjaki.

1.7 Prejemniki poročila in omejitve posredovanja poročila

Prejemnik končnega Poročila o pregledu je naveden v 16. točki Listine o poslu in 10. točki Načrta revizijskega posla. Končno Poročilo o pregledu bo v zaprti kuverti in v dveh izvodih dostavljeno poslovodnemu organu naročnika, naslovljeno na direktorja, g. Petra Martina.

2. Ozadje revizijskega posla

2.1 Podatki o naročniku, pomembni za izvedbo pregleda

Podjetje Gavioli d. o. o. (v nadaljevanju: podjetje) opravlja javno službo na podlagi koncesije in se ukvarja s preskrbo pitne vode in upravljanjem odpadne vode in kanalizacije. Podjetje deluje na območju obale, Istre in Krasa. S strani Republike Slovenije je bil določen kot upravljavec kritične infrastrukture in izvajalec bistvenih storitev. Skupno ima podjetje Gavioli več kot 450.000 odjemalcev, tako fizičnih oseb, ki jih je 400.000, kot tudi 50.000 pravnih oseb.

Podjetje ima v povprečju 550 zaposlenih. Sedež podjetja je v Kopru, podjetje pa ima poslovne prostore tudi v Sežani, Divači, Kozini in Izoli.

Podjetje ima veliko fluktuacijo, v letu 2022 je odšlo 15 zaposlenih, novo zaposleni so prišli 4, ostalo izvajajo študenti preko študentskega servisa. V letu 2023 je podjetje zapustilo še 10 zaposlenih, na novo jim je uspelo pridobiti 5 pripravnikov.

Podjetje je svoj poslovni informacijski sistem gradilo deloma samo, deloma pa v sodelovanju z različnimi izvajalci.

V podjetju je v ekipi za informacijsko tehnologijo 8 zaposlenih ter občasno 3 študenti. Dva zaposlena sta programerja, ki sta v podjetju že več kot 30 let in sta sodelovala pri razvoju ERP sistema. Za strojno opremo ter sistemsko programsko opremo skrbita dva sistemska inženirja, ki sta v podjetju od leta 2019. Vodja informatike se je priključil podjetju v januarju 2023.

Podjetje izvaja naslednje procese: pridobivanje pitne vode, zagotavljanje dobave pite vode, analiziranje kakovosti pitne vode, vzdrževanje cevovodov, zagotavljanje delovanje kanalizacije, vzdrževanje kanalizacije, čiščenje greznic, upravljanje čistilnih naprav, poslovodenje, strateško načrtovanje, letno načrtovanje, prodaja, obračun storitev, računovodstvo, upravljanje finančnih sredstev in obveznosti, investicije, nabava, skladiščno poslovanje, zagotavljanje in razvoj kadrov, zagotavljanje notranje revizije, upravljanje odnosov z javnostmi, varovanje okolja in zdravja zaposlenih, zagotavljanje informacijske podpore in zagotavljanje fizične zaščite.

Podjetje svoje ključne delovne procese podpira z različnimi operativnimi tehnologijami. Vodnjake, cevovode, kanalizacijske sisteme in čistilne naprave primarno nadzoruje s sistemi SCADA. SCADA sistem za upravljanje z odpadno vodo in kanalizacijo podjetje najema od podjetja Džubre Ltd. iz Banja Luke v BiH, pri čemer pa je projekt uvedbe zaključilo v letu 2012.

Za procesno kontrolo znotraj večjih naprav uporablja DCS. Za avtomatizacijo elektromehanskih procesov, kot so nadzor črpalk, ventilov in transporterjev uporablja podjetje različne PLC. S SCADA sistemi nadzira tudi same aktuatorje ter zbira podatke iz RTU in vanje vključenih senzorjev in merilnih naprav. Poleg tega ima uvedenih tudi več posebnih sistemov za nadzor kakovosti pitne vode. Za namene obračuna je podjetje vzpostavilo AMI, ki zbira podatke o pitni in odpadni vodi iz pametnih naprav pri odjemalcih skoraj v realnem času in je namenjena obračunavanju.

Zgoraj navedene sisteme in SCADA sistem za upravljanje z odpadno vodo in kanalizacijo, povezano infrastrukturo za upravljanje čistilnih naprav je podjetje nabavilo pri podjetju Avtomatiks d. o.o., ki

napravam nudi tudi kontinuirano podporo, vključno z varnostnimi popravki in nadgradnjami programske opreme.

Podatke o porabi pitne vode in odpadni vodi za obračun pridobi ERP iz AMI preko serijskih procesov, ki temeljijo na izvozu podatkov iz ene rešitve v .csv datoteko in uvozu datoteke v drugo rešitev. Urnike prenosov je podjetje vzpostavilo v orodju IBM Tivoli Workload Scheduler V 8.6, ki ga sicer uporablja tudi za izdelavo varnostnih kopij.

Podjetje je v letu 2019 kupilo tudi CRM informacijsko rešitev podjetja CRMzaVse AquaCRM. Gre za celovit sistem za upravljanje odnosov z odjemalci in je posebej prilagojen podpori procesov za izboljšanje zadovoljstva odjemalcev in racionalizacijo procesov, povezanih z odjemalci na področju oskrbe s pitno in upravljanja odpadne vode.

Komunikacijsko omrežje organizacije je sestavljeno iz »terenske« plasti oziroma »robne« plasti, ki združuje naprave operativne tehnologije, kot so aktuatorji, RTU in senzorji, nadzorne plasti, ki zajema SCADA in DCS sisteme in poslovodne plasti, ki zajema poslovodne sisteme.

Za upravljanje omrežne varnosti in za celostno informacijsko varnost skrbi v letu 2022 ustanovljeno podjetje VarniTu iz vasi Dekani s tremi zaposlenimi. Zunanji izvajalec upravlja vso aktivno in pasivno komunikacijsko opremo in izvaja storitve varnostnega operativnega centra.

Komunikacijske povezave vodnjakov upravlja podjetje PridemoTakoj iz Buj iz Hrvaške.

Strežniška oprema je locirana v kleti upravne stavbe, z rezervno lokacijo v prostorih Droge Portorož.

Za varnost in fizično zaščito objektov skrbi podjetje G10 iz Maribora, ki za podjetje upravlja tudi varnostno nadzorni center.

Vodstvo podjetja je imenovalo pooblaščenca za varovanje informacij v letu 2019, ki je po osnovni izobrazbi prof. zgodovine. Ta oseba je tudi kontaktna oseba med podjetjem in nosilcem sektorja kritične infrastrukture ter tudi kontaktna oseba zavezanca po ZInfV. Podjetje ima tudi službo notranje revizije, ki jo vodi Franci Martin, državni revizor, v službi notranje revizije so zaposlene še tri notranje revizorke.

Podjetje je v letu 2018 doživelo hekerski napad z izsiljevalskim virusom WannaCryII, ki jim je zaklenil datotečni sistem.Za šifrirni ključ je plačalo 150.000€ odkupnine.

V letu 2019 je vodenje podjetja prevzel Martin Peter.

2.2 Obveznosti naročnika v skladu z Zakonom o informacijski varnosti

Podjetje Gavioli, kot izvajalec bistvenih storitev po ZInfV, ima naslednje zakonske obveznosti:

- skladno z metodologijo iz tretjega odstavka 12. člena Zakona o informacijski varnosti, določiti svoje ključne, krmilne in nadzorne informacijske sisteme ter dele omrežja, s katerimi zagotavlja izvajanje bistvenih storitev;
- izvesti analizo, oceno in vrednotenje tveganj ter na tej osnovi pripraviti in izvajati potrebne ukrepe za obvladovanje tveganj glede varnosti omrežij in informacijskih sistemov, ki jih uporablja pri bistvenih storitvah;
- sprejeti ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost tistih omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje bistvenih storitev, da bi zagotovili neprekinjeno izvajanje teh storitev;
- za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostaviti in vzdrževati dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj: 1. analizo

obvladovanja tveganj z oceno sprejemljive ravni tveganj; 2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja; 3. seznam njegovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev; 4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje točke; 5. načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT in 6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo področne posebnosti;

- na podlagi varnostne dokumentacije iz prejšnje alineje mora pripraviti in izvajati potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe;
- zagotavljati ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja za obdobje najmanj šestih mesecev na ozemlju Republike Slovenije;
- nacionalnemu CSIRT brez nepotrebnega odlašanja priglasiti incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev in ob prijavi incidenta poskrbeti za ustrezno zavarovanje dnevniških zapisov oziroma revizijskih sledi, če te obstajajo.

Varnostno dokumentacijo podpiše zakoniti zastopnik izvajalca bistvenih storitev.

3. Metodologija za določanje stopenj tveganj

Metodologija določanja stopenj tveganj pri posameznih ugotovitvah revizijskega pregleda temelji na predpostavki, da se tveganje določa glede na ugotovljeno neskladje s predpisi v povezavi z možnim nastankom negativnih posledic za naročnika, ki je izvajalec bistvenih storitev po ZInfV, na področju oskrbe s pitno vodo in njene distribucije.

Stopnja tveganja je enaka zmnožku ocene vpliva na izvajanje bistvenih storitev in ocene stopnje verjetnosti realizacije dogodka, ki negativno vpliva na izvajanje bistvenih storitev.

Preglednica 1: stopnje tveganja

Stopnja tveganja	Vrednost
NIZKO	1 do 9
SREDNJE	10 do 19
VISOKO	20 do 25

Preglednica 2: Ocena vpliva

Ocena	Vpliv na izvajanje bistvenih storitev
1	Potencialen dogodek ima zanemarljiv ali majhen vpliv na izvajanje bistvenih storitev.
3	Potencialni dogodek lahko povzroči nedelovanje bistvenih storitev, ki v manjšem obsegu prekoračijo tolerirane čase izpada.
5	Potencialne dogodek lahko povzroči hujši oziroma daljši izpad delovanja bistvenih storitev.

Preglednica 3: Ocena verjetnosti nastanka neželenih posledic na območju Evropske unije

Ocena	Stopnja verjetnosti	Razlaga
1	redko	Dogodek se lahko zgodi redkeje kot 1-krat na tri leta.
2	malo verjetno	Dogodek se lahko zgodi vsaj 1-krat na tri leta ampak ne pogosteje kot 2-krat letno.
3	verjetno	Dogodek se lahko zgodi več kot 2 - krat letno ampak ne pogosteje kot 1-krat na mesec.
4	zelo verjetno	Dogodek se lahko zgodi več kot 1 - krat na mesec ampak ne pogosteje kot 1-krat tedensko.
5	zagotovo	Dogodek se lahko zgodi pogosteje kot 1-krat na teden.

Pri določanju metodologije se zavestno nista upoštevala kriterij nastanka potencialne materialne škode na poslovanje in kriterij negativnega vpliva na ugled naročnika. Za izračun stopnje tveganja sta se upoštevala vpliv na izvajanje/zagotavljanje bistvenih storitev in ocena verjetnosti realizacije neželenega dogodka, ki ima negativni vpliv na izvajanje bistvenih storitev (oskrba s pitno vodo in njena distribucija).

Pri določitvi ocene vpliva na izvajanje bistvenih storitev se je upoštevala naročnikova Ocena vpliva na poslovanje (BIA analiza), ki sicer ni zajela vseh poslovnih in podpornih procesov in je bila osredotočena predvsem na IT podporo, ni pa zajela ostalih tveganj. Pri določanju stopnje verjetnosti nastanka neželenih posledic so se upoštevali relevantni javno dostopni podatki o preteklih dogodkih in incidentih informacijske varnosti.

Zmnožek ocene posledic na izvajanje bistvenih storitev in ocene stopnje verjetnosti uresničitve neželenega dogodka, predstavlja ocenjeno stopnjo tveganja pri posamezni ugotovitvi.

Stopnja tveganja NIZKO pomeni, da ugotovljeno tveganje ne pomeni neskladnosti z ZInfV, pomeni pa lahko neskladje z drugimi predpisi ali neučinkovito ravnanje oziroma delovanje. Neskladje z drugimi predpisi (npr. s področja varstva osebnih podatkov) lahko predstavlja tveganje za uvedbo prekrškovnega postopka zoper revidiranca in izrek visoke globe.

Stopnja tveganja SREDNJE pomeni, da ugotovljeno tveganje pomeni neskladje z ZInfV in povečano tveganje za incidente informacijske varnosti (lahko tudi neučinkovito delovanje oziroma ravnanje).

Stopnja tveganja VISOKO pa pomeni, da ugotovljeno tveganje predstavlja (hujšo) kršitev določb ZInfV (kršitev je dlje časa trajajoča, ni podanih olajševalnih okoliščin) in pomembna tveganja za pojav incidentov informacijske varnosti s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev (lahko tudi neučinkovito delovanje oziroma ravnanje).

4. Ugotovitve opravljenih postopkov, tveganja in priporočila

Pregled je obsegal pridobitev in analizo oziroma presojo interne dokumentacije, ki jo je revizorju izročil predstavnik revidiranca. Revidirancu je bil posredovan v izpolnitev vprašalnik, ki je obsegal skupno 53 vprašanj v šestih vsebinskih sklopih.

Revizor je v okviru pregleda opravil razgovore z vodjo Službe za informatiko in njegovim namestnikom, pooblaščencem za varovanje informacij, vodjo Službe za notranjo revizijo, obema

programerjema v Službi za informatiko in obema sistemskima inženirjema v Službi za informatiko, skupno 8 razgovorov.

Pregledani sta bili dve fizični lokaciji, kjer so nameščeni ključni, krmilni in nadzorni informacijski sistemi: na sedežu revidiranca v Kopru (primarna lokacija) in v prostorih Droge Portorož v Portorožu (rezervna/sekundarna lokacija).

Izveden je bil pregled predpisanih organizacijskih, logično-tehničnih in tehničnih varnostnih ukrepov (kontrol), kot to predpisujeta 9. in 19. člen Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev. Opravljeno je bilo testiranje kontrol, razdeljeno v osemnajst sklopov: 1. Podpora vodstva revidiranca pri zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja izvajalca bistvenih storitev; 2. Integriteta kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve; 3. Notranji pregled sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov; 4. Upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito; 5. Ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev; 6. Upravljanje prometa in komunikacij; 7. Opredelitev varnostnih zahtev za ključne dobavitelje; 8. Fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi; 9. Varnostni mehanizmi v posamezni aplikativni programski opremi za izvajanje dejavnosti; 10. Preverjanje identitete uporabnikov; 11. Upravljanje in preprečevanje izrabe tehničnih ranljivosti; 12. Zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop; 13. Zaščita pred zlonamerno programsko kodo; 14. Evidentiranje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev; 15. Zaznavanje poskusov vdorov in preprečevanje incidentov; 16. Politika neprekinjenega poslovanja z načrtom njegovega upravljanja; 17. Načrt obnovitve delovanja informacijskih sistemov in 18. Odzivanje na incidente informacijske varnosti.

V nadaljevanju je podan pregled stanja in ključnih ugotovitev, tveganj in priporočil po posameznih segmentih.

4.1 Preverjanje upravljanja prometa in komunikacij, zaznavanja, poskusov vdorov in preprečevanja incidentov

V okviru preverjanja upravljanja prometa in komunikacij ter zaznavanja poskusov vdorov in preprečevanja incidentov sta bili med drugim pregledani tudi obstoječa dokumentacija zavezanca za požarno pregrado Cisco Firepower 4120 (varnostna politika) in dejanske tehnične nastavitve politik na požarni pregradi. Ugotovitve revizorja so naslednje:

Ugotovitev 1.1:	Zadnja posodobitev dokumentacije o požarni pregradi Cisco Firepower 4120 (varnostna politika in njene tehnične nastavitve) je bila v maju 2021.
Tveganja:	Zastarela in neposodobljena dokumentacija o požarni pregradi ne vsebuje informacij, ki odražajo dejansko stanje, kar lahko privede do izvedbe neustrezne analize obvladovanja tveganj in otežuje učinkovito upravljanje sprememb v informacijskih sistemih, kar pa predstavlja tveganja za pojav incidentov informacijske varnosti.
Ocena tveganja:	**SREDNJE**

Priporočilo:	Revidirancu priporočamo, da se čim prej, nato pa v rednih časovnih presledkih, najmanj pa enkrat letno oziroma ob vsaki spremembi programske opreme požarne pregrade, pregledajo in posodobijo politike in tehnične nastavitve požarne pregrade, da se zagotovi skladnost z najnovejšimi varnostnimi standardi, in priporočili proizvajalca.

Ugotovitev 1.2:	Požarna pregrada je sicer ustrezno omejevala vhodni promet, pri izhodnem prometu pa je bila nastavljena na "Allow all by default".
Tveganja:	Uporabljena permisivna politika izhodnega prometa na požarni pregradi z uporabo nastavitve »Allow all by default« za izhodni promet lahko omogoči nezaželen ali škodljiv izhodni promet, saj se iz notranjega dela omrežja pošiljajo podatki na katerikoli zunanji naslov brez kakršne koli kontrole ali filtriranja, kar pa predstavlja pomembno varnostno tveganje za izgubo podatkov in pojav incidentov informacijske varnosti. Brez filtracije izhodnega prometa je težje pravočasno zaznati sumljive ali neavtorizirane dejavnosti oziroma promet.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se čim prej: - Izvede analiza razlogov za nastavitev "Allow all by default" in preuči možnosti za omejitev izhodnega prometa. Če poslovanje organizacije to dopušča, bi bilo priporočljivo izhodni promet omejiti na nastavitev in »Block by default« in omogočiti samo zaupanja vredno in potrebno povezovanje navzven. - Določijo specifična ciljna vrata (ang. porti) za povezane kritične storitve in zagotovitev dostopa do teh virov/storitev samo pooblaščenim računom.

Ugotovitev 1.3:	Administratorski dostop do požarne pregrade ni bil omejen na konkreten spletni naslov.
Tveganja:	Ta varnostna pomanjkljivost lahko v kombinaciji z drugimi varnostnimi ranljivostmi morebitnemu napadalcu omogoči, da pridobi nadzor nad požarno pregrado in s tem nad omrežnim prometom. To pomeni, da se lahko do požarne pregrade dostopa iz kateregakoli računalnika/naprave, ki ima dostop do interneta. Navedeno predstavlja pomembno varnostno tveganje saj lahko nekdo, ki bi pridobil administratorsko geslo, spremenil nastavitve požarne pregrade ali jo celo izključil, s čimer bi ogrozil celotno omrežno varnost.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej omeji administratorski dostop do požarne pregrade na določen IP naslov ali določene IP naslove, ki pripadajo zaupanja vrednim napravam, za dostop pa se uvede uporaba močnega gesla ter večfaktorska avtentikacija.

Ugotovitev 1.4:	Od nekaj več kot 400 VPN dostopov za zaposlene, jih 12 ni zahtevalo več faktorske avtentikacije, kar pomeni, da se lahko do VPN poveže kdorkoli, ki pozna uporabniško ime in geslo, če ni omogočenega dodatnega preverjanja pristnosti z drugimi mehanizmi. To predstavlja pomembno varnostno tveganje, saj lahko nekdo, ki neupravičeno pridobi poverilnice ali z ugibanjem pridobi te podatke, pridobi dostop do notranjega omrežja podjetja, kjer lahko izvede kibernetski napad.

Tveganja:	Neuporaba večfaktorske avtentikacije (MFA) za VPN dostope na požarni pregradi predstavlja pomembno varnostno tveganje, ki lahko ogrozi varnost omrežja in podatkov organizacije saj se lahko do VPN poveže kdorkoli, ki pozna uporabniško ime in geslo ali nekdo, ki neupravičeno pridobi poverilnice.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej za vse VPN dostope brez izjem uvede večfaktorska avtentikacija, ki poleg uporabniškega imena in gesla ustrezne kompleksnosti zahteva še drug faktor, kot je na primer koda, ki jo pošlje aplikacija na mobilni telefon ali uporaba strojnega generatorja kod ter se v skladu s tem preveri in posodobi politika dostopa.

Ugotovitev 1.5:	Požarna pregrada je imela nastavitev časovne prekinitve povezav (angl. *Timeout*) za protokol TCP: 36.000 s, UDP: 3.600 s in ICMP: 300 s. Ti parametri so previsoki, saj lahko to povzroči nepotrebno obremenitev omrežja z dolgotrajnimi neaktivnimi sejami.
Tveganja:	Navedene ugotovljene nastavitve *timeout-a* za protokol TCP, UDP in ICMP predstavljajo varnostno tveganje, saj omogočajo, da se povezave ohranjajo odprte dlje časa, kot je to potrebno. To lahko povzroči zasedenost omrežnih virov, zmanjšanje zmogljivosti požarne pregrade ali določenih primerih celo izkoriščanje ranljivosti, ki temeljijo na zlorabi časovnih prekinitev.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se nastavitve časovne prekinitve povezav znižajo na razumne vrednosti, ki so odvisne od vrste prometa in uporabljenih aplikacij in so dovolj dolge, da omogočajo normalno delovanje omrežnih aplikacij, a dovolj kratke, da preprečijo zlorabo sistemskih virov (za TCP se priporoča vrednost 600 s, za UDP 60 s in za ICMP 10 s).

Ugotovitev 1.6:	Uporabljeno (nastavljeno) šifriranje na požarni pregradi je AES-128.
Tveganja:	Uporaba AES-128 je sicer varna oziroma ustrezna v sedanjih časovnih okoliščinah, vendar obstajajo ustreznejše možnosti, kot je na primer uporaba AES-256, ki zagotavlja večjo odpornost in zmanjšuje tveganje tudi na potencialne napade z uporabo kvantnih računalnikov, ki se pospešeno razvijajo.
Ocena tveganja:	**NIZKO**
Priporočilo:	Revidirancu priporočamo, da se za šifriranje na požarni pregradi izbere/nastavi in uporabi najvišji možni nivo varnosti, ki ga podpira obstoječa požarna pregrada oziroma AES-256.

Ugotovitev 1.7:	Za IPS na požarni pregradi je uporabljena nastavitev »*monitor*« namesto »*inline*«.
Tveganja:	Navedena nastavitev predstavlja varnostno tveganje, saj se spremlja le omrežni promet in zaznava morebitne napade, vendar se ne ukrepa proti njim oziroma ne preprečuje prehoda škodljivega prometa skozi omrežje in lahko potencialni napadalec izvaja svoje dejavnosti, ne da bi bil pri tem oviran.
Ocena tveganja:	**SREDNJE**

Priporočilo:	Revidirancu priporočamo, da se za IPS, če je to izvedljivo, uporabi nastavitev »*inline*« za aktivno blokiranje škodljivega prometa in potencialnih groženj, ki omogoča, da se samodejno blokira ali preusmeri promet, ki je na požarni pregradi označen oziroma prepoznan kot škodljiv oziroma nevaren. Če pa to ni izvedljivo, se priporoča implementacija dodatnih varnostnih kontrol pri spremljanju omrežnega prometa.

Ugotovitev 1.8:	Na požarni pregradi ni bilo nameščenih oziroma uporabljenih zadnjih popravkov sistemske programske opreme.
Tveganja:	Neuporaba zadnjih popravkov sistemske programske opreme na požarni pregradi predstavlja pomembno varnostno tveganje, saj to lahko pomeni, da požarna pregrada ni zaščitena pred izrabo znanih tehničnih ranljivosti, ki jih uspešno za kibernetske napade izkoriščajo napadalci ali pa požarna pregrada deluje z zastarelo funkcionalnostjo, kar lahko vpliva na njeno učinkovitost in zmogljivost.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej vzpostavijo postopki in ukrepi za redno in sistemsko preverjanje razpoložljivosti novih varnostnih popravkov ter verzij programske opreme ter se jih namešča, ob upoštevanju potrebnih varnostnih postopkov in navodil proizvajalca. Zadnja verzija sistemske programske opreme za Cisco Firepower 4120 je verzija 7.4.x, ki je bila posodobljena 10. novembra 2023.

Ugotovitev 1.9:	Komunikacijsko omrežje organizacije je sestavljeno iz "terenske" plasti (angl. *Field Layer*) oziroma robne (angl. *Edge*) plasti, ki združuje naprave operativne tehnologije, kot so aktuatorji, RTU in senzorji, nadzorne plasti, ki zajema SCADA in DCS sisteme in poslovodne plasti, ki zajema poslovodne sisteme. Naprave terenske plasti so v nekaterih primerih neposredno povezane v kontrolno plast z neposredno ethernet povezavo ali z brezžičnim Wi-Fi omrežjem. Druge naprave pošiljajo podatke v koncentratorje podatkov ali vmesnike, ki so povezani v kontrolno plast. Naprave kontrolne plasti so povezane v komunikacijski center poslovodnega sistema z najetimi vodi in redundančno preko mobilnega komunikacijskega omrežja.
Tveganja:	Neposredne povezave med terensko plastjo in kontrolno plastjo lahko v kombinaciji z drugimi varnostnimi ranljivostmi predstavljajo varnostno tveganje, saj lahko potencialni napadalci izkoristijo te neposredne ali brezžične povezave za nepooblaščen dostop do kontrolne plasti ali drugih delov omrežja. Brezžične povezave, ki niso ustrezno zaščitene, so lahko ranljive za kibernetske napade, kot so napadi na Wi-Fi dostopne točke.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se izvede ustreznejša segmentacija omrežja, ki bo popolnoma ločila terensko plast od kontrolne plasti z uporabo požarnih zidov, omrežnih prehodov ali drugih varnostnih ukrepov. Prav tako se priporoča dodatna zaščita vseh brezžičnih povezav končnih naprav terenske plasti, ki so povezane v kontrolno plast, na primer uporaba močnih gesel, obveznega šifriranja, implementacija standarda IEEE 802.1X in izvedba varnostnega pregleda s penetracijskim testiranjem (redno periodično izvajanje).

4.2 Preverjanje opredelitve varnostnih zahtev za ključne dobavitelje revidiranca

V okviru preverjanja opredelitve varnostnih zahtev za ključne dobavitelje revidiranca in dejanske izvedbe prenosa zahtev informacijske varnosti v pogodbe za upravljanje, dopolnjevanje in vzdrževanje informacijskih rešitev in sistemov, ki zagotavljajo izvajanje bistvenih storitev zavezanca, so ugotovitve revizorja naslednje:

Ugotovitev 2.1:	V letu 2023 veljavna pogodba o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta, ni jasno in v skladu z Zakonom o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15, 63/16 – ZKUASP, 59/19 in 130/22) opredeljevala lastništva nad deli ERP sistema, ki jih je razvijalo podjetje Soča.
Tveganja:	Nejasnosti, kdo ima pravico do uporabe, spreminjanja, razširjanja ali licenciranja teh delov ERP sistema sicer predstavlja poslovna tveganja, saj lahko povzroči spore, tožbe ali celo izgubo intelektualne lastnine. Modul »Upravljanje kakovosti vode« nadzira in upravlja podatke o kakovosti pitne vode in poroča o metrikah ter odstopanjih kakovosti pitne vode (bistvena storitev zavezanca), zato bi lahko izguba popolnega nadzora nad razvitimi deli ERP sistema pomenilo varnostna tveganja.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se sklene aneks k pogodbi o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta, kjer se natančno določi, kateri deli ERP sistema so last podjetja Soča, kateri deli so last podjetja Gavioli ter kakšne so pravice in obveznosti vsake stranke glede posameznih delov (komponent) ERP sistema.

Ugotovitev 2.2:	V letu 2023 veljavna pogodba o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta ni določala oziroma opredeljevala ravnanja s kopijami produkcijskih podatkov, ki jih je podjetje Soča prevzelo iz produkcije za namene testiranja.
Tveganja:	Navedena ugotovitev predstavlja tveganje za izgubo zaupnosti podatkov, ker ni jasno, na kakšen način se zagotavljata varnost in zaupnost produkcijskih podatkov za namene testiranja, ki lahko vsebujejo tudi občutljive ali osebne podatke. Ugotovitev pa predstavlja tudi tveganja neskladja z Zakonom o varstvu osebnih podatkov in Splošno uredbo o varstvu podatkov.
Ocena tveganja:	**NIZKO**
Priporočilo:	Revidirancu priporočamo, da se sklene aneks k pogodbi o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta, kjer se določi, kako se izvaja anonimizacija, šifriranje, varnostno kopiranje, uničevanje in nadzor nad prevzetimi kopijami produkcijskih podatkov, ter kakšne so odgovornosti, ukrepi in pogodbena kazen v primeru kršitve teh določb (ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, za obdobje najmanj šestih mesecev).

Ugotovitev 2.3:	V letu 2023 veljavna pogodba o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta ni določala ravnanja obeh pogodbenih strank v primeru prekinitve pogodbe.
Tveganja:	Neopredeljeno ravnanje obeh pogodbenih strank v primeru prekinitve pogodbe o podpori pri razvoju in vzdrževanju ERP sistema lahko privede do nejasnosti, kako se bo zagotovilo nemoteno delovanje ERP sistema, prenos znanja, dokumentacije in podpore, kako se bo uredilo plačilo za opravljene storitve in morebitne odškodnine ter kako se bo izvršil prenos produkcijskih podatkov. Nedelovanje ali motnje pri delovanju ERP sistema oziroma modula »upravljanje kakovosti vode« predstavlja varnostno tveganje pri neprekinjenem zagotavljanju bistvenih storitev.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se sklene aneks k pogodbi o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta, kjer se določi, pod kakšnimi pogoji in s kakšnim odpovednim rokom se lahko navedena pogodba prekine, ter kakšne so obveznosti in pravice vsake stranke v primeru prekinitve pogodbe (npr. postopki za varno vračilo ali uničenje kopij produkcijskih podatkov).

Ugotovitev 2.4:	V letu 2023 veljavna pogodba o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta ni določala in opredeljevala ravnanja podjetja Soča v vlogi pomembnega zunanjega izvajalca/ponudnika informacijskih storitev za izvajalca bistvenih storitev.
Tveganja:	Neopredeljeno ravnanje podjetja Soča kot pomembnega zunanjega izvajalca informacijskih storitev za izvajalca bistvenih storitev v pogodbi o podpori ERP sistema lahko privede do varnostnih tveganj, ker ni jasno, kako bo podjetje Soča ravnalo v skladu z zahtevami, s katerimi jih je naročnik izvajalec bistvenih storitev dolžan zavezati s pogodbo, kot so na primer zagotavljanje visoke ravni informacijske varnosti in odpornosti, neprekinjenosti zagotavljanja storitev, izvajanje varnostnih ukrepov za preprečevanje in obvladovanje incidentov, poročanje o varnostnih dogodkih in izpolnjevanje drugih obveznosti, ki jih določa zakonodaja.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se sklene aneks k pogodbi o podpori pri razvoju in vzdrževanju ERP sistema s podjetjem Soča iz Novega mesta, kjer se določi minimalne organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki obsegajo najmanj izvajanje ukrepov za zagotavljanje visoke ravni informacijske varnosti in odpornosti, neprekinjenosti zagotavljanja storitev, izvajanje varnostnih ukrepov za preprečevanje in obvladovanje incidentov in poročanje o varnostnih dogodkih ter kakšne so posledice v primeru neizpolnjevanja teh zahtev.

Ugotovitev 2.5:	V letu 2023 veljavna pogodba o podpori pri razvoju in vzdrževanju ERP sistema, sklenjena s podjetjem CRMzaVse ni opredeljevala ravnanja z osebnimi podatki strank, do katerih je podjetje CRMzaVse lahko dostopalo v okviru vzdrževanja CRM rešitve. To pomeni, da ni jasno, kako se zagotavlja skladnost z Zakonom o varstvu osebnih podatkov in Splošno uredbo o varstvu podatkov, ki določata pravila in obveznosti glede obdelave osebnih podatkov.
Tveganja:	Neopredeljeno ravnanje z osebnimi podatki strank v pogodbi o vzdrževanju CRM rešitve lahko privede do nejasnosti, kako se zagotavlja skladnost z Zakonom o varstvu osebnih podatkov in Splošno uredbo o varstvu podatkov,

	ki določata pravila in obveznosti glede obdelave osebnih podatkov, kar predstavlja tveganje za uvedbo prekrškovnega postopka zoper revidiranca in izrek visoke globe.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se sklene aneks k pogodbi o podpori pri razvoju in vzdrževanju ERP sistema, sklenjena s podjetjem CRMzaVse, kjer se določi, za kakšne namene, pod kakšnimi pogoji in s kakšnimi varnostnimi ukrepi lahko podjetje CRMzaVse dostopa do osebnih podatkov strank podjetja Gavioli, ter kakšne so njegove odgovornosti in pravice glede teh podatkov. Prav tako priporoča sklenitev pogodbe o obdelavi osebnih podatkov, ki bo urejala razmerje med upravljavcem in obdelovalcem osebnih podatkov.

Ugotovitev 2.6:	Podjetje Gavioli v letu 2023 ni imelo sklenjene ažurne vzdrževalne pogodbe za sisteme DCS, PLC in druge naprave podjetja Avtomatiks, saj je zadnja vzdrževalna pogodba potekla v novembru 2020. Podjetje Gavioli je kljub preteku roka, za katerega je bila pogodba sklenjena, nadaljevalo s plačevanjem vzdrževalnine in drugih stroškov, podjetje Avtomatiks pa je zanj še vedno izvajalo vse storitve. Zaposleni podporne službe Avtomatiks imajo za namen vzdrževanja do omrežja oziroma naprav podjetja Gavioli neposreden oddaljen dostop.
Tveganja:	Neobstoj ažurne vzdrževalne pogodbe za sisteme DCS, PLC in druge naprave lahko privede nejasnosti in nedorečenosti, na kakšni pravni podlagi se izvajajo te storitve, kakšne so obveznosti in pravice vsake stranke, ter kakšna je kakovost in (informacijska) varnost teh storitev. Neuporaba ustreznih varnostnih elementov pri neposrednem oddaljenem dostopu do omrežja in sistemov revidiranca (npr. Telnet), lahko predstavlja pomembno varnostno tveganje (npr. vdor v informacijski sistem).
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej sklene nova vzdrževalna pogodba s podjetjem Avtomatiks, ki bo določala obseg, ceno, roke, garancije, odgovornosti in druge pogoje za izvajanje vzdrževalnih storitev za sisteme DCS, PLC in druge naprave podjetja Avtomatiks. Priporoča se vključitev varnostne klavzule v pogodbo, ki bo določala minimalne organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki obsegajo najmanj izvajanje ukrepov za zagotavljanje visoke ravni informacijske varnosti in odpornosti, neprekinjenosti zagotavljanja storitev, izvajanje varnostnih ukrepov za preprečevanje in obvladovanje incidentov in poročanje o varnostnih dogodkih. V novi vzdrževalni pogodbi se določijo tudi varnostni elementi načina in pogojev oddaljenega dostopa zaposlenih pogodbenega izvajalca, npr. uporaba VPN, uporaba dvojne avtentifikacije, omejitev na določene IP naslove in beleženje vseh dejavnosti, ki se izvajajo med sejo oddaljenega dostopa.

Ugotovitev 2.7:	Podjetje Gavioli ni imelo sklenjene nobene vzdrževalne pogodbe za sistem SCADA s podjetjem BCC, od katerega je leta 2003 kupilo navedeni sistem ter izven uporabe kupljenega sistema, s podjetjem ne sodeluje več. Prav tako podjetje Gavioli ni izvajalo vzdrževanja in ni posodabljalo sistema.
Tveganja:	Neizvajanje vzdrževanja in neposodabljanje sistema SCADA, ki se uporablja za izvajanje bistvenih storitev, predstavlja pomembno varnostno tveganje, saj podjetje Gavioli nima nobene podpore ali garancije za sistem SCADA, ki se

	uporablja za izvajanje bistvenih storitev, naveden sistem pa je tudi neposodobljen in tako izpostavljen možnostim za okvare ali kibernetske napade.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej sklene ustrezna vzdrževalna pogodba z ustreznim podjetjem, ki bo določala obseg, ceno, roke, garancije, odgovornosti in druge, vključno potrebne varnostne pogoje za izvajanje vzdrževalnih storitev za sistem SCADA. Prav tako se priporoča izvedba varnostnega pregleda sistema SCADA, ki upravlja procese pridobivanja pitne vode, zagotavljanje dobave pitne vode in analiziranje kakovosti pitne vode.

4.3 Preverjanje identifikacije, pridobivanja, uvajanja in preverjanja posodobitev programske opreme

V okviru preverjanja identifikacije, pridobivanja, uvajanja in preverjanja posodobitev programske opreme (v nadaljevanju: upravljanje s posodobitvami), ki neposredno ali posredno zagotavlja procese izvajanja bistvenih storitev, so ugotovitve revizorja naslednje:

Ugotovitev 3.1:	SCADA sistem za upravljanje vodnjakov je bil zadnjič posodobljen v maju 2005.
Tveganja:	Neposodobljen SCADA sistem za upravljanje vodnjakov predstavlja pomembno varnostno tveganje, saj gre za zelo staro in zastarelo različico verzije programske opreme, ki vsebuje znane ranljivosti zaradi pomanjkanja združljivosti z novejšimi varnostnimi standardi, pomanjkljive funkcije overjanja in nadzora dostopa ali uporabe starejših ranljivih protokolov. Poleg tega gre za sistem, ki nadzoruje procese, ki so bistveni za oskrbo s pitno vodo oziroma izvaja bistvene storitve. Tak zastarel sistem je lahko bolj podvržen okvaram in je bolj dovzeten za varnostne ranljivosti ter je lahka tarča za kibernetske napade in v kombinaciji z nekaterimi drugimi ugotovljenimi pomanjkljivostmi, predstavlja pomembno varnostno tveganje.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se navedeni sistem čim prej nadgradi na novejšo različico, ki zagotavlja večjo varnost, stabilnost in funkcionalnost ter se zagotovi redno preverjanje razpoložljivosti novih popravkov.

Ugotovitev 3.2:	Operacijski sistem z/OS in orodje za upravljanje zbirk podatkov DB2 sta bila zadnjič posodobljena v aprilu 2021.
Tveganja:	Neposodobljena operacijski sistem z/OS in orodje za upravljanje zbirk podatkov DB2, predstavljata pomembno varnostno tveganje, saj gre za stari različici, ki vsebujeta številne znane ranljivosti CVE-2023-47152 in CVE-2023-47141; ocena kritičnosti po standardu CVSS od 7.8 do 8,8). Poleg tega sta naveden operacijski sistem in orodje pomembna tudi za delovanje glavnega strežnika, ki shranjuje in obdeluje podatke in je pomemben tudi za delovanje ERP modula »upravljanje kakovosti vode«, ki je del bistvenih storitev. Neposodobljena sistema lahko v kombinaciji z nekaterimi drugimi odkritimi pomanjkljivostmi pomenita pomembno varnostno tveganje, lahko pa pomenita tudi zmanjšane učinkovitosti in zmogljivosti.
Ocena tveganja:	**VISOKO**

Priporočilo:	Revidirancu priporočamo, da se Operacijski sistem z/OS sistem in orodje za upravljanje zbirk podatkov DB2, čim prej nadgradita na novejšo različico, ki zagotavlja večjo varnost, stabilnost in funkcionalnost. Prav tako se priporoča redno preverjanje razpoložljivosti novih popravkov in namestitev čim prej, ob upoštevanju potrebnih varnostnih postopkov, standardov in priporočil proizvajalca.

Ugotovitev 3.3:	Operacijski sistem domenskega strežnika je bil zadnjič posodobljen v maju 2022.
Tveganja:	Neposodobljen operacijski sistem domenskega strežnika (Windows Server 2022), ki je odgovoren za upravljanje z domenskimi imeni, uporabniškimi računi, skupinami, pravicami in politikami v omrežju, predstavlja pomembno varnostno tveganje, saj je to zastarela različica, ki vsebuje znane ranljivosti (CVE-2022-30190 in CVE-2022-26937; ocena kritičnosti po standardu CVSS 7,8 in 9,8). Sistemi, ki niso redno posodobljeni, so bolj dovzetni za varnostne ranljivosti, kibernetske napade in so lahko tudi manj zmogljivi ter manj učinkoviti.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se operacijski sistem domenskega strežnika čim prej nadgradi na novejšo različico, ki zagotavlja večjo varnost, stabilnost in funkcionalnost. Prav tako je treba redno preverjati razpoložljivost novih popravkov in jih namestiti čim prej, ob upoštevanju potrebnih varnostnih postopkov, standardov in priporočil proizvajalca.

Ugotovitev 3.4:	Operacijski sistem strežnika Ubuntu 20.04 LTS in orodje za upravljanje zbirk podatkov PostgreSQL 13 sta bila zadnjič posodobljena v maju 2022.
Tveganja:	Neposodobljen operacijski sistem strežnika Ubuntu 20.04 LTS in orodje za upravljanje zbirk podatkov PostgreSQL 13 sta zastareli različici, ki vsebujeta znane ranljivosti (CVE-2023-39417 in CVE-2023-5869; ocena kritičnosti po standardu CVSS 8,8). Navedeni sistem in orodje sta sicer pomembna za delovanje spletnih aplikacij, ki uporabljajo podatkovno bazo PostgreSQL, vendar bi lahko imela izraba navedenih ranljivosti negativni vpliv tudi na sisteme, ki izvajajo bistvene storitve (lateralno premikanje storilca po omrežju v primeru kibernetskega napada).
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se operacijski sistem strežnika Ubuntu 20.04 LTS in orodje za upravljanje zbirk podatkov PostgreSQL 13 čim prej nadgradita na novejšo različico, ki zagotavlja večjo varnost in stabilnost. Prav tako se priporoča redno preverjanje razpoložljivost in nameščanje novih popravkov, ob upoštevanju potrebnih varnostnih postopkov, standardov in priporočil proizvajalca.

Ugotovitev 3.5:	Platforma za virtualizacijo VMware ESXi 7.0 je bil zadnjič posodobljena septembra 2021.
Tveganja:	Neposodobljena platforma za virtualizacijo VMware ESXi 7.0, predstavlja pomembno varnostno tveganje, saj je to zastarela različica, ki vsebuje znane ranljivosti: CVE-2021-21972 in CVE-2021-21974; ocena kritičnosti CVSS 9,8 in 8,8. Neposodobljena platforma lahko v kombinaciji z nekaterimi drugimi

	odkritimi pomanjkljivostmi pomeni pomembno varnostno tveganje za revidiranca.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da hipervisor VMware ESXi 7.0 čim prej nadgradi na novejšo različico, ki zagotavlja večjo varnost in stabilnost. Prav tako se priporoča redno preverjanje razpoložljivost in nameščanje novih popravkov, ob upoštevanju potrebnih varnostnih postopkov, standardov in priporočil proizvajalca.

Ugotovitev 3.6:	Podjetje je svoj poslovni informacijski sistem deloma razvilo samo, deloma pa v sodelovanju z različnimi izvajalci. Podjetje je že leta 2002 vzpostavilo ERP sistem, ki ga je razvilo v okolju z/OS na osrednjem računalniku IBM. Sistem ERP je bil razvit v jeziku COBOL v okolju CICS in deluje na orodju za upravljanje zbirk podatkov DB2 13 na operacijskem sistemu z/OS 2.4. Podjetje za verzioniranje uporablja orodje IBM Engineering Workflow Management. Moduli ERP so integrirani, kar zagotavlja celovit in koheziven ERP sistem, prilagojen specifičnim potrebam podjetja. Podjetje je leta 2020 vzpostavilo nov osrednji računalnik IBM z15 s 190 procesorskimi enotami in 40 TB razpoložljivega pomnilnika. Računalnik je konfiguriran s 5,2 GHz procesorjem in je izjemno zmogljiv. Podjetje je nanj preneslo svoj obstoječi ERP.
Tveganja:	COBOL je zelo star jezik, ki se danes redko uporablja. To lahko povzroči težave pri vzdrževanju in nadgradnji sistema, saj je težko najti strokovnjake za COBOL. Čeprav je podjetje nadgradilo svoj osrednji računalnik, obstaja tveganje, da je ERP sistem (ki je bil prvotno razvit leta 2002) zastarel in morda ne izpolnjuje vseh zahtev informacijske varnosti in je tudi manj zmogljiv. Zaradi pomanjkanja strokovnjakov za COBOL in zastarelosti tehnologije se lahko pojavijo težave pri vzdrževanju in nadgradnji sistema.
Ocena tveganja:	**NIZKO**
Priporočilo:	Revidirancu priporočamo, da preuči možnosti za nadgradnjo ERP sistema na sodobnejšo tehnologijo, ki je bolj prilagodljiva in zmogljivejša ter lažja in cenejša za vzdrževanje, ker je na voljo več strokovnjakov. Starejše tehnologije so tudi pogosto nezdružljive z novimi tehnologijami, kar lahko omeji možnosti za integracijo z novimi sistemi ali tehnologijami in zmanjša učinkovitost.

4.4 Preverjanje izvajanja logično-tehničnih in tehničnih varnostnih ukrepov za zaznavanje poskusov vdorov in preprečevanja incidentov

V okviru preverjanja izvajanja logično-tehničnih in tehničnih varnostnih ukrepov za zaznavanje poskusov vdorov in preprečevanja incidentov so bila med drugim pregledana poročila o izvedenih varnostnih pregledih omrežja in izvedenih vdornih testih. Podjetje Gavioli je 2020 naročilo izvedbo vdornega testa pri podjetju RiskSI. Pri pregledu poročil o izvedbi vdornega atesta je bilo ugotovljeno, da je bil test izveden pomanjkljivo in nepopolno. Rezultati testiranja tudi niso odražali dejanskega stanja, kakor tudi ne stanja, ki je bilo opisano v poročilu. Ugotovitve revizorja iz Poročila o vdornem testu so naslednje:

Ugotovitev 4.1:	Izvajalec vdornega testa je v obseg testiranja vključil le poslovne informacijske sisteme, operativni sistemi pa niso bili vključeni v obseg testiranja.

Tveganja:	Izključitev operativnih sistemov iz vdornega testiranja pomeni pomembno varnostno tveganje za organizacijo, saj so ti sistemi ključni del informacijske infrastrukture za izvajanje bistvenih storitev in bi morali biti obvezno vključeni v obseg vdornega testiranja. Slednje bi omogočalo identifikacijo morebitnih ranljivosti v operativnih sistemih in izpostavljenosti tveganjem kibernetskih napadov.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej izvede celovit vdorni test, z najemom drugega zanesljivega in kompetentnega ponudnika, ki bo vključeval tako vse poslovne informacijske sisteme kot vse operativne sisteme - aplikacije in naprave v omrežju.

Ugotovitev 4.2:	Izvajalec vdornega testiranja se je osredotočil le na pretoke podatkov poslovnih informacijskih sistemov in zunanjih omrežij, ni pa izvedel testov internih pretokov podatkov, na primer prenosa podatkov med ERP sistemom in CRM rešitvijo. Preverjanje internih pretočnosti podatkov je ključno za odkrivanje morebitnih ranljivosti v notranji komunikaciji, zato ne izvedba pregleda in testiranja internih pretokov podatkov predstavlja pomembno varnostno tveganje za izvajanje bistvenih storitev.
Tveganja:	Ne izvedba testiranja internih pretokov podatkov, kot je prenos podatkov med ERP sistemom in CRM rešitvijo, predstavlja pomembno varnostno tveganje, saj lahko v notranji komunikaciji obstajajo ranljivosti, ki niso bile odkrite in bi lahko bile izrabljene za zlonamerne namene (npr. prestrezanje podatkov, spreminjanje podatkov med prenosom, *Man-in-the-Middle* napad).
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se v čim krajšem možnem času izvede celovit vdorni test, z najemom drugega zanesljivega in kompetentnega ponudnika, ki bo obsegal tudi testiranje internih pretokov podatkov, kar vključuje tudi preverjanje pravilnosti konfiguracij, posodobitev in popravkov ter ugotavljanje morebitnih ranljivosti.

Ugotovitev 4.3:	Izvajalec vdornega testiranja v vdorni test ni vključil pregleda odpornosti OT VLAN-ov.
Tveganja:	Ne vključitev pregleda odpornosti OT VLAN-ov v vdorni test predstavlja pomembno varnostno tveganje za podjetje, saj OT VLAN-i igrajo ključno vlogo pri zagotavljanju varnosti in segmentacije v industrijskih kontrolnih sistemih. Preverjanje odpornosti OT VLAN-ov je ključno za odkrivanje morebitnih ranljivosti v OT omrežni infrastrukturi, ki zagotavlja delovanje bistvenih storitev. Izpostavljenost OT VLAN-ov kibernetskim grožnjam lahko povzroči izgubo nadzora ali motnje oziroma prekinitev delovanja bistvenih storitev.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se čim prej izvede celovit vdorni test, z najemom drugega zanesljivega in kompetentnega ponudnika, ki bo obsegal tudi pregled odpornosti OT VLAN-ov, varnostni pregled konfiguracij, posodobitev in popravkov ter preverjanje obstoja ranljivosti.

Ugotovitev 4.4:	Izvajalec vdornega testiranja v vdorni test ni vključil pregleda učinkovitosti nastavitve vseh zaščit med posameznimi VLAN-i.
Tveganja:	Ne vključitev pregleda učinkovitosti nastavitve zaščit med posameznimi VLAN-i v vdorni test predstavlja pomembno varnostno tveganje za organizacijo, saj VLAN-i igrajo ključno vlogo pri zagotavljanju varnosti in segmentacije omrežja, kar je ključno za pravilno nastavitev in delovanje ustreznih zaščit. Ne testirani VLAN-i lahko predstavljajo izpostavljenost kibernetskim napadom, kar lahko povzroči izgubo nadzora ali motnje v delovanju bistvenih storitev.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se v čim krajšem možnem času izvede celovit vdorni test, z najemom drugega zanesljivega in kompetentnega ponudnika, ki bo obsegal tudi pregled preverjanje učinkovitosti nastavitve vseh zaščit med posameznimi VLAN-i.

Ugotovitev 4.5:	Izvajalec vdornega testa v poročilo ni vključil nekaterih pomembnih navedb, na primer omejitev v povezavi z distribucijo poročila in omejitev pri razkrivanju podatkov tretjim strankam. Prav tako ni razkril samodejnih orodij, s katerimi je izvedel testiranja ali priložil neobdelanih rezultatov testiranja poročilu. Iz poročila tudi ni razvidno, katere neavtomatizirane aktivnosti je izvajalec testa izvedel.
Tveganja:	Pomanjkljivosti v poročilu o vdornem testu, kot so ne vključitev omejitev distribucije poročila, omejitev pri razkrivanju podatkov tretjim strankam, ne izkazovanje uporabljenih samodejnih orodij in ne preložitve neobdelanih rezultatov testiranja, predstavljajo varnostno tveganje saj brez navedenih podatkov ni mogoče oceniti ali preveriti natančnosti in celovitosti izvedenega testiranja, razumeti obsega in globine testiranja. Brez jasnih omejitev glede distribucije in razkrivanja podatkov lahko pride do kršitev pogodbenih ali zakonskih obveznosti oziroma do neupravičenega razkritja poslovne skrivnosti.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se od izvajalca vdornega testiranja zahteva obvezna navedba omejitev v povezavi z distribucijo poročila in omejitev pri razkrivanju podatkov tretjim strankam. Izvajalec naj v prihodnje v poročilu tudi razkrije samodejna orodja, ki jih je uporabil za testiranje, priloži neobdelane rezultate testiranja in navede katere neavtomatizirane aktivnosti je izvedel. Z razpolaganjem z navedenimi podatki bo mogoče oceniti kakovost in ustreznost opravljene storitve in se zanesti na rezultate testiranja.

4.5 Preverjanje ustreznosti izvajanja varnostnega kopiranja podatkov in ohranjanja dnevniških zapisov o delovanju ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja

V okviru preverjanja ustreznosti izvajanja varnostnega kopiranja podatkov in ohranjanja dnevniških zapisov o delovanju ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja so bile ugotovitve revizorja naslednje:

Ugotovitev 5.1:	Orodje IBM Tivoli Workload Scheduler, ki ga je podjetje uporabljalo za načrtovanje različnih operacij, med drugim za izdelavo varnostnih kopij, ni evidentiralo izvedenih operacij v dnevnik, iz katerega bi bilo mogoče za

	določeno časovno obdobje potrditi ustreznost izvajanja varnostnega kopiranja in razbrati morebitne napake v izvedeni operaciji. Orodje IBM Tivoli Workload Scheduler ni ustrezno konfigurirano za beleženje izvedenih operacij v dnevnik, kar bi omogočilo potrditev ustreznosti izvajanja varnostnega kopiranja in razkrivanje morebitnih napak v izvedeni operaciji. Ker brez dnevnika ni mogoče potrditi ustreznosti izvajanja varnostnega kopiranja ali identificirati napak, predstavlja slednje pomembno tveganje informacijske varnosti in za neprekinjeno delovanje bistvenih storitev.
Tveganja:	Neustrezne nastavitve orodja IBM Tivoli Workload Scheduler za evidentiranje izvedenih operacij v dnevnik predstavlja pomembno varnostno tveganje za revidiranca, saj orodje IBM Tivoli Workload Scheduler ni ustrezno konfigurirano za beleženje izvedenih operacij v dnevnik, kar bi omogočilo potrditev ustreznosti izvajanja varnostnega kopiranja in razkrivanje morebitnih napak v izvedeni operaciji. Neustrezna konfiguracija lahko povzroči težave pri odkrivanju napak, povečuje tveganje za izgubo podatkov in onemogoča potrditev ustreznosti izvajanja varnostnega kopiranja.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej izvede konfiguracija orodja IBM Tivoli Workload Scheduler za ustrezno samodejno beleženje vseh izvedenih operacij v dnevnik, kar bo omogočilo sledenje in beleženje vseh operacij, razkrivanje morebitnih napak in zagotavljanje revizijske sledi v izvedenih operacijah, ki jih izvaja IBM Tivoli Workload Scheduler. Revidirancu se priporočata tudi redno preverjanje in posodabljanje nastavitev orodja, da se ohrani oziroma poveča njegova učinkovitost.

Ugotovitev 5.2:	Administrator orodja IBM Tivoli Workload Scheduler naj bi sicer redno prejemal poročila o izvedbi načrtovanih nalog in napakah pri izvedbi operacij na svoj elektronski naslov, a je večino poročil brisal, zaradi česar te navedbe ni bilo mogoče potrditi. Ne administrator orodja ne drugi informatiki, ki so imeli dostop do orodja, v okviru svojega dela niso imeli izrecno navedene naloge pregleda dnevniških zapisov o poteku operacij, ki jih izvaja IBM Tivoli Workload Scheduler.
Tveganja:	Neustrezno upravljanje z IBM Tivoli Workload Scheduler predstavlja tveganje za organizacijo saj lahko administrator, ki ne pregleduje poročil o izvedbi nalog, spregleda kritične napake. Odsotnost jasno določenih nalog za pregledovanje dnevniških zapisov pa povečuje možnost, da se napake ne odkrijejo pravočasno, kar pa lahko vodi do kritičnih zamud pri odkrivanju in odzivanju na incidente.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se uvede politika oziroma postopek za redno pregledovanje dnevniških zapisov oziroma se implementira politika za shranjevanje in arhiviranje vseh poročil ter se določi odgovornost za reden pregled dnevniških zapisov o poteku operacij (poročil o izvedenih nalogah in napakah), ki jih izvaja IBM Tivoli Workload Scheduler. Revidirancu se priporoča tudi implementacija avtomatizacije pregledovanja (npr. uporaba skript za pregledovanje poročil in dnevniških zapisov) in vzpostavitev sistema samodejnega opozarjanja ob morebitnih odstopanjih od pričakovanega delovanja.

Ugotovitev 5.3:	Podjetje je hranilo varnostne kopije na diskih na glavni lokaciji in ni uporabljalo drugih medijev za varnostne kopije.
Tveganja:	Centralizirano shranjevanje varnostnih kopij povečuje tveganje izgube podatkov v primeru okvare ali katastrofe, kar predstavlja pomembno tveganje informacijske varnosti. V primeru okvare, naravnih nesreč, kibernetskega napada ali drugih katastrofalnih dogodkov lahko pride do izgube vseh podatkov, kar bi lahko imelo resne posledice za neprekinjeno delovanje bistvenih storitev.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej implementira politika varnostnega kopiranja, ki vključuje uporabo različnih medijev in vsaj dveh lokacij za shranjevanje varnostnih kopij (politika oddaljenega in večnivojskega varnostnega kopiranja). Priporoča se hramba ene varnostne kopije na primarni lokaciji, ene varnostne kopije na drugi lokaciji in ene varnostne kopije, ločene od omrežja (*Off-line*).

Ugotovitev 5.4:	Kopiranje podatkov se je izvajalo inkrementalno, podjetje nima posebnih tedenskih, mesečnih in niti ne letnih kopij. Vsi podatki so na diskovju že od same vzpostavitve informacijske podpore v letu 1992, baza ima 150 Tb, letni prirastek je 5Tb v zadnjih dveh letih.
Tveganja:	Inkrementalno kopiranje podatkov brez ustrezne strategije za dolgoročno shranjevanje in obnovo predstavlja pomembno varnostno tveganje za podjetje, še posebej če se ne izvajajo redne celovite (polne) varnostne kopije. Opisano stanje bistveno otežuje obnovitev podatkov v primeru katastrofe in povečuje tveganje za izgubo podatkov (inkrementalno kopiranje morda ne zajema vseh potrebnih metapodatkov). V primeru okvare sistema ali izgube podatkov je lahko obnova iz samo inkrementalnih kopij tehnično zapletena in časovno zelo potratna (obnoviti je treba najprej celotno kopijo, nato pa še vse inkrementalne kopije). V primeru kibernetskega napada z izsiljevalskim virusom obstaja velika verjetnost okužbe tudi inkrementalnih kopij, kar bistveno oteži obnovo podatkov.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej implementira politika varnostnega kopiranja, ki bo obsegala tudi postopke za redno izvajanje celovitih varnostnih kopij podatkov. To lahko vključuje tedenske, mesečne ali letne celovite varnostne kopije. Priporoča se tudi preučitev možnosti uporabe tehnologije deduplikacije, kar zmanjša količino prostora, potrebnega za shranjevanje varnostnih kopij (velika količina podatkov). Priporoča se tudi implementacija sistema za sledenje spremembam v podatkovni zbirki, ki omogoča spremljanje vsake spremembe, dodajanja ali izbrisa podatkov.

Ugotovitev 5.5:	Podjetje ni izvajalo arhiviranja podatkov, od leta 1992 je v bazi 150 Tb, letni prirastek v zadnjih dveh letih pa je 5 Tb.
Tveganja:	Neizvajanje ustreznega arhiviranja podatkov lahko predstavlja bistveno večje stroške hrambe podatkov za revidiranca in predstavlja neskladje z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Uradni list RS, št. 30/06 in 51/14).
Ocena tveganja:	**NIZKO**
Priporočilo:	Revidirancu priporočamo, da uvede postopke in ustrezne tehnologije za arhiviranje podatkov, ki omogočajo ustrezno dolgoročno shranjevanje in

	dostopanje do starih podatkov ter zmanjšuje stroške hrambe in pri tem upošteva tudi določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih.

Ugotovitev 5.6:	Podjetje še ni izvedlo testa restavriranja podatkov. Slednje predstavlja pomembno tveganje informacijske varnosti, saj tako ni znano ali se varnostno kopiranje dejansko izvaja ali se izvaja ustrezno in ali bi bila obnova podatkov v primeru katastrofe oziroma potrebe lahko izvedena.
Tveganja:	Neizvajanje testov restavriranja podatkov predstavlja pomembno varnostno tveganje za podjetje. Brez preverjanja postopkov obnovitve podatkov ni mogoče zagotoviti, da se ti postopki sploh izvajajo, se izvajajo ustrezno in bodo ti postopki delovali pravilno v primeru dejanske potrebe po obnovi, kar lahko vodi do izgube podatkov ali do podaljšanega časa nedostopnosti sistemov, ki izvajajo bistvene storitve. Slednje lahko pomeni tudi nezmožnost nadaljevanja poslovanja revidiranca.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da v politiki varnostnega kopiranja podatkov predpiše redno periodično izvajanje testov obnovitve podatkov, da se zagotovi njihova obnovljivost in se potrdi kakovost varnostnih kopij. Vsi postopki obnovitve bi morali biti jasno dokumentirani, vključno s koraki, odgovornostmi in pričakovanim časom obnovitve. Treba bi bilo uvesti tudi sistem nadzora, ki bo spremljal uspešnost obnovitvenih testov in omogočal pravočasno odkrivanje morebitnih napak.

4.6 Preverjanje politike neprekinjenega poslovanja in načrta njegovega upravljanja ter načrta obnovitve delovanja informacijskih sistemov

V okviru preverjanja politike neprekinjenega poslovanja in načrta njegovega upravljanja ter načrta obnovitve delovanja informacijskih sistemov podjetja Gavioli, so ugotovitve revizorja naslednje:

Ugotovitev 6.1:	Podjetje je v letu 2018 pripravilo načrt neprekinjenega poslovanja in obnove po škodnem dogodku. Pripravljeni načrt se osredotoča predvsem na proces pridobivanja in distribucije pitne vode in od nastanka dalje kljub več pomembnim spremembam v sistemih in organizaciji, na katere se nanaša, ni bil posodobljen. Lastnik (skrbnik) načrta je v letu 2019 zapustil podjetje.
Tveganja:	Neobstoj lastnika oziroma skrbnika načrta neprekinjenega poslovanja pri revidirancu in neposodobljen načrt neprekinjenega poslovanja, predstavljata pomembno varnostno tveganje saj ne odražata trenutnega dejanskega stanja informacijskih sistemov, pomembnih sprememb v sistemih in podjetju, odgovornosti in procesov, kar lahko vodi do neustreznega odziva v krizni situaciji in nezmožnost hitre in učinkovite obnove po katastrofi, kar pa lahko povzroči prekinitve delovanja glavnih in podpornih procesov oziroma prekinitev delovanja bistvenih storitev.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej določijo vloge in odgovornosti za izvajanje politike oziroma načrta neprekinjenega poslovanja in njuno posodabljanje, ki se mora izvajati v rednih časovnih presledkih, ali kadar so predlagane ali nastanejo bistvene spremembe. Priporočljiva je tudi

	vzpostavitev rednih periodičnih postopkov testiranja in posodabljanja načrta neprekinjenega poslovanja in načrta obnovitve delovanja informacijskih sistemov, da se zagotovi njuna učinkovitost v primeru resničnega incidenta. Prav tako se revidirancu priporoča revizija ustreznosti načrta neprekinjenega poslovanja glede na dejansko stanje, kar vključuje tudi revizijo ustreznosti ocene vpliva na poslovanje.

Ugotovitev 6.2:	Pri pregledu analize vpliva na poslovanje, ki jo je izvedlo podjetje RiskSI v letu 2018 smo ugotovili, da ta analiza (BIA) ni zajela vseh poslovnih in podpornih procesov in je bila osredotočena predvsem na IT podporo, ni pa zajela ostalih tveganj (finančnih, okoljevarstvenih, kadrovskih, okoljskih, ter tveganj izgube ugleda).
Tveganja:	Nepopolna ocena vpliva na poslovanje predstavlja pomembno varnostno tveganje za podjetje, saj to lahko pomeni, da ključni procesi niso prepoznani in tveganja niso ustrezno obravnavana. Nezadostna je lahko tudi pripravljenost na nepredvidene dogodke, ki lahko negativno vplivajo na ključne (in tudi podporne) poslovne procese oziroma izvajanje bistvenih storitev.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da se čim prej izvede celovita analiza vplivov na poslovanje (BIA), ki zajema vse poslovne in podporne procese ter vključuje finančna, okoljevarstvena, kadrovska, okoljska tveganja in tveganja izgube ogleda. Obvezno pa mora ponovna izvedba analize vplivov na poslovanje vsebovati navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije znotraj podjetja in odpovedi storitev pogodbenih izvajalcev.

Ugotovitev 6.3:	Pri pregledu pogodb podizvajalcev in v okviru pogovorov s skrbniki pogodb s podizvajalci pri revidirancu smo izvedeli, da noben podizvajalec nima ustreznih načrtov neprekinjenega poslovanja, politik neprekinjenega poslovanja in postopkov za neprekinjeno izvajanje pogodbenih obveznosti.
Tveganja:	Nezmožnost zagotavljanja neprekinjenosti storitev pogodbenih izvajalcev ogroža celotno dobavno verigo in tako tudi neprekinjenost izvajanja bistvenih storitev ter predstavlja pomembno varnostno tveganje. Prekinitve v dobavni verigi lahko vodijo do zamud pri dobavi storitev, kar pa lahko ima resne posledice za neprekinjeno delovanje bistvenih storitev.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da z zunanjimi ponudniki storitev oziroma podizvajalci, ki zagotavljajo bistvene storitve, čim prej sklene aneks k pogodbam, ki bodo vsebovali zahteve po izdelavi politike in načrta neprekinjenega poslovanja z mednarodnimi standardi (npr. ISO 22301) oziroma varnostnimi ukrepi ter redno preverjanje njune ustreznosti. Določi pa naj se tudi možnost izvedbe dolžnega nadzorstva podjetja Gavioli nad zunanjimi ponudniki storitev oziroma podizvajalci za področje neprekinjenega poslovanja.

4.7 Preverjanje osnovnih nastavitev domenske varnosti in varnostne politike uporabniških računov

V okviru preverjanja osnovnih nastavitev domenske varnosti in varnostne politike uporabniških računov v domeni gavioli.com smo pregledali varnostne politike in upravljanje uporabniških računov. Ugotovitve revizorja so naslednje:

Ugotovitev 7.1:	*Enforce password history*: Nastavitev je konfigurirana tako, da si sistem zapomni zadnjih 6 uporabljenih gesel. *Maximum password age*: Gesla potečejo po 60 dneh. *Minimum password age*: Ni minimalne starosti gesla, kar pomeni, da lahko uporabniki takoj spremenijo svoje geslo. *Minimum password length*: Minimalna dolžina gesla je 8 znakov. *Password must meet complexity requirements*: Kompleksnost gesla ni zahtevana. *Store passwords using reversible encryption*: Shranjevanje gesel z uporabo reverzibilnega šifriranja je onemogočeno.
Tveganja:	Nizka kompleksnost gesel: Brez zahteve po kompleksnosti gesel obstaja tveganje, da bodo gesla lahko uganjena ali razbita. Hitra rotacija gesel: Možnost, da uporabniki pogosto spreminjajo gesla, lahko vodi do slabše kakovosti gesel, saj se uporabniki lahko odločijo za manj varne vzorce in tako obstaja tveganje za uspešno izvedbo napada z ugibanjem gesel. Pomanjkanje raznolikosti gesel: Z minimalno dolžino gesla 8 znakov in brez zahtev po kompleksnosti lahko pride do pomanjkanja raznolikosti gesel, kar povečuje tveganje za uspešno izvedbo napada z ugibanjem ali razbijanjem gesel. Navedena tveganja lahko imajo negativen vpliv na zaupnost in celovitost informacij in informacijskih sistemov.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da se: - Minimalna dolžina gesla poveča na vsaj 12 znakov. - Uvede zahteva po kompleksnosti gesla, kjer gesla vsebujejo kombinacijo črk, številk in posebnih znakov. - Omeji pogostost spreminjanja gesel tako, da se nastavi minimalno starost gesla na vsaj en dan. - Uporabi seznam pogosto uporabljenih gesel (črna lista) pri čemer se prepreči uporaba najbolj pogostih gesel s črne liste. - Izvede se usposabljanje oziroma ozaveščanje s področja informacijske varnosti za vse zaposlene, imetnike uporabniških računov.

Ugotovitev 7.2:	*Account lockout duration*: Trajanje zaklepanja računa je nastavljeno na 5 minut. *Account lockout threshold*: Prag za zaklepanje računa je nastavljen na 0 neveljavnih poskusov prijave (politika zaklepanja računa ni omogočena). *Reset account lockout counter after*: Števec za ponastavitev zaklepanja računa se ponastavi po 5 minutah.
Tveganja:	Ne omogočena politika zaklepanja računa: Ker prag za zaklepanje računa ni nastavljen, obstaja tveganje za uspešno izvedbo napada z ugibanjem gesla z uporabo surove sile (angl. *brute-force attacks*). Možnost za DoS napade: Če bi bil prag za zaklepanje računa omogočen, bi lahko prenizka nastavitev praga povzročila tveganje za DoS napade, kjer potencialni napadalec namerno zaklene račune z več neuspešnimi poskusi prijave. Navedena tveganja lahko imajo negativen vpliv na zaupnost in celovitost informacij in informacijskih sistemov.

Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da se: - Omogoči politiko zaklepanja računa: Nastavitev praga za zaklepanje računa na priporočeno vrednost, ki uravnoteži varnost (in operativno učinkovitost) na primer 10 neuspešnih poskusov prijave. - Nastavi ustrezno trajanje zaklepanja računa: Nastavitev povečanja trajanja zaklepanja računa, da preprečite hitro ponovno prijavo potencialnega napadalca, na primer na 15 minut. - Ponastavi števec zaklepanja računa po primernem času: Nastavitev časa za ponastavitev števca zaklepanja računa na vrednost, ki je enaka ali večja od trajanja zaklepanja računa, da se prepreči hitro ponovno zaklepanje računa po odklepanju, na primer na 15 minut.

Ugotovitev 7.3:	*Account Logon*: Beleženje uspešnih in neuspešnih prijav je omogočeno.
Tveganja:	Nezadostno spremljanje: Čeprav je beleženje uspešnih in neuspešnih prijav omogočeno (primer dobre prakse, ki omogoča sledenje vseh dejavnosti, povezanih z računi), brez nadaljnjega spremljanja in analize teh podatkov obstaja tveganje, da se ne zazna sumljivih ali neavtoriziranih poskusov dostopa, kar ima negativen vpliv na zaupnost in celovitost informacij in informacijskih sistemov.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da se uvede sistem za spremljanje in analizo oziroma se implementira rešitev za samodejno spremljanje varnostnih dnevnikov, ki bo omogočala hitro odkrivanje sumljivih aktivnosti in avtomatizirano obveščanje o več zaporednih neuspešnih poskusih prijave.

Ugotovitev 7.4:	*Audit Computer Account Management*: Beleženje uspešnih in neuspešnih dogodkov upravljanja uporabniških računov je omogočeno. *Audit Other Account Management Events*: Beleženje drugih dogodkov upravljanja računov, tako uspešnih kot neuspešnih, je omogočeno. *Audit Security Group Management*: Beleženje dogodkov upravljanja varnostnih skupin, tako uspešnih kot neuspešnih, je omogočeno. *Audit User Account Management*: Beleženje dogodkov upravljanja uporabniških računov, tako uspešnih kot neuspešnih, je omogočeno.
Tveganja:	Preobremenitev z dnevniki: Čeprav je beleženje vseh teh dogodkov koristno za spremljanje in analizo lahko privede do velike količine dnevniških zapisov, ki jih je težko obvladovati in analizirati. Pomanjkanje ciljnega spremljanja: Brez ciljnega spremljanja in analize dnevniških zapisov lahko varnostni incidenti ostanejo neopaženi oziroma ne zaznani.
Ocena tveganja:	**NIZKO**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da se: - Preuči in izvede optimizacija politike revizije dnevniških dogodkov ter omeji na beleženje ključnih dogodkov, ki so najbolj relevantni za varnostno politiko podjetja. - Implementira napredna orodja za upravljanje dnevnikov, ki omogočajo filtriranje, opozarjanje in avtomatizirano analizo in izboljšajo odziv na incidente.

Ugotovitev 7.5:	Skupno število uporabniških računov v domeni je 752. 55 uporabniških računov ima administrativne privilegije. 71 uporabniških računov ima gesla, ki nikoli ne potečejo. 53 uporabniških računov z administrativnimi privilegiji ima gesla, ki nikoli ne potečejo. 262 uporabniških računov ni spremenilo gesla v zadnjih 30 dneh. Število uporabniških računov, ki se niso prijavili v zadnjih 30, 60, 120 in 180 dneh, je 158, 162, 173 in 173. 5 uporabniških računov se nikoli ni prijavilo. Pri revidirancu je v povprečju zaposlenih 550 uslužbencev.
Tveganja:	Veliko število administratorskih računov (administrativne pravice) predstavlja tveganje za notranje in zunanje grožnje ter predstavlja pomembno varnostno tveganje za napade (kompromitirani administrativni računi omogočajo širok dostop do sistema). Uporabniški računi z gesli, ki nikoli ne potečejo, so bolj izpostavljeni tveganju zlorabe in predstavljajo pomembno varnostno tveganje za napade. Uporabniški računi, ki dolgo časa ne spremenijo gesla, predstavljajo pomembno varnostno tveganje za napade. Neaktivni računi lahko predstavljajo pomembno varnostno tveganje, saj jih napadalci pogosto izkoriščajo, ker so običajno določena privzeta (generična) prva gesla. Obstajata 202 uporabniška računa (752 uporabniških računov in povprečno 550 zaposlenih), ki pripadata nekomu, ki ni več zaposlen pri revidirancu, kar pa predstavlja pomembno varnostno tveganje za nepooblaščen dostop do informacijskega sistema ali podatkov.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da se: - Omeji število računov z administrativnimi privilegiji na minimum, ki je potreben za poslovanje. - Uvede politika poteka gesel oziroma implementira politika, ki zahteva redno spreminjanje gesel in prepreči uporabo gesel, ki nikoli ne potečejo. - Uvede politika spreminjanja gesel, ki zahteva redno spreminjanje gesel, na primer vsakih 60 ali 90 dni. - Redno pregleduje in deaktivira račune, ki se niso prijavili v določenem časovnem obdobju ali pa je osebam prenehala zaposlitev pri revidirancu. - Uvede obvezno večfaktorsko avtentikacijo pri prijavi v uporabniške račune z administrativnimi privilegiji.

4.8 Preverjanje zagotavljanja ustreznosti ravni dostopnosti informacij, upravljanja s pooblastil za dostop in integritete kadrov

V okviru preverjanja zagotavljanja ustreznosti ravni dostopnosti informacij in upravljanja s pooblastil za dostop do aplikacij, podatkov in sistemov, so ugotovitve revizorja naslednje:

Ugotovitev 8.1:	Modul ERP sistema »Nadzor kakovosti vode«, podpira spremljanje in upravljanje kakovosti tako pitne kot odpadne vode in vsebuje občutljive podatke, kot so kemične sestave, urniki čiščenja in poročila o skladnosti. V AD ima skupina »Splošno osebje«, ki vsebuje člane iz različnih podpornih služb, kot so človeški viri, trženje in služba za stranke, dodeljeno pravico »Branje-Pisanje« do modula »Nadzor kakovosti vode«.
Tveganja:	Zaradi omogočenega prekomernega dostopa imajo vsi člani skupine »Splošno osebje« več dostopa, kot je to potrebno za njihovo delo, kar povečuje tveganje nenamerne ali namerne zlorabe (razkritja) občutljivih podatkov.

Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da se izvede popolna omejitev dostopa do modula »Nadzor kakovosti vode« za vse uporabnike, ki dejansko ne potrebujejo teh informacij za opravljanje svojega dela. Za tiste uporabnike, ki pa navedene informacije z svoje delo potrebujejo, pa lastnik/skrbnik ERP sistema omeji pravice dostopa do modula »Nadzor kakovosti vode«, na pravico »Branje«.

Ugotovitev 8.2:	CSV datoteke, ki nastajajo pri izmenjavi podatkov med ERP in CRM rešitvijo, se nahajajo na posebnem odlagališču. Vsi člani AD skupine »Zaposleni« so imeli do tega dela datotečnega sistema dodeljeno pravico »Branje-Pisanje«. CSV Datoteke niso šifrirane. Prav tako datoteke nimajo nobene kontrolne zgoščene vrednosti (angl. *check sum*).
Tveganja:	Nedovoljen dostop: Člani skupine »Zaposleni« imajo več dostopa, kot je potrebno, kar povečuje tveganje za nenamerno ali namerno zlorabo podatkov (npr. poseg v .csv datoteke, ki vplivajo izplačila), lahko pa pomeni tudi neskladje z Zakonom o varstvu osebnih podatkov in Splošno uredbo o varstvu podatkov. Pomanjkanje šifriranja: Nešifrirane datoteke so bolj izpostavljene tveganju prestrezanja in zlorabe. Pomanjkanje zagotavljanja integritete podatkov: Brez kontrolne zgoščene vrednosti ni mogoče preveriti integritete podatkov po prenosu. Navedena tveganja lahko imajo negativen vpliv na zaupnost in celovitost informacij in informacijskih sistemov.
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da izvede: - Omejitev dostopa do CSV datotek, ki nastajajo pri izmenjavi podatkov med ERP in CRM rešitvijo oziroma se spremenijo nastavitve pravic za skupino »Zaposleni« za to odlagališče v orodju AD na uporabnike, ki dejansko potrebujejo te informacije za opravljanje svojega dela. - Šifriranje datotek za vse CSV datoteke, da se zagotovi njihova varnost med shranjevanjem in prenosom. - Uporaba kontrolnih zgoščenih vrednosti (npr. MD5, SHA-256) na način, da se za vsako datoteko ustvari (izračuna) kontrolna zgoščena vrednost, ki se preverja po prenosu, zgoščene vrednosti pa se hranijo na varnem mestu.

Ugotovitev 8.3:	Vsaj 150 uporabnikov je v letu 2023 dostopalo do ERP sistema in CRM rešitve v času, ko so bili v skladu s kadrovskimi evidencami na dopustu ali bolniško odsotni. V 10 primerih so do ERP sistema dostopale osebe, ki niso bile več v rednem delovnem razmerju s podjetjem.
Tveganja:	Nedovoljen dostop: Dostop do sistemov s strani odsotnih ali nezaposlenih oseb povečuje tveganje za neavtorizirano uporabo in morebitno zlorabo podatkov ter predstavlja pomembno varnostno tveganje za pojav incidentov. Pomanjkanje nadzora: Očitno je pomanjkanje ustreznega nadzora nad dostopom do sistemov in podatkov, kar predstavlja pomembno varnostno tveganje za pojav incidentov.
Ocena tveganja:	**VISOKO**
Priporočilo:	Revidirancu priporočamo, da čim prej preuči možnost izvedbe:

	- Revizije dostopnih pravic za vse uporabnike in blokiranje dostopa za tiste, ki ne delajo več za podjetje. - Rednega periodičnega izvajanja pregledovanja dostopnih pravic s strani lastnikov informacijskih sredstev oziroma procesov. - Uvedbe sistema za nadzor dostopa, ki preverja status uporabnikov (npr. ali so na dopustu, bolniški, porodniški, ipd.) preden jim je dovoljen dostop do sistema (integracija sistema za upravljanje človeških virov z ERP in CRM sistemom).

Ugotovitev 8.4:	Vodstvo podjetja je imenovalo pooblaščenca za varovanje informacij v letu 2019, ki je po osnovni izobrazbi prof. zgodovine. Ta oseba je tudi kontaktna oseba med podjetjem in nosilcem sektorja kritične infrastrukture ter tudi kontaktna oseba zavezanca po ZInfV. Ni pa podjetje imenovalo namestnika kontaktne osebe po ZInfV.
Tveganja:	Zaradi pomanjkanja ustreznega tehničnega znanja in razumevanja informacijsko komunikacijskih tehnologij oziroma neustrezne izobrazbe lahko pooblaščenec za varovanje informacij nepravilno upravlja varnostne ukrepe, kar pa lahko pripelje do varnostnih incidentov, ki imajo negativni vpliv na bistvene storitve. Pooblaščenec za varovanje informacij bi moral imeti ustrezno znanje in strokovne kompetence na področju informacijske varnosti. Ne imenovanje namestnika kontaktne osebe po ZInfV lahko pomeni tveganje za nedosegljivost kontaktne osebe v primeru potrebe po vzpostavitvi stika, ko je kontaktna oseba odsotna z delovnega mesta (letni dopust, bolniški stalež, ipd.).
Ocena tveganja:	**SREDNJE**
Priporočilo:	Revidirancu priporočamo, da preuči možnost, da podjetje zagotovi ustrezna usposabljanja za pooblaščenca za varovanje informacij, ki je tudi kontaktna oseba zavezanca po ZInfV, za pridobitev potrebnih znanj in kompetenc ali pa imenuje drugo ali dodatno ustrezno usposobljeno osebo s potrebnimi kompetencami za opravljanje nalog pooblaščenca za varovanje informacij (informacijsko varnost), da bi se zmanjšala tveganja in zagotovilo učinkovito upravljanje informacijske varnosti. Priporočljivo je tudi čimprejšnje imenovanje namestnika kontaktne osebe po ZInfV.

4.9 Povzetek ugotovitev

V okviru revizijskega pregleda je bila za dosego ciljev revizijskega pregleda pridobljena, pregledana in analizirana dokumentacija (interni dokumenti), katere predpisuje zakon in natančneje opredeljuje podzakonski predpis, opravljeni so bili razgovori s predstavniki revidiranca in drugimi zaposlenimi, pregledane so bile lokacije, kjer se izvajajo procesi, povezani z izvajanjem bistvenih storitev, revidirancu so bila postavljena pisna vprašanja, pridobljena in analizirana so bila dokazila o izvajanju predpisanih ukrepov in izvedeni so bili testi varnostnih ukrepov za varnost omrežij in informacijskih sistemov, ki vplivajo na neprekinjeno izvajanje bistvenih storitev.

Skupno je bilo v okviru revizijskega pregleda ugotovljenih 40 neskladij z Zakonom o informacijski varnosti, 5 ugotovitev pa je bilo ocenjenih z NIZKO stopnjo tveganja kar pomeni, da lahko gre za kršitve drugih predpisov ali neučinkovitost.

Za 20 ugotovitev je bila ocenjena SREDNJA stopnja tveganja, kar pomeni neskladnost z Zakonom o informacijski varnosti in zmerna varnostna tveganja za varnost omrežij in informacijskih sistemov revidiranca.

Za 20 ugotovitev je bila ocenjena VISOKA stopnja tveganja, ki za revidiranca pomenijo pomembna varnostna tveganja za varnost omrežij in informacijskih sistemov ter kršitev Zakona o informacijski varnosti.

Skupno je bilo tako podanih 45 priporočil za izboljšanje varnosti omrežij in informacijskih sistemov revidiranca oziroma za odpravo neskladij s predpisi ali izboljšanje učinkovitosti.

Za izvedbo priporočil, ki so ocenjena z VISOKO stopnjo tveganj, se revidirancu priporoča, da jih izvede čim prej oziroma v roku, ki ni daljši od 120 dni. Za izvedbo priporočil, ki so ocenjena s SREDNJO stopnjo tveganja, pa se revidirancu priporoča izvedba v roku, ki ni daljši od 240 dni.

5. Mnenje revizorja

Na podlagi izsledkov izvedenega revizijskega posla revizor ugotavlja, da so bili revizijski cilji v času izvedbe pregleda med 4. 9. 2023 in 22. 9. 2023 doseženi. Podjetje Gavioli, ki je zavezanec – izvajalec bistvenih storitev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23), v času izvedenega revizijskega posla **ni izpolnjeval vseh zahtev iz Zakona o informacijski varnosti** in Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23) za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji.

Podjetje Gavioli je odstopalo od meril, ki so bila uporabljena kot sodila pri revizijskem poslu in splošnih dobrih praks informacijske varnosti. Ugotovljene pomanjkljivosti, tveganja in priporočila za njihovo odpravo so navedeni v 4. poglavju tega poročila. Pri ugotovitvah, ki so bile ocenjene z najvišjo - VISOKO oceno tveganja, obstajajo pomembna varnostna tveganja za pojav incidentov oziroma dogodkov, ki lahko imajo dejanski negativen učinek na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov oziroma na neprekinjeno izvajanje bistvenih storitev. Ocenjeno tveganje pri vsaki ugotovitvi, ki je določeno kot SREDNJE in VISOKO pomeni tudi neskladje z Zakonom o informacijski varnosti. Tveganje, ki je posameznih ugotovitvah ocenjeno kot NIZKO, pa lahko predstavlja neskladnost z drugimi predpisi (npr. Zakon o varstvu osebnih podatkov, Splošna uredba o varstvu podatkov in Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih).

Revizor je na podlagi izsledkov opravljenega pregleda, ki je bil omejen na vnaprej določene postopke, ugotovil neskladja z Zakonom o informacijski varnosti in tako **ne more podati zagotovila, da je podjetje Gavioli d. o. o., kot izvajalec bistvenih storitev po Zakonu o informacijski varnosti, v celoti skladen z veljavnimi predpisi.**

V Kopru, 5. 10. 2023

Matjaž Mravljak
preizkušen revizor informacijskih sistemov

Priloga A: Seznam uporabljenih kratic

AD – aktivni imenik (angl. *Active Directory*)

CICS – sistem za nadzor informacij o strankah (angl. *Customer Information Control System*)

COBOL - kompiliran programski jezik (angl. *Common Business Oriented Language*)

CSIRT - skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov (angl. *Computer Security Incident Response Team*)

CVE - seznam javno razkritih varnostnih ranljivosti informacijskih sistemov (angl. *Common Vulnerabilities and Exposures*)

CVSS - okvir za ocenjevanje značilnosti in resnosti varnostnih ranljivosti programske opreme (angl. *Common Vulnerability Scoring System*)

CSV – tekstovna datoteka, ki uporablja vejice za ločevanje vrednosti. (angl. *Comma-separated values*)

DCS - razpršeni kontrolni sistem (angl. *Distributed Control System*)

DoS - zanikanja storitve, kot vrsta kibernetskega napada (angl. *Denial of Service*)

EDR – odkrivanje in odzivanje na končnih točkah (angl. *Endpoint Detection and Response*)

IDS – sistem za zaznavo vdorov (angl. *Intrusion Detection System*)

IPS – sistem za preprečevanje vdorov (angl. *Intrusion Prevention System*)

MFA – večfaktorska avtentifikacija (angl. *Multi-Factor Authentication*)

NOKI – Nacionalni načrt odzivanja na kibernetske incidente

OT VLAN - segmentirano omrežje znotraj industrijskega okolja, ki je namenjeno posebej za operativno tehnologijo (angl. *Operational Technology Virtual Local Area Networks*)

PLC - programirljivi logični krmilnik (angl. *Programmable Logic Controller*)

RTU - oddaljena terminalna enota (angl. *Remote Terminal Unit*)

SCADA - sistem za nadzor in pridobivanje podatkov (angl. *Supervisory Control and Data Acquisition*)

SIEM – upravljanje varnostnih informacij in dogodkov (angl. *Security Information and Event Management*)

VLAN - navidezno lokalno omrežije (angl. *Virtual Lan*)

VPN – navidezno zasebno omrežje (angl. *Virtual Private Network*)

XDR – razširjeno odkrivanje in odzivanje (angl. *Extended Detection and Response*)

Priloga B: Vprašalnik za revidiranca

I. Seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev
1. Ali ste izdelali dokument Seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev? 2. Ali ste v zgornjem dokumentu navedli sredstva znotraj sistema upravljanja varovanja informacij, od katerih je odvisno zagotavljanje bistvenih storitev? 3. Ali ste v dokumentu iz prvega vprašanja opredelili ključne, krmilne in nadzorne informacijske sisteme ter navedli njihove upravljavce? 4. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

II. Analiza obvladovanja tveganj
1. Ali ste izdelali dokument Analiza obvladovanja tveganj? 2. Ali ste v zgornjem dokumentu navedli uporabljene metodologije za izvedbo analize obvladovanja tveganj, ki mora biti primerljiva, verodostojna in ponovljiva ter v skladu s pravili stroke? 3. Ali ste v dokumentu iz prvega vprašanja navedli sredstva znotraj sistema upravljanja varovanja informacij in navedli upravljavce teh sredstev oziroma odgovorne osebe za ta sredstva? 4. Ali ste v dokumentu iz prvega vprašanja navedli možne groženje tem sredstvom? 5. Ali ste v dokumentu iz prvega vprašanja navedli ranljivosti sredstev, ki bi jih prepoznane grožnje lahko prizadele? 6. Ali ste v dokumentu iz prvega vprašanja ocenili vpliv uresničitve groženj na zaupnost, celovitost in razpoložljivost sredstev iz tretjega vprašanja zaradi ranljivosti? 7. Ali ste v dokumentu iz prvega vprašanja izvedli oceno vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube zaupnosti, celovitosti ali razpoložljivosti? 8. Ali ste v dokumentu iz prvega vprašanja ocenili verjetnosti, da pride do kršitev informacijske varnost? 9. Ali ste v dokumentu iz prvega vprašanja izvedli ovrednotenje ravni tveganj? 10. Ali ste v dokumentu iz prvega vprašanja določili in obrazložili sprejemljivo raven tveganj? 11. Ali ste v dokumentu iz prvega vprašanja navedli ukrepe za odpravo ali zmanjšanje tveganj nad sprejemljivo ravnjo? 12. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

III. Politika neprekinjenega poslovanja
1. Ali ste izdelali dokument Politika neprekinjenega poslovanja z načrtom njegovega upravljanja? 2. Ali ste v zgornjem dokumentu navedli cilje in načela za zagotavljanje neprekinjenega poslovanja oziroma neprekinjenega izvajanja bistvenih storitev, ob upoštevanju področnih posebnosti? 3. Ali ste izvedli popis poslovnih procesov? 4. Ali ste v dokumentu iz prvega vprašanja navedli postopke neprekinjenega poslovanja, ki se izdelajo na podlagi popisa poslovnih procesov?

5. Ali ste izvedli oceno vpliva na poslovanje, ki zajema najmanj navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije znotraj revidiranca in odpovedi storitev pogodbenih izvajalcev?
6. Ali ste v dokumentu iz prvega vprašanja določili minimalno raven poslovanja?
7. Ali ste v dokumentu iz prvega vprašanja navedli ukrepe za zagotavljanje neprekinjenega poslovanja, ki se izdelajo na podlagi ocene vpliva na poslovanje in minimalne ravni poslovanja?
8. Ali ste v dokumentu iz prvega vprašanja določili vloge in odgovornosti za izvajanje politike neprekinjenega poslovanja in njeno posodabljanje?
9. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

IV. Načrt obnovitve delovanja informacijskih sistemov

1. Ali ste izdelali dokument Načrt obnovitve delovanja informacijskih sistemov?
2. Ali ste v zgornjem dokumentu opisali odgovornosti in postopke za obnovitev delovanja ključnih, krmilnih in nadzornih informacijskih sistemov po dogodku, ki povzroči prekinitev njihovega delovanja?
3. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

IV. Načrt odzivanja na incidente

1. Ali ste izdelali dokument Načrt odzivanja na incidente?
2. Ali ste v zgornjem dokumentu opisali sistem za zaznavo incidentov informacijske varnosti?
3. Ali ste v zgornjem dokumentu opisali sistem za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo?
4. Ali ste v zgornjem dokumentu opisali postopke za odziv na incidente informacijske varnosti, obravnavo in analizo incidentov informacijske varnosti, vključno z evidentiranjem vseh odzivnih aktivnosti?
5. Ali ste v zgornjem dokumentu opisali odgovornosti oseb oziroma organizacijskih enot, ki jih je treba vključiti v aktivnosti iz prejšnjega vprašanja?
6. Ali ste v zgornjem dokumentu opisali postopke in odgovornosti za poročanje o incidentih znotraj revidiranca in zunaj revidiranca?
7. Ali ste v zgornjem dokumentu opisali protokol obveščanja nacionalnega CSIRT o incidentu informacijske varnosti?
8. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

V. Načrt varnostnih ukrepov in minimalni obseg ter vsebina varnostnih ukrepov

1. Ali ste izdelali dokument Načrt varnostnih ukrepov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežja in informacijskih sistemov?
2. Ali zagotavljate podporo vodstva revidiranca pri zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja?
3. Ali zagotavljate integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve?
4. Ali izvajate notranji pregled sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja najmanj enkrat letno in kadar so predlagane ali so

nastale bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov?

5. Ali izvajate potrebne ukrepe za upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito?
6. Ali zagotavljate ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov ter delov omrežja iz prejšnjega vprašanja?
7. Ali izvajate potrebne in primerne ukrepe za upravljanje prometa in komunikacij?
8. Ali ste opredelili varnostne zahteve za ključne dobavitelje?
9. Ali zagotavljate ustrezno in primerno fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi?
10. Ali imate določene in implementirane ustrezne ter primerne varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti?
11. Ali imate določene in implementirane ustrezne ter primerne mehanizme za preverjanje identitete uporabnikov?
12. Ali izvajate upravljanje in preprečevanje izrabe tehničnih ranljivosti?
13. Ali zagotavljate ustrezne ravni dostopnosti informacij in upravljanje pooblastil za dostop?
14. Ali zagotavljate zaščito pred zlonamerno programsko kodo?
15. Ali izvajate evidentiranje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev?
16. Ali izvajate ukrepe za zaznavanje poskusov vdorov in preprečevanje incidentov?
17. Ali je dokument iz prvega vprašanja podpisal zakoniti zastopnik revidiranca?

Priloga C: Načrt testiranj

I.	**Podpora vodstva revidiranca pri zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja izvajalca bistvenih storitev**
1.	Pregled letnega programa dela revidiranca za 2023 za področje informacijske varnosti.
2.	Pregled finančnih sredstev, ki jih je revidiranec v 2023 namenil za informacijsko varnost.
3.	Pregled zadnjih treh zaposlitev za področje informacijske varnosti in pregled zahtevanih kompetenc.

II.	**Integriteta kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve**
4.	Pregled ustreznosti opisov nalog delovnih mest za področje informacijske varnosti v aktu o sistemizaciji delovnih mest.
5.	Pregled zahtev glede predpisanih strokovnih referenc (izobrazba), usposobljenosti (certifikati) za delovna mesta na področju informacijske varnosti.
6.	Pregled izvajanja varnostnega preverjanja pred zaposlitvijo oseb za področje informacijske varnosti.
7.	Pregled izvajanja usposabljanj zaposlenih (pred in med zaposlitvijo) s področja informacijske varnosti.
8.	Pregled udeležbe na strokovnih usposabljanjih in izobraževanjih za ključen kader za področje informacijske varnosti.
9.	Pregled opredelitve nalog in odgovornosti v internih aktih v zvezi s koncem ali spremembo zaposlitve (odvzem pravic in službenih informacijskih sredstev uporabnikom).

III.	**Notranji pregled sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov**
10.	Pregled internih aktov glede predpisa presoje SUVI in SUNP v rednih časovnih presledkih in določitev nosilca/izvajalca.
11.	Pregled zapisov o izvajanju presoje SUVI in SUNP v rednih časovnih presledkih.

IV.	**Upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito**
1.	Pregled izvajanja nadzora nad omrežnimi napravami in njihovo programsko opremo.
2.	Pregled izvajanja varnostnega kopiranja konfiguracij ključnih omrežnih naprav.
3.	Pregled postopkov in odgovornosti upravljanja z omrežno opremo (izvajanje posodobitev omrežne opreme, dostopi do omrežne opreme in posegi).
4.	Pregled postopkov in odgovornosti upravljanja s spremembami (nadgradnje, posodobitve).
5.	Pregled ločenosti razvojnega, produkcijskega in testnega okolja.

6. Pregled izvajanja periodičnih varnostnih pregledov notranje in zunanje informacijske infrastrukture.
7. Pregled določenosti ključnih procesov in delovnih postopkov ter njihovih odgovornih oseb.

V. Ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev

8. Pregled treh dnevniških dogodkov starih med 5 in 6 mesecev o delovanju treh ključnih sistemov.
9. Ugotovitev in ogled lokacije hrambe zapisov dnevniških dogodkov.

VI. Upravljanje prometa in komunikacij

10. Pregled segmentacije omrežja (pregled logičnega in tehničnega diagrama omrežja).
11. Pregled beleženja omrežnega prometa na vhodno/izhodni točki.
12. Pregled odprtih vrat (angl. *Port*) in identifikacija potencialnih odprtih vrat, ki niso v uporabi.
13. Pregled tehnične dokumentacije in dejanskih osnovnih nastavitev na požarnih pregradah.
14. Pregled uporabljanih varnostnih mehanizmov na brezžičnih omrežjih.
15. Pregled vzpostavitve redundantna komunikacijske poti za bistvene (kritične) storitve.
16. Pregled postopkov in pogojev oddaljenega dostopa do omrežja.
17. Pregled pravil uporabe službene elektronske pošte.
18. Pregled pravil uporabe interneta.
19. Pregled izvajanja varnostnega kopiranja konfiguracij požarnih pregrad.
20. Pregled ustreznosti ločenosti poslovnega dela omrežja od tehničnega (OT) omrežja.

VII. Opredelitev varnostnih zahtev za ključne dobavitelje

21. Pregled minimalnih varnostnih zahtev, ki jih mora izpolnjevati dobavitelj.
22. Pregled seznamov osebja dobavitelja, ki ima dostop do informacijskih sistemov in informacij zavezanca, ter opis postopkov za odobritev in preklic odobritve za dostop osebja dobavitelja do informacijskih sistemov in informacij zavezanca.
23. Pregled načina dostopa do notranjih informacij in sredstev zavezanca s strani dobavitelja (odobritev za vsak posamezni dostop do omrežja, ki je časovno omejen).
24. Pregled določenosti postopkov ob pojavu varnostnega incidenta (obveščanje, poročanje, ukrepanje).
25. Pregled izvajanja dolžnega nadzorstva zavezanca nad ključnimi dobavitelji (način in obseg).

VIII. Fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi

26. Pregled ustreznosti (lokacije) prostora glede na možne naravne grožnje (poprava, porušitev, zalitje, ipd.).
27. Pregled ustreznosti aktivne in pasivne protivlomne zaščite (vrata, alarm, ključavnica, kamera).
28. Pregled ustreznosti proti požarne zaščite v podatkovnih centrih.

29. Pregled ustreznosti hlajenja prostora podatkovnega centra (senzor vlage in temperature - alarm, rezervna hladilna naprava).
30. Pregled zaščite ožičenja oziroma glavnih/ključnih komunikacijskih vodov.
31. Pregled izvajanja nadzora dostopa do podatkovnih centrov in vodenje evidence vstopov (dvo-faktorska avtentifikacije pri vstopu (ključ+kartica, kartica+koda)).

IX.	Varnostni mehanizmi v posamezni aplikativni programski opremi za izvajanje dejavnosti

32. Pregled določenosti in izvajanja intenzivnega testiranje aplikacije pri dobavitelju.
33. Pregled produkcijskih aplikacij glede vsebnosti potrjenih izvršnih kod (ne razvojnih).
34. Pregled izvajanja statičnih in/ali dinamičnih pregledov izvorne kode aplikacij.
35. Pregled zagotavljanja revizijske sledi v posamezni aplikaciji.
36. Uporaba šifriranja pri pretoku podatkov.

X.	Preverjanje identitete uporabnikov

37. Pregled izvajanja politike močnih gesel.
38. Pregled določenosti omejitev števila neuspešnih prijav uporabnikov v omrežje.
39. Pregled izvajanja več faktorskega postopka prijave/preverjanja identitete uporabnika.
40. Pregled izvajanja beleženja uspešnih in neuspešnih prijav v sistem.

XI.	Upravljanje in preprečevanje izrabe tehničnih ranljivosti

41. Pregled izvajanja predpisanega/priporočenega posodabljanja programske opreme v informacijskem sistemu.
42. Pregled načina spremljanja varnostnih obvestil in opozoril o pojavu ranljivosti ničelnega dne.
43. Pregled izvajanja (redne) revizije tehničnih ranljivosti (skeniranje) strojne in programske opreme v informacijskem sistemu.

XII.	Zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop

44. Pregled seznama/matrike uporabniških imen in pravic.
45. Pregled postopka odobritve uporabe informacijskega sredstva uporabnikom.
46. Pregled postopkov za izvedbo takojšnje blokade pravic dostopa uporabnikov, ki so zapustili organizacijo ali zamenjali delovno mesto.
47. Pregled izvajanja postopkov rednega pregledovanja pravic dostopa z lastniki informacijskih virov (sredstev).
48. Pregled določenosti politike dostopa do informacij različnih stopenj zaupnosti po funkciji in/ali delovnih mestih (potreba po vedenju).
49. Pregled posebnih postopkov za dodeljevanje in odvzem administratorskih pravic.
50. Pregled postopka dodelitve, spremembe in izbrisa uporabnika.
51. Pregled omejenosti dostopa do podatkov, sistemskih funkcij in aplikacij v skladu s politiko.
52. Pregled uporabe kriptografskih rešitev (šifriranje) in zgoščenih vrednosti pri hrambi ključnih/pomembnih informacij.
53. Pregled osnovnih nastavitev domenske varnosti uporabniških računov v AD.

XIII. Zaščita pred zlonamerno programsko kodo
54. Pregled implementacije proti-virusne/EDR/XDR rešitve na strežnikih, delovnih postajah in prenosnih informacijskih napravah. 55. Pregled izvajanja politike glede posodabljanja programske opreme za zaznavo in odpravo škodljive programske opreme. 56. Pregled izvajanja politike onemogočanja snemanja, nameščanja in uporabe neodobrene programske opreme. 57. Pregled implementacije preverjanja datotek na magnetnih ali optičnih medijih in datotek, prejetih prek omrežij, preden se uporabijo, glede okuženosti s škodljivo programsko opremo. 58. Pregled izvajanja varnostnega preverjanja priponk elektronske pošte in snetih datotek, preden se uporabijo, na poštnih strežnikih ter namiznih računalnikih. 59. Pregled izvajanja preverjanja spletnih strani glede vsebovanja škodljive programske opreme. 60. Pregled postopka v primeru okužbe ali suma okužbe s škodljivo programsko opremo.

XIV. Evidentiranje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev
61. Pregled beleženja zagonov in ustavitev ključnih sistemov. 62. Pregled beleženja sistemskih napak in izvedenih popravnih ukrepov. 63. Pregled beleženja dostopov do kritičnih registrov in aplikacij. 64. Pregled beleženja uspešnih in zavrnjenih poskusov dostopa. 65. Pregled beleženja pošiljateljev in prejemnikov poštnega prometa. 66. Pregled beleženja prejemnikov in pošiljateljev internetnega prometa. 67. Pregled vzdrževanja ključnih, krmilnih in nadzornih informacijskih sistemov ter pripadajočih podatkov naročnika.

XV. Zaznavanje poskusov vdorov in preprečevanje incidentov
68. Pregled uporabe požarnih pregrad ustreznih konfiguracij (pravila, vrata). 69. Pregled uporabe IDS in IPS. 70. Pregled uporabe SIEM. 71. Pregled izvajanja funkcije SOC. 72. Pregled politike/postopkov za pregledovanje in obravnavo alarmov v SIEM. 73. Pregled števila in obsega varnostih dogodkov v zadnjem letu. 74. Pregled ugotovljenih varnostnih pomanjkljivosti v zadnjem letu. 75. Pregled izvajanja varnostih pregledov in izvedenih vdornih testov (analiza poročil).

XVI. Politika neprekinjenega poslovanja z načrtom njenega upravljanja
76. Pregled virov za neprekinjeno napajanje ključnih lokacij (UPS, dizel agregat). 77. Pregled virov za neprekinjeno hlajenje ključnih lokacij (podvojena arhitektura klimatskih naprav). 78. Pregled zagotavljanja redundance delovanja ključnih sistemov. 79. Pregled prenosa zahtev za neprekinjeno poslovanje v pogodbe s ključnimi dobavitelji. 80. Pregled izvajanja testiranja načrta neprekinjenega poslovanja v zadnjem letu. 81. Pregled hrambe (lokacij) načrtov neprekinjenega poslovanja.

XVII. Načrt obnovitve delovanja informacijskih sistemov
82. Pregled dokumentiranih operativnih postopkov obnovitve delovanja posameznih ključnih sistemov. 83. Pregled načina in oblike hrambe varnostnih kopij, potrebnih za obnovo ključnih sistemov po katastrofi. 84. Pregled prenosa zahtev za obnovitev delovanja informacijskih sistemov v pogodbe s ključnimi dobavitelji. 85. Pregled izvajanja periodičnega preverjanja kakovosti varnostih kopij (restavracija).

XVIII. Odzivanje na incidente informacijske varnosti
86. Pregled vlog, odgovornosti in zadolžitev posameznih deležnikov pri odzivanju na incidente informacijske varnosti. 87. Pregled zadnjih treh poročil o incidentih informacijske varnosti (upoštevanje NOKI).

Priloga D: Listina o poslu

Naročnik: Podjetje Gavioli d. o. o. , Industrijska cesta 10, Izola, matična številka 111111, davčna številka 222222, katerega zastopa direktor Martin Peter

in

Izvajalec: Matjaž Mravljak s. p., Obala 10, Koper, matična številka 111111, davčna številka 222222, preskušeni revizor informacijskih sistemov

skleneta in dogovorita

L I S T I N O O P O S L U

1. Naročnik in izvajalec uvodoma ugotavljata, da je naročnik izvajalec bistvenih storitev - zavezanec iz Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23, v nadaljevanju: ZInfV).

2. S to listino se naročnik in izvajalec podrobneje dogovorita o strokovnih podrobnostih, medsebojnih razmerjih in načinu izvedbe pregleda, kot tipa dajanja zagotovil oziroma revizijskega posla, ki je predmet te listine o poslu.

3. Cilj revizijskega posla je opraviti pregled in podati zagotovilo, da naročnik – izvajalec bistvenih storitev, v času izvajanja pregleda, izpolnjuje zahteve z ZInfV in Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. , v nadaljevanju: uredba) na način in v obsegu, kot je določeno v nadaljevanju te listine o poslu.

4. Pregled bo opravil izvajalec Matjaž Mravljak, CIS-M, CIS-A in preskušeni revizor informacijskih sistemov, kot neodvisen in nepristranski strokovnjak na ravni posla, funkcije ali organizacije, osvobojen od okoliščin, ki ogrožajo nepristranskost in ima vse potrebne veščine in strokovno znanje ter je ustrezno strokovno usposobljen za izvedbo pregleda, ki je predmet te listine o poslu. Pri izvedbi posla se bo izvajalec ravnal s potrebno poklicno skrbnostjo in z upoštevanjem veljavnih strokovnih, poklicnih in etičnih standardov za izvedbo pregleda.

5. V okviru izvedbe pregleda, bo izvajalec opravil pregled naročnikovega načrta varnostnih ukrepov (in drugih predpisanih dokumentov v povezavi z načrtom varnostnih ukrepov) ter implementacije in učinkovitosti izvajanja predpisanih minimalnih varnostnih ukrepov (kontrolnih postopkov), povezanih z izvajanjem bistvenih storitev iz 6. točke prvega odstavka 12. člena ZInfV oziroma 9. in 11. člena uredbe in podati zagotovilo o naročnikovi skladnosti z ZInfV in uredbo v obsegu, kot je določeno in opredeljeno v nadaljevanju.

6. Pregled ne bo obsegal pregleda izvajanja predpisanih ukrepov (kontrol) pri pogodbenih izvajalcih naročnika.

7. Izvajalec bo za potrebe izvedbe pregleda v skladu z Zakonom o revidiranju (Uradni list RS, št. 65/08, 63/13 – ZS-K, 84/18 in 115/21) ter Okvirjem strokovnega ravnanja za dajanje zagotovil/revidiranja informacijskih sistemov (ITAF V3.), ovrednotenje in oblikovanje sklepa uporabil naslednja merila oziroma sodila:
- relevantne določbe Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2 in 18/23 – ZDU-1O) in
- relevantne določbe Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23).

8. Izvajalec bo pregled opravil v trajanju največ petnajst delovnih dni, med 09.00 in 15.00, s pričetkom 4. 9. 2023 ob 09.00 na sedežu naročnika in sicer v dveh delih.
   V prvem delu bo izvajalec na sedežu podjetja v trajanju največ dveh delovnih dni opravil pregled dokumentacije in ocenil tveganja ter na podlagi ugotovitev ustrezno dopolnil Načrt revizijskega posla z načrtom pregleda kontrol in ukrepov.
   V drugem delu bo izvajalec na sedežu naročnika in po potrebi na drugem kraju opravil pregled dokumentacije, razgovore s skrbniki in ključnimi uporabniki in pregled ter testiranje kontrol in ukrepov.

9. Naročnik se obvezuje, da bo za potrebe izvedbe pregleda:
- na sedežu naročnika izvajalcu omogočil uporabo primernega prostora za izvedbo pregleda;
- dal izvajalcu na razpolago dostop do vseh svojih internih dokumentov, ki so povezani s sistemom upravljanja in varovanja informacij oziroma izvajanja bistvenih storitev pri naročniku oziroma so relevantni za izvedbo pregleda;
- izvajalcu omogočil dostop do prostorov, kjer so nameščeni ključni, krmilni in nadzorni informacijski sistemi, deli omrežja in pripadajoči podatki, ki so bistvenega pomena za delovanje bistvenih storitev naročnika oziroma so relevantni za izvedbo pregleda;
- določil osebo, ki bo na razpolago izvajalcu v času izvedbe pregleda, za potrebe podaje morebitnih dodatnih pojasnil;
- izvajalcu omogočil izvedbo razgovorov z določenimi zaposlenimi naročnika, ki bi bili potrebni za izvedbo pregleda.

10. Izvajalec Matjaž Mravljak, telefonska številka 031/456-234, elektronska pošta matjaz.mravljak@pris.com, bo z naročnikom komuniciral preko osebe Franci Martin, in sicer preko mobilnega telefona 041/222-333 in elektronske pošte franci.martin@gavioli.com.

11. Naročnik je odgovoren za avtentičnost, celovitost in veljavnost posredovanih internih aktov in drugih informacij izvajalcu, prav tako je naročnik odgovoren za točnost in popolnost podanih izjav in pojasnil njegovih zaposlenih.

12. Izvajalec ne prevzema nobene odgovornosti za ugotovitve oziroma podana zagotovila, ki so bila sprejeta na podlagi nepopolnih, necelovitih, neveljavnih ali neavtentičnih posredovanih internih dokumentov oziroma neresničnih, nepopolnih ali zavajajočih izjav naročnikovih zaposlenih, ki bi bile podane v okviru izvedenega pregleda.

13. V primeru ugotovljenih hujših nepravilnosti ali okoliščin, ki ogrožajo varnost omrežij ali informacijskih sistemov naročnika, bo izvajalec takoj oziroma brez nepotrebnega odlašanja obvestil poslovodstvo naročnika.

14. Izvajalec bo pridobljene informacije, ki predstavljajo poslovno skrivnost naročnika ali tajne podatke obravnaval in varoval v skladu z Zakonom o poslovni skrivnosti (Uradni list RS, št. 22/19) oziroma Zakonom o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O).

15. Plačilo za opravljen posel znaša 8.200,00 EUR (brez DDV). Naročnik plačilo izvede z nakazilom na poslovni račun izvajalca najkasneje osem delovnih dni po izročitvi zaključnega poročila.

16. Izvajalec bo najkasneje pet delovnih dni po končanem pregledu osnutek poročila predstavil naročniku in z njim uskladil ugotovitve. V roku petih delovnih dni po predstavitvi osnutka poročila naročniku bo izvajalec poslovodnemu organu naročnika oziroma predsedniku uprave v zaprti kuverti, v dveh izvodih, dostavil pisno mnenje z ugotovitvami oziroma končno revizijsko poročilo in ga na željo naročnika tudi predstavil.

17. Naročnik in izvajalec si bosta prizadevala, da bosta morebitne spore v zvezi s to listino reševala sporazumno, v kolikor jima to ne bi uspelo, je za reševanje sporov pristojno sodišče v Ljubljani.

18. Ta listina je sklenjena in veljavna, ko jo podpišeta naročnik in izvajalec in jo potrdi poslovodni organ naročnika.

19. Ta listina je sestavljena v treh izvodih, od katerih prejme naročnik dva podpisana izvoda, izvajalec pa en podpisan izvod.

Naročnik:

direktor Martin Peter _____

Datum: _____

Izvajalec:

Matjaž Mravljak, PRIS _____

Datum: _____

Potrditev listine o poslu na seji uprave dne _____, številka sklepa: _____ .

Priloga E: Načrt revizijskega posla

Številka: 386-29/2023

Datum: 3. 10. 2023

Načrt revizijskega posla

Namen tega dokumenta: Podrobneje opredeliti posamezne vidike revizijskega posla: področje izvedbe revizijskega posla, cilje in podcilje, vrsto načrtovanih postopkov, obseg dela, uporabljene standarde oziroma sodila, roke za izvedbo, potrebe vire za izvedbo, omejitve pri delovanju, način pridobivanja revizijskih dokazov, ocenjevanje tveganj, komunikacijo z naročnikom in poročanje naročniku.

Tip revizijskega posla: PREGLED

Naziv revidiranca - naročnika: Podjetje Gavioli d. o. o. , Industrijska cesta 10, Izola, matična številka 111111, davčna številka 222222, katerega zastopa direktor Martin Peter.

Naziv revizije: Pregled skladnosti naročnika – izvajalca bistvenih storitev z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2 in 18/23 – ZDU-1O, v nadaljevanju: ZInfV) in Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23, v nadaljevanju: uredba).

Izvajalec revizije: Matjaž Mravljak s. p., Obala 10, Koper, matična številka 111111, davčna številka 222222, preskušeni revizor informacijskih sistemov.

---

1. **Področje revizijskega posla:** Pregled ustreznosti in izvajanja načrta varnostnih ukrepov naročnika - izvajalca bistvenih storitev po ZInfV v obsegu, kot je določen v 5. točki Listine o poslu.

2. **Cilj revizijskega posla:** Opraviti pregled in podati zagotovilo, da naročnik – izvajalec bistvenih storitev, v času izvajanja pregleda, izpolnjuje zahteve z ZInfV in uredbe na način in v obsegu, kot je določeno v listini o poslu. V okviru navedenega cilja se bo tudi preverila implementacija in učinkovitost izvajanja predpisanih minimalnih varnostnih ukrepov (kontrolnih postopkov), povezanih z izvajanjem bistvenih storitev iz 6. točke prvega odstavka 12. člena ZInfV oziroma 9. in 11. člena uredbe.

3. Obseg revizijskega posla in način dela: Revizijski posel (pregled) bo obsegal:

A. Spoznavanje informacijskega okolja naročnika in tistih informacijskih rešitev, ki so pomembne za izvajanje bistvenih storitev s ciljem ugotoviti:

- kateri so ključni procesi, ki izvajajo bistvene storitve in njihova kritičnost z vidika zagotavljanja razpoložljivosti, celovitosti in zaupnosti;

- katere informacijske rešitve naročnika so pomembne za izvajanje bistvenih storitev oziroma podpirajo ključne procese (programska oprema, aplikacije, operacijski sistemi, zaščita pred zlonamerno programsko kodo);

- na kateri tehnološki infrastrukturi delujejo (stikala, usmerjevalniki, strežniki, požarne pregrade, ipd.);

- podatke o javnem naslovnem prostoru zavezanca;

- kako je segmentirano omrežje naročnika (poslovno omrežje, tehnološko omrežje)

in

- kako je organizirana informacijska podpora naročnika.

B. Pregled obvezne dokumentacije naročnika, povezane s sistemom upravljanja varovanja informacij iz Zakona o informacijski varnosti, ki podpira izvajanje bistvenih storitev in sicer:

- analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj;

- politiko neprekinjenega poslovanja z načrtom njenega upravljanja;

- seznam naročnikovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev;

- načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje;

- načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT in

- načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo področne posebnosti.

C. Ocena tveganj in priprava podrobnega načrta pregleda kontrol in ukrepov na lokaciji. Revizor bo po pregledu ocene tveganj naročnika ustrezno dopolnil načrt revizijskega posla z načrtom pregleda in preskušanja kontrol ter varnostnih ukrepov, pri pripravi načrta pa je revizor inicialno upošteval naslednja tveganja:

- tveganje, da naročnik ni določil odgovornih in zadolženih oseb za področje SUVI;
- tveganje, da tehnične kontrole niso skladne s politiko naročnika;

- tveganje, da naročnik ni prepoznal predpisov, ki ga zavezujejo kot izvajalca bistvenih storitev in ni pripravil predpisane dokumentacije ali pa ta dokumentacija ni sklada s predpisi;
- tveganje, da vodstvo naročnika nima ustreznega odnosa do informacijske varnosti in ne zagotavlja integritete kadrov pred, med in po prenehanju zaposlitve;
- tveganje, da naročnik ne zagotavlja revizijskih sledi oziroma ohranjanja dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja za obdobje najmanj šestih mesecev;
- tveganje, da se ključni procesi ne izvajajo skladno s sprejetimi politikami oziroma internimi akti naročnika in
- tveganje, da naročnikovo osebje ni seznanjeno s politikami ali odgovorne/zadolžene osebe niso seznanjene s predpisi in internimi akti s področja informacijske varnosti.

D. Podrobnejši pregled skladnosti Načrta varnostnih ukrepov s predpisi, za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki podpirajo bistvene storitve ter pridobitev in pregled naslednjih informacij oziroma dokumentov:

- letni načrt zavezanca za preteklo in prihodnje leto;

- organizacijsko shema zavezanca;

- seznam zaposlenih z delovnim mestom in opisom nalog ter zahtev (referenc) za zasedbo delovnega mesta (povezanih z IT področjem);

- matrika vlog in odgovornosti na področju varovanja informacij pri naročniku;

- poročila o morebitnih predhodnih pregledih (vodstveni pregled, revizija Računskega sodišča, notranja revizija, interni nadzor, presoja po standardu, ipd.);

- oceno vpliva na poslovanje (BIA analiza);

- seznam morebitnih certifikatov (npr. ISO);

- skupno varnostno politiko in/ali varnostne politike za posamezna področja;

- shemo IT-infrastrukture (logični in fizični diagram omrežja);

- podatke o naslovnem prostoru zavezanca;

- seznam programske in strojne opreme;

- seznam IT storitev, ki ji zavezanec najema pri zunanjih izvajalcih;

- seznam zunanjih izvajalcev in pogodbe ter dogovore o ravni storitve – SLA;

- poročila o izvedenih varnostnih pregledih informacijsko-komunikacijske infrastrukture;

- seznam obravnavanih incidentov informacijske varnosti za obdobje od 1. 1. 2022 do 1. 6. 2023 in

- poročila o obravnavi incidentov informacijske varnosti iz prejšnje alineje.

E. Pregled izvajanja Načrta varnostnih ukrepov, za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov z ogledom dejanskega stanja, izvedbo vzorčenja ter testiranj učinkovitosti izvajanja kontrolnih postopkov in sicer:

- pregled izvajanja usposabljanja/ozaveščanja zaposlenih s področja informacijske varnosti med zaposlitvijo;

- izvedba pregleda postopkov upravljanja s spremembami (prepoznavanje in beleženje pomembnih sprememb, testiranje sprememb, postopek za odobritev sprememb, rezervni postopki);

- izvedba pregleda postopkov upravljanja in obvladovanja tehničnih ranljivosti (vloge in odgovornosti, informacijska sredstva, testiranje);

- preveritev ustreznosti dolžine, strukture in časovne zamenjave gesel navadnih uporabniških računov in privilegiranih uporabniških računov;

- v aktivnem imeniku identificirati morebitni obstoj neaktivnih ali neevidentiranih uporabniških računov;

- opazovanje izvajanja procesa dodeljevanja, spremembe ali odvzema dostopnih pravic in pooblastil navadnih in privilegiranih uporabniških računov;

- pregled ustreznosti in učinkovitosti zaščite pred zlonamerno in prenosno kodo (licenčna programska oprema, posodabljanje programskih rešitev, obveščanje o anomalijah);

- pregled varnostnih mehanizmov v posamezni aplikativni programski opremi, ki se uporablja za izvajanje bistvenih storitev naročnika (varnostno testiranje, način prijave, dnevniki dogodkov);

- izvedba pasivnega skeniranja naslovnega prostora zavezanca, kjer se izvajajo bistvene storitve, z orodjem shodan.io (pridobiti podatke o obstoju kritičnih tehničnih ranljivosti naročnikovih ključnih, krmilnih in nadzornih informacijskih sistemov). Glede na dobljene rezultate in po potrebi s predhodnim dogovorom, izvedba še aktivnega skeniranja z orodjem nmap za potrditev rezultatov testa.

Za kritične tehnične ranljivosti se bodo smatrale vse tiste, katerih (skupna) ocena bo po matriki CVSS presegala oceno 7,9;

- izvedba pregleda izpostavljenosti uporabniških imen, gesel in poštnih naslovov na spletu zaposlenih pri zavezancu z uporabo orodja Luminar;

- pridobitev izpisa treh dnevniških zapisov (dogodkov) o delovanju določenih ključih sistemov za določena obdobja, od tega en izpis za obdobje 6 mesecev od dneva odvzema vzorca;

- ogled lokacij in preveritev ustreznosti izvajanja predpisanih ukrepov fizičnega in tehničnega varovanja dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi;

- izvedba morebitnih drugih preizkusov delovanja in učinkovitosti delovanja kontrolnih postopkov, po predhodni seznanitvi naročnika, za namen pridobitve zadostnih in ustreznih revizijskih dokazov za izrek mnenja.

4. Omejitve pri izvedbi revizijskega posla:

Revizor ne bo opravil pregleda izvajanja predpisanih ukrepov (kontrol) pri pogodbenih izvajalcih naročnika. Omejitve pri izvedbi pregleda, skladno z Listino o poslu, bo revizor ustrezno navedel in pojasnil v poročilu.

5. Pomembnejša tveganja revidiranega področja in revizijska tveganja:

Za potrebe izvedbe revizijskega posla je revizor ocenil revizijska tveganja pri odkrivanju in pri kontroliranju na podlagi ugotovitev že opravljenih enakih ali podobnih revizij pri zavezancih – izvajalcih bistvenih storitev, kjer so bile ugotovljena različna neskladja oziroma odstopanja od zakonskih zahtev pri določanju vsebine in obsega varnostnih ukrepov ter samem izvajanju varnostnih ukrepov (kontrol) ter na podlagi dejstva, da ni bila predhodno pridobljena ocena tveganja naročnika, na podlagi katere bi revizor lahko ocenil primernost in zanesljivosti ocene tveganja. Revizijsko tveganje se je ocenilo po tri stopenjski lestvici: nizko tveganje, srednje tveganje in visoko tveganje.
Revizor je na podlagi dobrih praks upravljanja informacijskih sistemov in po osnovnih sestavinah upravljanja COBIT prepoznal tveganja revidiranega področja.

Revizijska tveganja: Revizor ocenjuje, da obstaja visoko tveganje pri kontroliranju saj ni mogoče definirati (splošnih) notranjih kontrol in oceniti uspešnosti in ustreznosti delovanja notranjih kontrol. Revizor ocenjuje, da obstaja visoko tveganje pri delovanju, ker bi morebitni učinki napak ali odsotnost ustreznih kontrol v neustrezno zaščitenem informacijskem sistemu naročnika lahko bistveno vplivali na nemoteno izvajanje bistvenih storitev naročnika.

Tveganje revidiranega področja: Revizor prepoznava naslednja tveganja pri naročniku, ki so bila uporabljena kot izhodišče za načrtovanje in pripravo načrta revizije (COBIT):
- *Organizacijska struktura*: tveganje, da naročnik ni določil odgovornih in zadolženih oseb za področje SUVI in SUNP;
- *Storitve, infrastruktura in aplikacije*: tveganje, da tehnične kontrole niso skladne s politiko naročnika;
- *Politike, postopki in pristopi*: tveganje, da naročnik ni prepoznal predpisov, ki ga zavezujejo kot izvajalca bistvenih storitev in ni pripravil predpisane dokumentacije ali pa ta dokumentacija ni skladna s predpisi;
- *Kultura, etika in vedenje*: tveganje, da vodstvo naročnika nima ustreznega odnosa do informacijske varnosti in ne zagotavlja integritete kadrov pred, med in po zaposlitvi;

- *Informacije*: tveganje, da naročnik ne zagotavlja revizijskih sledi oziroma ohranjanja dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja za obdobje najmanj šestih mesecev;
- *Procesi*: tveganje, da se ključni procesi ne izvajajo skladno s sprejetimi politikami oziroma internimi akti naročnika.
- *Ljudje, spretnosti in kompetence*: tveganje, da naročnikovo osebje ni seznanjeno s politikami ali odgovorne/zadolžene osebe niso seznanjene s predpisi in internimi akti s področja informacijske varnosti.

6. Izvedba testiranj in vzorčenja: Revizor bo za potrebe izvedbe testiranj delovanja določenih kontrolnih postopkov in dosego revizijskih ciljev izvedel vzorčenje po ne-statistični metodi vzorčenja po lastni presoji, glede na pridobitev zadostnih, zanesljivih in ustreznih dokazov o delovanju kontrolnih postopkov, v povezavi s tveganjem napačnega sprejetja in tveganjem napačne zavrnitve.

7. Sodila, ki bodo uporabljena pri izvajanju revizijskega posla: Za potrebe pregleda bodo uporabljena naslednja sodila:
Zakon o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2 in 18/23 – ZDU-1O),

Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23),

Standard ISO/IEC 27002:2013 in sicer naslednja poglavja z relevantnimi kontrolami podpoglavij v povezavo z zahtevami iz 9. in 11. člena Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev:

- A.7.1.2, A.7.2 in A.7.3;
- A.8.1;
- A.9.1, A.9.2 in A.9.4;
- A.11.1 in A.11.2;
- A.12.1, A.12.2, A.12.3, A.12.4, A.12.5 in A.12.6;
- A.13.1;
- A.14.1 in A.14.2;
- A.15.1 in A.15.2;
- A.16.1 in
- A 17.1.

8. Časovni razpored revizije in roki za dokončanje posameznih faz izvedbe revizije (načrtovanje, izvajanje, poročanje): Za potrebe pregleda je načrtovan naslednji urnik opravil:

- do 1. 8. 2023 podpis listine o poslu in potrditev listine o poslu na seji uprave naročnika;
- do 15. 8. 2023 potrditev načrta revizijskega posla;
- 28. 8. 2023 seznanitev kontaktne osebe naročnika (Franci Martin) z bistvenimi deli načrta revizije;

- 4. 9. 2023 in 5. 9. 2023, med 09.00 in 15.00, pregled dokumentacije na sedežu naročnika in izvedba ocene tveganj ter dopolnitev Načrta revizijskega posla z načrtom pregleda kontrol in ukrepov (seznanitev kontaktne osebe naročnika);
- od 8. 9. 2023 do 22. 9. 2023, med 09.00 in 15.00, izvajanje pregleda na sedežu naročnika in po potrebi na drugem kraju;
- 29. 9. 2023 predstavitev osnutka revizijskega poročila naročniku in uskladitev vsebine;
- 6. 10. 2023 dostava revizijskega poročila poslovodnemu organu naročnika v dveh izvodih v zaprti kuverti. Revizor bo na predhodno izraženo željo naročnika revizijsko poročilo naročniku oziroma poslovodnemu organu tudi osebno predstavil na dan dostave revizijskega poročila;
- 18. 10. 2023 izdaja računa za revizijski posel;
- 30. 10. 2023 rok za plačilo računa revizijskega posla, v skladu z določbami listine o poslu.

9. Spremembe in dopolnitve načrta revizijskega posla:

- Po pregledu dokumentacije in oceni tveganj bo revizor Načrt revizijskega posla ustrezno dopolnil s podrobnim načrtom pregleda kontrol in ukrepov.
- Zaradi nastopa nepredvidenih dogodkov ali okoliščin lahko revizor ustrezno dopolni ali spremeni načrt izvajanja revizije, da bi se dosegel revizijski cilj.
- Z vsako morebitno bistveno ali pomembno spremembo ali dopolnitvijo načrta revizije bo revizor brez odlašanja seznanil kontaktno osebo naročnika.

10. Prejemniki revizijskih izsledkov: Za potrebe pregleda bo revizor:

- Z bistvenimi deli načrta revizije seznanil kontaktno osebo naročnika in sicer Francija Martina, preko elektronske pošte franci.martin@gavioli.com.
- Osnutek revizijskega poročila bo predstavljen na sestanku kontaktni osebi naročnika in drugim osebam, ki jih bo določil ali pooblastil naročnik. En izvod osnutka revizijskega poročila bo na sestanku izročen pooblaščencu naročnika.
- Končno revizijsko poročilo bo v zaprti kuverti in v dveh izvodih dostavljeno poslovodnemu organu naročnika, naslovljeno na predsednika uprave.