ZAVOD ZA SIGURNOST
INFORMACIJSKIH SUSTAVA

Prilog C – Katalog kontrola

Verzija: 1.0

Sadržaj

Uvod

Prilog C - Katalog kontrola sadrži kontrole za mjere i podskupove mjera upravljanja kibernetičkim sigurnosnim rizicima propisanih Prilogom II. *„Mjere upravljanja kibernetičkim sigurnosnim rizicima“* Uredbe o kibernetičkoj sigurnosti („Narodne novine“, broj: 135/24, u daljnjem tekstu Uredba).

U kontekstu ovog dokumenta, kontrolom se smatra organizirani skup politika, procedura, procesa ili tehničkih mehanizama koji imaju za cilj upravljanje i smanjenje rizika u području kibernetičke sigurnosti kroz prevenciju, detekciju ili odgovor na potencijalne prijetnje.

Kontrole imaju različite svrhe, ovisno o njihovoj vrsti i funkciji unutar pravila za kibernetičku sigurnost. Glavne svrhe uključuju:

1. **Ublažavanje rizika**: Kontrole umanjuju vjerojatnost ili utjecaj rizika u području kibernetičke sigurnosti i otpornosti, osiguravajući da su potencijalne ranjivosti i prijetnje prepoznate i upravljane.
2. **Zaštita imovine**: Kontrole štite imovinu subjekta (podatke, sustave, fizičku opremu itd.) pružajući slojeve obrane, sprječavajući neovlašteni pristup i osiguravajući povjerljivost osjetljivih informacija.
3. **Uspostava odgovornosti**: Dodjelom specifičnih uloga, odgovornosti i procedura, kontrole promoviraju odgovornost, osiguravajući da pojedinci razumiju svoje odgovornosti u održavanju kibernetičke sigurnosti.
4. **Povećanje svijesti i obuke**: Određene kontrole usmjerene su na podizanje svijesti o kibernetičkoj sigurnosti među zaposlenicima i drugim dionicima koji imaju aktivan pristup, informacijskoj i drugoj imovini, osiguravajući da razumiju potencijalne prijetnje i slijede najbolje sigurnosne prakse.
5. **Praćenje i detekcija**: Kontrole omogućuju subjektima kontinuirano praćenje sustava, rano otkrivanje potencijalnih incidenata i pravovremeno reagiranje, čime se smanjuje vjerojatnost ozbiljnije štete.

Kontrole predstavljaju osnovu strategije kibernetičke sigurnosti osiguravajući da su potencijalni rizici sustavno upravljani, čime doprinose otpornosti subjekta na kibernetičke prijetnje.

Postupak ocjenjivanja

Sukladno kategorizaciji subjekata tijelima je dodijeljena razina kibernetičke sigurnosti koju moraju postići – Osnovna, Srednja i Napredna. Svaka razina predstavlja povećanu složenost i dubinu u implementaciji kontrola kibernetičke sigurnosti. Ova struktura omogućava subjektima razumijevanje vlastite pozicije u području kibernetičke sigurnosti te pomaže u identificiranju područja za poboljšanje, kao i usklađenost s definiranim minimalnim uvjetima koje subjekt mora zadovoljiti.

Ocjenjivanje kontrola provodi se prema definiranim kriterijima koji osiguravaju objektivnost i dosljednost u procjeni razine ispunjenja zahtjeva kontrole. Svaka kontrola ocjenjuje se u rasponu od 1 do 5, pri čemu niža ocjena označava nedostatnu primjenu, dok viša ocjena ukazuje na potpunu usklađenost s definiranim zahtjevima. Ocjena se utvrđuje uzimajući u obzir relevantne aspekte primjene kontrole, uključujući dokumentirane postupke i njihovu provedbu u praksi. Subjekt može provoditi samoprocjenu kontrola temeljem ovih kriterija. Ovisno o zahtijevanoj razini kibernetičke sigurnosti, subjekt mora zadovoljiti propisane minimalne bodovne pragove ocjenjivanja za pojedinu kontrolu. Postupak ocjenjivanja kontrola odvija se sukladno sljedećim smjernicama za ocjenjivanje:

Ocjena	Dokumentacija	Implementacija
1	Dokumentacija i ključni dokumenti poput politike ne postoje ili provoditelji procesa nisu s njom upoznati.	Proces nije strukturiran, aktivnosti se provode *ad-hoc*, a postupci su neregularni i nepraćeni.
2	Postoji osnovna dokumentacija koja nije redovito ažurirana i pokriva samo osnovne elemente kontrole.	Proces je neformalno uspostavljen i provodi se sporadično, bez potpune dosljednosti ili formalne strukture.
3	Dokumentacija je formalno odobrena, ažurirana s definiranim iznimkama; većina elemenata dokumentacije je jasna.	Proces je formaliziran i strukturiran, provodi se redovito; postoje dokazi za većinu aktivnosti, uz manje iznimke (<10%).
4	Dokumentacija je potpuna, ažurirana i uključuje sve ključne elemente i procese; uz postojanje manjih iznimaka (<3%).	Proces je potpuno implementiran s dokazima za sve aktivnosti, uključujući praćenje metrike i izvještavanje; uz postojanje manjih iznimaka (<5%).
5	Dokumentacija je u potpunosti usklađena, redovito ažurirana i kontinuirano se poboljšava; iznimke <0,5%.	Proces je implementiran na najvišoj razini, s naprednim praćenjem, redovitim poboljšanjima i minimalnim iznimkama (<1%).

Kroz primjenu ovih kriterija, osim osiguravanja dosljednosti u ocjenjivanju, subjektima se pruža jasna povratna informacija o njihovoj trenutačnoj razini usklađenosti s najboljim praksama u području kibernetičke sigurnosti.

Kategorizacija kontrola

Kontrole kibernetičke sigurnosti se prema njihovom primarnom fokusu unutar okvira upravljanja kibernetičkom sigurnosti dijele u nekoliko kategorija koje su kako slijedi:

- **Politike i procedure (POL)**
  Ova kategorija obuhvaća kontrole usmjerene na izradu, implementaciju i ažuriranje sigurnosnih politika, formalnih procesa i procedura te izvještavanja o stanju kibernetičke sigurnosti. Kontrole osiguravaju jasno definirana pravila, odgovornosti i smjernice za sustavno upravljanje rizicima, incidentima i drugim ključnim sigurnosnim aspektima. Osim toga, omogućuju pravovremenu dostupnost ključnih sigurnosnih informacija za donošenje strateških odluka i osiguranje usklađenosti s poslovnim i regulatornim zahtjevima.

- **Organizacijske odgovornosti i ovlasti (ORG)**
  Kontrole koje se odnose na definiranje uloga, odgovornosti, ovlasti u skladu s organizacijskom strukturom, osiguravajući učinkovitost i usklađenost. Primjeri kontrola bile bi one koje se odnose na razdvajanje odgovornosti, imenovanje odgovornih osoba i jasno definiranje zadataka.

- **Podizanje svijesti i edukacija (EDU)**
  Kontrole fokusirane na edukaciju zaposlenika, partnera i drugih dionika koji imaju pristup informacijskoj i drugoj imovini, povećavajući svijest o prijetnjama i sigurnosnim praksama. Koriste se za provjeru provođenja edukacija o sigurnosnim politikama i osiguranja svijesti o kibernetičkim prijetnjama.

- **Upravljanje resursima (RES)**
  Ova kategorija obuhvaća kontrole usmjerene na osiguravanje dostupnosti, pravilne alokacije i otpornosti ljudskih, financijskih i tehničkih resursa potrebnih za provedbu mjera kibernetičke sigurnosti. Kontrole uključuju godišnju procjenu resursa, osiguranje financijskih sredstava te prilagodbu tehničkih kapaciteta kako bi se omogućio kontinuitet poslovanja i otpornost na nepredviđene situacije. Također, obuhvaćaju implementaciju redundancije ključnih sustava i resursa, osiguravanje rezervnih kapaciteta te uspostavu alternativnih komunikacijskih kanala u kriznim uvjetima.

- **Upravljanje i sudjelovanje (UPR)**
  Kontrole koje osiguravaju transparentan protok informacija i uključivanje ključnih dionika u donošenje odluka i sudjelovanje u inicijativama kibernetičke sigurnosti. Svrha im je ustanoviti postojanje mehanizama sudjelovanja, transparentnosti između timova i prioritizacije sigurnosnih aktivnosti.

- **Praćenje i nadzor (NAD)**
  Ova kategorija obuhvaća kontrole usmjerene na kontinuirano praćenje i nadzor kibernetičke sigurnosti, uključujući automatizirane sustave za detekciju prijetnji i nadzor u stvarnom vremenu. Kontrole osiguravaju praćenje, bilježenje i analizu aktivnosti unutar mrežnih i informacijskih sustava subjekta, čime se omogućava pravovremena detekcija, istraga i odgovor na sigurnosne incidente. Također, obuhvaćaju upravljanje dnevničkim zapisima, usklađivanje vremena među sustavima te analizu ključnih sigurnosnih metrika za praćenje sigurnosnog stanja i donošenje informiranih odluka.

- **Upravljanje imovinom (INV)**
  Kontrole koje pokrivaju inventar, praćenje, klasifikaciju i upravljanje programskom i sklopovskom imovinom. Kontrole provjeravaju održavanje inventara, identifikaciju kritične imovine i upravljanje manje kritičnim resursima.

- **Zaštita podataka (POD)**
  Ova kategorija obuhvaća kontrole usmjerene na pravilno upravljanje, zaštitu i sigurnost podataka, uključujući njihovu klasifikaciju, identifikaciju rizika i upravljanje osjetljivim informacijama. Kontrole osiguravaju sigurno pohranjivanje, prijenos i obradu podataka te zaštitu prijenosnih medija i uređaja kroz implementaciju kriptiranja i sigurnosnih mjera za prijenosne i osobne uređaje.

- **Upravljanje rizicima (RIZ)**
  Obuhvaćene su kontrole za identificiranje, analizu i upravljanje rizicima vezanim uz imovinu subjekta. Cilj je pravovremeno prepoznavanje i dokumentacija rizika radi provedbe mjera za njihovo smanjenje ili uklanjanje. Kontrole pokrivaju fizičke prijetnje, kibernetičke ranjivosti i rizike od trećih strana, osiguravajući proces usklađen s poslovnim potrebama i sigurnosnim standardima te jačajući otpornost subjekta i kontinuitet poslovanja.

- **Digitalni identiteti (DID)**
  Kontrole osiguravaju uspostavu jedinstvenih digitalnih identiteta povezanih s korisnicima mrežnih i informacijskih sustava radi odgovornosti i transparentnosti. Fokus je na vođenju evidencije, praćenju promjena te uspostavi kompenzacijskih mjera za dijeljene identitete, uz osiguranje usklađenosti sa zakonodavstvom i najboljim praksama, čime se štite podaci i sigurnost sustava.

- **Sigurnosne konfiguracije i mehanizmi (SKM)**
  Ova kategorija obuhvaća kontrole usmjerene na zaštitu krajnjih točaka, upravljanje ranjivostima i sigurnu konfiguraciju mrežnih i informacijskih sustava. Kontrole osiguravaju implementaciju antivirusnih alata, sustava za detekciju i odgovor na prijetnje te upravljanje sigurnosnim zakrpama kako bi se smanjila izloženost sustava sigurnosnim prijetnjama. Također, uključuju sustavno identificiranje i procjenu ranjivosti kroz sigurnosna testiranja i skeniranja, uz pravovremeno smanjenje rizika. Upravljanje konfiguracijama osigurava dosljednu primjenu sigurnih postavki, njihovu dokumentaciju i redovite revizije kako bi se spriječile sigurnosne slabosti i održala stabilnost sustava.

- **Sigurnost razvoja softvera (SRZ)**
  Kategorija obuhvaća kontrole koje osiguravaju primjenu sigurnosnih praksi u svim fazama životnog ciklusa razvoja softvera. Fokus je na identifikaciji i sanaciji ranjivosti, sigurnosnoj analizi komponenti i testiranju softvera prije njegove implementacije u produkcijsko okruženje. Kontrole unutar ove kategorije pomažu subjektima u izgradnji sigurnosno otpornog softvera, smanjenju rizika i osiguravanju usklađenosti s najboljim praksama u razvoju.

- **Kriptografija (KRIP)**
  Kategorija obuhvaća kontrole koje osiguravaju definiranje, implementaciju i nadzor kriptografskih metoda za zaštitu podataka. Cilj je osigurati dostupnost, autentičnost, cjelovitost i povjerljivost podataka kroz primjenu odgovarajućih kriptografskih tehnika i metoda uz upravljanje kriptografskim ključevima.

- **Fizička sigurnost (FIZ)**
  Cilj ovih kontrola je osiguravanje fizičke zaštite prostora, imovine i opreme unutar subjekta. Fokus je na implementaciji mjera koje sprječavaju neovlašteni pristup, štite kritične resurse i smanjuju rizike povezane s fizičkim prijetnjama. Primjeri kontrola uključuju postavljanje fizičkih barijera, implementaciju sustava za kontrolu pristupa, sigurnosnih kamera te osiguranje sigurnosnih perimetara prema procjeni rizika.

Korelacija s relevantnim standardima i postojanje politika

Korelacija kontrola s relevantnim standardima

Kontrole definirane u ovom dokumentu mogu se kontekstualno povezati s klauzulama i kontrolama iz drugih relevantnih standarda, poput *ISO/IEC 27001*, *NIST Cybersecurity Framework*, *CIS Controls* i drugih. U ovom dokumentu navedeni su primjeri kontrola iz tih standarda koje su tematski srodne, funkcionalno povezane ili mogu poslužiti kao referenca za bolje razumijevanje i primjenu sigurnosnih kontrola definiranih ovim dokumentom.

Ove poveznice imaju informativnu svrhu i služe kao podrška organizacijama pri usporedbi i usklađivanju različitih sigurnosnih okvira. Navedene korelacije ne predstavljaju izravno preslikavanje zahtjeva, već smjernice za lakšu integraciju kontrola u skladu s potrebama i specifičnostima okruženja u kojem se primjenjuju.

Poveznice se nalaze u dijelu *Reference* nakon *smjernica za ocjenjivanje* pojedine kontrole.

Dokumentiranje politika unutar interne regulative subjekta

Kontrole mogu zahtijevati da subjekt ima izrađenu, dokumentiranu ili na drugi način utvrđenu određenu politiku, pri čemu nije nužno da dokument bude naslovljen upravo tim nazivom, primjerice „Politika sprječavanja sukoba interesa”. Bitno je da sadržaj predmetne politike bude jasno definiran unutar bilo kojeg dokumenta koji je formalno odobren od strane upravljačkog tijela subjekta i koji ima važeći status u okviru interne regulative subjekta.

Ključno je da dokument u kojem se politika nalazi ima važeći status, da je dostupan relevantnim dionicima te da omogućava dosljednu primjenu i nadzor. Na taj način se osigurava funkcionalna usklađenost s očekivanjima kontrole, bez obzira na naziv ili strukturu pojedinačnog dokumenta.

POL-001: Postojanje strateškog akta kibernetičke sigurnosne politike

Ova kontrola osigurava da subjekt ima formalno usvojen strateški akt kibernetičke sigurnosne politike, odobren od strane upravljačkog tijela. Strateški akt predstavlja temelj za organizacijske aktivnosti subjekta u kibernetičkoj sigurnosti i daje okvir za definiranje ključnih ciljeva, mjera upravljanja rizicima, organizacijskih struktura te raspodjele uloga, odgovornosti, ovlasti i obveza, pri čemu jasno definirani ciljevi kibernetičke sigurnosti i otpornosti imaju ključnu ulogu u osiguravanju učinkovitosti mjera zaštite, omogućujući usklađivanje sigurnosnih aktivnosti s poslovnim potrebama i okruženju subjekta te usmjeravanje napora prema prioritetnim rizicima. Subjekt je obvezan najmanje jednom godišnje procjenjivati djelotvornost mjera te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike.

U procesu provjere provjerava se postoji li dokument koji je formalno usvojen od strane upravljačkog tijela kao i jesu li svi ključni dionici informirani o njegovom sadržaju. Provjerava se pokriva li dokument ključne aspekte kao što su ciljevi, mjere i raspodjela odgovornosti i ovlasti te je li ažuriran prema potrebi nakon što je najmanje jednom tijekom tekuće godine prethodno provedena procjena djelotvornosti mjera. Na taj način se osigurava da strateški akt ostaje relevantan i prilagođen promjenjivim sigurnosnim izazovima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Strateški akt ne postoji.
2	Strateški akt je u pripremi i sadrži sve osnovne elemente, ali nije formalno usvojen od strane upravljačkog tijela.
3	Strateški akt je dokumentiran, sadrži sve osnovne elemente i formalno je usvojen od strane upravljačkog tijela.
4	Strateški akt je dokumentiran, sadrži sve osnovne elemente, formalno usvojen od strane upravljačkog tijela i implementiran u poslovne procese subjekta, uzimajući u obzir poslovne prioritete subjekta.
5	Strateški akt je dokumentiran, sadrži sve osnovne elemente, formalno je usvojen od strane upravljačkog tijela i implementiran u poslovne procese subjekta te ažuriran po potrebi kao i po provedbi procjene djelotvornosti mjera koja se provodi najmanje jednom tijekom tekuće godine.

Reference:

- **ISO/IEC 27001:2022** (5.2)
- **ISO 22301:2019** (6.2)
- **NIST SP 800-53 Rev. 5** (PM-1)
- **NIST CSF v2.0** (Kategorija GV)

POL-002: Izbjegavanje sukoba interesa u kibernetičkoj sigurnosti

Ova kontrola osigurava da subjekt ima jasno adresirano sprječavanje sukoba interesa u vezi s ulogama u kibernetičkoj sigurnosti. Cilj je postaviti jasne smjernice i postupke za identifikaciju i sprječavanje sukoba interesa u aktivnostima koje bi mogle utjecati na neovisnost procjena ili učinkovitost sigurnosnih mjera. Posebno je važno razdvojiti odgovornosti procjene rizika i provedbe mjera zaštite kako bi se osigurala objektivnost i nepristranost odluka. Ove mjere posebno su važne u manjim organizacijama, gdje ograničeni resursi otežavaju provedbu stroge podjele uloga.

Revizori provjeravaju je li sukob interesa adresiran u kontekstu kibernetičke sigurnosti u formalno usvojenom dokumentu (razne domenske politike, ISMS politike ili drugo), s posebnim naglaskom na pravila o razdvajanju uloga između procjene rizika i provedbe sigurnosnih mjera. Također se ocjenjuje način implementacije tih smjernica unutar subjekta te mehanizmi koji osiguravaju njihovu dosljednu primjenu. Dodatno, procjenjuje se dostupnost edukacijskih programa i resursa namijenjenih zaposlenicima, koji im omogućuju bolje razumijevanje potencijalnih sukoba interesa te učinkovitu primjenu relevantnih politika u praksi.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje smjernice za sprječavanje sukoba interesa.
2	Postoje osnovne smjernice, ali nisu formalizirane.
3	Sprječavanje sukoba interesa je formalno adresirano, ali nije dosljedno primjenjivano.
4	Sprječavanje sukoba interesa je formalno adresirano i primjenjivano, ali ne uključuje razdvajanje uloga između procjene rizika i provedbe mjera.
5	Sprječavanje sukoba interesa je implementirano, jasno komunicirano i redovito se prilagođava u skladu s promjenama u subjektu te uključuje razdvajanje uloga kako bi se spriječio sukob interesa.

Reference:

- **ISO/IEC 27001:2022** (5.3, A.5.3)
- **ISO 22301:2019** (5.3)
- **NIST SP 800-53 Rev. 5** (AC-5)
- **NIST CSF v2.0** (Kategorija GV)

POL-003: Politika fizičke sigurnosti

Kontrola osigurava izradu i provedbu politike fizičke sigurnosti koja jasno definira opseg primjene, razine zaštite prostora, odgovorne osobe, načine primjene i redovitost provjere djelotvornosti mjera. Politika mora biti prilagođena identificiranim unutarnjim i vanjskim rizicima subjekta, a promjene politike moraju se dokumentirati i komunicirati sa svim zaposlenicima i relevantnim pravnim osobama.

Analizira se dokumentirana politika fizičke sigurnosti, uključujući opseg, razine zaštite i odgovornosti i ovlasti. Također se ispituje način komunikacije politike prema zaposlenicima i ostalom osoblju koje ima pristup u perimetar fizičke sigurnosti, te odnosi s trećim stranama (ako su uključene u osiguravanje perimetra fizičke sigurnosti, bilo u aspektima fizičke ili tehničke zaštite odnosno kroz upravljanje objektom), kao i definirani postupci provjere učinkovitosti mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Politika fizičke sigurnosti nije razvijena niti dokumentirana.
2	Politika je djelomično razvijena, ali nije dokumentirana ili komunicirana.
3	Politika je dokumentirana, ali implementacija i komunikacija su ograničeni.
4	Politika je dokumentirana, formalno usvojena od strane upravljačkog tijela, implementirana i djelomično komunicirana prema dionicima.
5	Politika je potpuno dokumentirana, formalno usvojena od strane upravljačkog tijela, implementirana, sustavno komunicirana te redovito ažurirana.

Reference:

- **ISO/IEC 27001:2022** (A.7.4, A.7.5, A.7.6)
- **NIST SP 800-53 Rev. 5** (PE-1, PE-2, PE-3, PE-6)
- **NIST CSF v2.0** (Kategorija PR)

POL-004: Politike lozinki i autentifikacije

Ova kontrola osigurava implementaciju i održavanje politika lozinki i autentifikacije korisnika u skladu s najboljim praksama i tehničkim mogućnostima sustava. Politike trebaju obuhvatiti minimalne zahtjeve za duljinu i složenost lozinki kako je definirano mjerom u Uredbi, pravila za njihovu izmjenu (ukoliko se iste koriste za autentifikaciju kako je definirano Uredbom), korištenje višefaktorske autentifikacije (MFA) gdje je moguće te definiranje specifičnih pravila za privilegirane i servisne korisničke račune – ukoliko se koristi MFA umanjuje se zahtjev za duljinom lozinke sukladno zahtjevima mjere Uredbe. Poseban naglasak stavlja se na sigurno dodjeljivanje, pohranu i zaštitu vjerodajnica, uključujući generiranje kriptografskih sažetaka uz „soljenje“ i/ili „paprenje“. Za sustave s tehničkim ograničenjima potrebno je uvesti odgovarajuće kompenzacijske mjere koje minimiziraju rizike. Dodijeljene lozinke i autentifikacijska sredstva moraju biti usklađeni s dobrom praksom, redovito revidirani i prilagođavani novim prijetnjama. Kontrola također uključuje edukaciju osoblja o sigurnosnim praksama te definiranje postupaka za zaštitu vjerodajnica i osiguravanje sigurnog prijenosa vjerodajnica.

Provjera usklađenosti obuhvaća pregled dokumentacije politika lozinki i autentifikacije, analizu sigurnosnih procedura za upravljanje lozinkama te konzultacije s odgovornim osobama kako bi se potvrdila dosljedna i pravilna primjena definiranih pravila.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje i ne poštuju se nikakva specifična pravila / standard za kompleksnost lozinki i mehanizme autentifikacije, odnosno ne postoji definirana politika.
2	Na pojedinim sustavima primijenjena su interna nepisana pravila za lozinke iz mehanizme autentifikacije, ali na neuniformni nekonzistentan način ili nisu u skladno s smjernicama Uredbe.
3	Postoji jasna politika za kompleksnost lozinka i mehanizme autentifikacije sukladno Uredbi.
4	Uspostavljen je sustavni proces koji osigurava automatsku primjenu jasno propisanih pravila za kompleksnost lozinka i mehanizme autentifikacije sukladno Uredbi.
5	Uspostavljen je sustavni proces koji osigurava automatsku primjenu i neovisnu provjeru primjene jasno propisanih pravila za kompleksnost lozinka i mehanizme autentifikacije sukladno Uredbi ili subjekt za autentifikaciju koristi dva faktora – navedeno je sustavni proces koji je jasno implementiran i dokumentiran.

Reference:

- **ISO/IEC 27001:2022** (A.5.15, A.5.16, A.5.17, A.8.3, A.8.4)
- **NIST SP 800-53 Rev. 5** (IA-2, IA-4, IA-5)

- **NIST SP 800-63B**

POL-005: Upravljanje sigurnosnim politikama korisničkih računa

Ova kontrola obuhvaća uspostavu i održavanje procesa sigurnosnog upravljanje cijelim životnim ciklusom korisničkih računa u mrežnim i informacijskim sustavima subjekta. Proces treba uključivati postupke za pravovremeno otvaranje i obaveznu inicijalnu promjenu osobnih pristupnih podataka (*lozinke i PIN*) prilikom prvog korištenja korisničkog računa, deaktivaciju neaktivnih računa nakon unaprijed definiranog perioda i brisanje računa, te zahtjeve za sigurnost privilegiranih i servisnih računa. Poseban naglasak stavlja se na uspostavu evidencije korisničkih računa, redovitu reviziju prava pristupa te praćenje aktivnosti korisnika kako bi se osigurala usklađenost s poslovnim potrebama i zaštita od zloupotreba tj. zaključavanje računa nakon višestrukih neuspjelih pokušaja prijave (*account lockout*). Sustave s tehničkim ograničenjima treba osigurati dodatnim kompenzacijskim mjerama za kontrolu pristupa.

Provjera usklađenosti uključuje analizu evidencija korisničkih računa, reviziju dokumentacije politika te ispitivanje praktične primjene sigurnosnih mjera kroz konzultacije s odgovornim osobama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Korisnički računi se otvaraju na nekontrolirani način bez jasne poslovne potrebe i bez pravila te ne postoje nikakva pravila ili nadzor korištenja istih.
2	Postoji ustaljeni ali nedokumentirani proces otvaranja korisničkih računa ali ne i pravila korištenja ili nadzora koja su dokumentirana.
3	Implementirana i dokumentirana su jasna pravila i postupak otvaranja korisničkih računa ali bez redovitih revizija i evidencija.
4	Postoje mehanizmi provjere primjene jasnih pravila upravljanja s korisničkim računima.
5	Uspostavljene su automatske kontrole koje osiguravaju da je se propisana pravila konzistentno primjenjuju, računi pravovremeno gase i korištenje nadzore, te se automatizmom gase neaktivne korisničke sjednice.

Reference:

- **ISO/IEC 27001:2022** (A.5.18, A.8.2)
- **NIST SP 800-53 Rev. 5** (AC-2, AC-6, AC-7, IA-4)
- **NIST CSF v2.0** (Kategorija PR)

POL-006: Proces upravljanja kibernetičkim sigurnosnim rizicima

Ova kontrola osigurava da subjekt ima jasno razvijen, dokumentiran, implementiran i na godišnjoj osnovi ažuriran proces upravljanja rizicima koji uključuje procjenu rizika (identifikacija, analiza, evaluacija), određivanje razine i kritičnosti rizika, načine obrade rizika, identifikaciju vlasnika rizika i njihovo područje odgovornosti. Ti procesi trebaju uključivati identifikaciju, analizu i kontinuirano praćenje rizika, čime se omogućuje pravovremeno prepoznavanje prijetnji i prilagodba mjera zaštite.

U postupku provjere ispituje se postojanje dokumentiranog procesa upravljanja rizicima i prati se njihova usklađenost s promjenama u poslovanju i sigurnosnom okruženju. Ocjenjuje se kako se prate ključni pokazatelji sigurnosti kako bi subjekt pravovremeno reagirao na potencijalne rizike. Također se u postupku provjera i dostupnost dokumentacije relevantnim zaposlenicima i dosljednost komunikacije s odgovornim osobama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Procesi ne postoje.
2	Postoje osnovni procesi uz osnovnu identifikaciju vlasnika rizika , ali nisu formalno dokumentirani.
3	Procesi i identifikacija vlasnika rizika postoje te su formalno dokumentirani, ali bez jasno definirane provedbe.
4	Procesi i identifikacija vlasnika rizika postoje te su formalno dokumentirani i implementirani. Formalizirani procesi postoje, ali se ne prate dosljedno.
5	Procesi i identifikacija vlasnika rizika postoje, formalno su dokumentirani, implementirani i ažurirani tijekom tekuće godine.

Reference:

- **ISO/IEC 27001:2022** (5.3, 5.4, A.5.3, A.5.4)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (5.3)
- **ENISA Interoperable Risk Framework**
- **NIST SP 800-39**
- **NIST SP 800-30 Rev. 1**

POL-007: Uspostava obaveznih mjera zaštite mreže

Ova kontrola osigurava da subjekt primijeni odgovarajuće tehničke mjere zaštite mrežne infrastrukture u skladu s vlastitom mrežnom arhitekturom i razinom izloženosti javnim mrežama. Njezina provedba doprinosi sveukupnoj kibernetičkoj otpornosti sustava putem sustavnog korištenja vatrozida, virtualnih privatnih mreža (VPN), principa nultog povjerenja (zero trust), sigurnih mrežnih protokola, kao i segmentacije mreže temeljem kritičnosti podataka ili funkcionalnosti pojedinih mrežnih segmenata (npr. uredska, nadzorna, produkcijska, mreža za goste i slične). Time se minimizira rizik od neovlaštenog pristupa i smanjuje površina napada.

Provjerava se dokumentacija kojom su definirane potrebne obavezne mjere zaštite mreže uspostavljene sukladno mrežnoj arhitekturi i izloženosti javnim mrežama. Nakon provjere takve dokumentacije, dodatno se analizira koje su od definiranih mjera stvarno primijenjene u praksi sukladno procjeni iz dokumentacije te postoji li dosljednost između dokumentiranog i implementiranog stanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt nije razmatrao mrežnu zaštitu sukladno izloženosti; ne postoje dokumentirane mjere ni arhitektura.
2	Subjekt je djelomično razmotrio, no nije formalno dokumentirao potrebu za obaveznim mjerama zaštite mreže – neke mjere su implementirane.
3	Dokumentirane i implementirane su osnovne mjere zaštite (poput vatrozida), a za preostale mjere ne postoji dokumentacija ili implementacija.
4	Sve mjere su dokumentirane i implementirane sukladno procijenjenoj potrebi (samo za javno izložene mreže).
5	Sve mjere su dokumentirane i implementirane sukladno procijenjenoj potrebi (uključujući javno izložene i unutarnje mreže).

Reference:

- **ISO/IEC 27001:2022** (A.8.20, A.8.21, A.8.22)
- **ISO/IEC 27002:2022** (8.20, 8.21, 8.22)

POL-008: Razrada i održavanje pravila osnovne prakse kibernetičke higijene

Ova kontrola osigurava razvoj, dokumentaciju, održavanje i implementaciju pravila osnovne prakse kibernetičke higijene unutar subjekta. Pravila trebaju biti jasno definirana, lako dostupna korisnicima te redovito ažurirana kako bi odražavala promjene u tehnologiji i sigurnosnim prijetnjama. Pravila moraju uključivati smjernice za sigurno korištenje elektroničke pošte, lozinki, prijenosnih uređaja i drugih ključnih aspekata digitalne sigurnosti.

Provjera usklađenosti uključuje pregled dokumentacije, analizu sadržaja pravila te konzultacije s korisnicima kako bi se osigurala razumljivost i primjena pravila u praksi.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Pravila kibernetičke higijene nisu definirana, a subjekt ne može demonstrirati provedbu dobre prakse kibernetičke higijene.
2	Pravila su djelomično dokumentirana, ali se u praksi ne primjenjuju ili se primjenjuju nepisana pravila dobre prakse kibernetičke higijene.
3	Pravila su dokumentirana, dostupna svim korisnicima i u primjeni.
4	Postoje ručni mehanizmi povremene provjere primjene propisanih pravila.
5	Uspostavljen je sustavni proces koji osigurava automatsku primjenu i neovisnu provjeru primjene propisanih pravila.

Reference:

- **ISO/IEC 27001:2022** (7.5, A.5.10, A.5.37, A.6.3)
- **ISO 22301:2019** (7.5)

POL-009: Planovi odgovora na incidente koji uključuju ključne dobavljače

Ova kontrola osigurava razvoj, dokumentiranje, održavanje i primjenu planova odgovora na incidente koji uključuju ključne dobavljače i pružatelje usluga. Planovi trebaju definirati uloge, odgovornosti i ovlasti, komunikacijske kanale, aktivnosti i postupke, odnosno sadržavati jasne procedure za koordinaciju, komunikaciju i djelovanje koje ključni dobavljači moraju provesti tijekom odgovora u slučaju incidenata koji mogu utjecati na kritične mrežne i informacijske sustave. Cilj je osigurati brzu i koordiniranu reakciju te smanjenje potencijalnih posljedica incidenata na kritične mrežne i informacijske sustave. Poseban naglasak stavlja se na redovitu reviziju i ažuriranje planova te uključivanje dobavljača u testiranje i simulacije odgovora na incidente.

Provjera usklađenosti obuhvaća pregled dokumentacije planova odgovora na incidente, analizu dokumentacije koja opisuje postupke za uključivanje dobavljača u odgovore na incidente uz analizu procedura i provjeru postupaka za koordinaciju s dobavljačima, analizu zapisa o testiranjima i simulacijama, simulaciju odgovora na incidente te konzultacije s odgovornim osobljem za upravljanje incidentima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje planovi odgovora na incidente koji uključuju ključne dobavljače.
2	Postoji osnovni plan odgovora na incidente, ali ključni dobavljači nisu formalno uključeni. Neke odgovornosti su implicitno podijeljene, ali bez jasno definiranih procedura, komunikacijskih kanala i kontaktnih točaka.
3	Planovi su razvijeni i uključuju ključne dobavljače, ali nisu testirani niti se redovito ažuriraju.
4	Sveobuhvatni planovi su razvijeni, dokumentirani i testirani s ključnim dobavljačima te se ažuriraju periodično, uključujući reviziju ugovora i SLA-ova.
5	Subjekt ima proaktivno i integrirano upravljanje incidentima s ključnim dobavljačima, uključujući zajedničke planove odgovora, tehničke i komunikacijske protokole, te automatizirane alate za koordinaciju u realnom vremenu.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.24, A.5.26, A.5.30)
- **ISO 22301:2019** (8.4.1, 8.4.2)
- **NIST SP 800-53 Rev. 5** (IR-4)
- **NIST SP 800-61 Rev. 2** (4.1)
- **NIST CSF v2.0** (RS.CO-2, RS.CO-3)

POL-010: Razvoj i dokumentiranje procedura za postupanje s incidentima

Ova kontrola osigurava razvoj, dokumentiranje, održavanje i implementaciju procedura za postupanje s incidentima. Procedura treba definirati uloge, odgovornosti i ovlasti, komunikacijske kanale te korake za praćenje, sprječavanje, otkrivanje, analizu, zaustavljanje i oporavak od incidenata. Također uključuje jasno definirane vremenske okvire za prijavljivanje incidenata unutar subjekta.

Provjera revizora uključuje pregled dokumentacije o procedurama za postupanje s incidentima, analizu definiranih uloga, odgovornosti i ovlasti, provjeru vremenskih okvira za prijavu incidenata, te konzultacije s odgovornim osobljem za upravljanje incidentima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Postupci za postupanje s incidentima nisu razvijeni niti dokumentirani.
2	Postoji osnovni plan, ali je nedovoljno razvijen i djelomično primijenjen. Vremenski rokovi za prijavu nisu precizno definirani. Uloge su djelomično poznate, komunikacija neformalna. Plan nije testiran, a incidenti se rijetko analiziraju formalno.
3	Plan odgovora na incidente dokumentiran i obuhvaća sve osnovne faze (poput PICERL modela). Uloge i odgovornosti su definirane, komunikacija među uključenim stranama je formalizirana, a vremenski okviri za prijavu su propisani. Plan se koristi u praksi, ali se ne primjenjuje ujednačeno u svim organizacijskim dijelovima. Formalna evaluacija provodi se selektivno. Plan se povremeno ažurira i testira.
4	Plan odgovora na incidente je sveobuhvatan, primijenjen i poznat uključenom osoblju.
5	Plan je u potpunosti integriran u sigurnosno upravljanje subjekta. Osigurava automatiziranu evidenciju, eskalaciju i praćenje učinkovitosti. Postoje jasno definirani vremenski pragovi za internu i eksternu prijavu. Testiranja, vježbe i kontinuirano poboljšanje su dio sigurnosne kulture.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.25, A.5.37)
- **NIST SP 800-53 Rev. 5** (IR-1, IR-4, IR-6, IR-8)
- **NIST SP 800-61 Rev. 2**
- **NIST CSF v2.0** (RS.CO-2)

POL-011: Sigurna komunikacija tijekom postupanja s incidentima

Ova kontrola osigurava primjenu sigurnih komunikacijskih metoda tijekom postupanja s incidentima. Po potrebi se uključuje korištenje višefaktorske autentifikacije (MFA), kontinuirane provjere autentičnosti, kriptirane glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava za hitne situacije. Cilj je osigurati povjerljivost, integritet i dostupnost informacija tijekom odgovora na incidente.

Provjera usklađenosti uključuje pregled implementacije višefaktorske autentifikacije i drugih sigurnosnih mehanizama te testiranje sigurnosti komunikacijskih kanala tijekom odgovora na incidente. Također se pregledava i analizira dokumentacija o procedurama sigurne komunikacije i sigurnim komunikacijskim praksama te se provode konzultacije s IT osobljem odgovornim za sigurnost komunikacija kako bi se osigurala dosljedna primjena sigurnih metoda komunikacije i sigurnih komunikacijskih praksi.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurna komunikacija tijekom postupanja s incidentima nije uspostavljena.
2	Pojedini komunikacijski kanali su zaštićeni osnovnim sigurnosnim mehanizmima (npr. lozinke ili VPN), Ne postoji plan za hitnu sigurnu komunikaciju niti jasno definirane prakse u dokumentaciji. Definirani kanali se ne koriste dosljedno.
3	Postoji dokumentiran plan za primjenu sigurnih komunikacijskih metoda tijekom incidenta kao i planirani alternativni komunikacijski kanal za hitne situacije, ali njegova dostupnost i otpornost nisu redovito testirani.
4	Tijekom odgovora na incidente koriste se samo sigurni i prethodno testirani komunikacijski kanali. Višefaktorska autentifikacija, enkripcija i kontrole pristupa koriste se sukladno potrebi. Komunikacijski sustavi su testirani kroz simulacije incidenata.
5	Subjekt koristi centraliziran, visoko siguran i redundantan sustav komunikacije za sve faze odgovora na incidente, uključujući glasovne, video i tekstualne kanale s enkripcijom u stvarnom vremenu. Višefaktorska autentifikacija i kontinuirano praćenje autentičnosti korisnika su standard. Postoji integrirani sustav za hitne komunikacije, neovisan o primarnoj infrastrukturi s mogućnošću rada u uvjetima prekida mrežnih usluga. Planovi komunikacije se redovito testiraju kroz tehničke i organizacijske vježbe. Svi zaposlenici uključeni u upravljanje incidentima educirani su o pravilima sigurne komunikacije.

Reference:

- **ISO/IEC 27001:2022** (7.4, A.5.29, A.5.30, A.5.37)
- **NIST SP 800-53 Rev. 5** (SC-8, IR-4)
- **NIST CSF v2.0** (PR.DS-2)

POL-012: Godišnje izvještavanje o stanju kibernetičke sigurnosti

Ova kontrola osigurava da subjekt redovito, jednom tijekom tekuće godine, izrađuje sveobuhvatan izvještaj o stanju kibernetičke sigurnosti za osobe odgovorne za provedbu mjera o stanju kibernetičke sigurnosti. Izvještaji trebaju sadržavati evaluaciju učinkovitosti postojećih sigurnosnih mjera, pregled identificiranih prijetnji i moguće rizike te preporuke za unapređenje razine kibernetičke sigurnosti. Jasno strukturirani izvještaji i njihova redovita evaluacija, omogućuju upravljačkom tijelu subjekta bolje razumijevanje trenutne sigurnosne situacije, donošenje informiranih strateških odluka za podizanje razine kibernetičke sigurnosti i osiguravaju kontinuirano praćenje napretka u upravljanju sigurnosnim rizicima i poboljšanju sigurnosnih mjera. Izvještaji trebaju biti dostupni svim relevantnim dionicima, uključujući osobe odgovorne za provedbu mjera o stanju kibernetičke sigurnosti, kako bi se osigurala transparentnost i pravovremeno usklađivanje sigurnosnih inicijativa s poslovnim ciljevima. Ključno je da izvještaji budu pravovremeni, arhivirani i da omogućuju dosljedno praćenje sigurnosnog stanja tijekom vremena.

U postupku provjere pregledava se postojanje godišnjih izvještaja te se provjerava i analizira sadržaj izvještaja, odnosno sadrži li izvještaj sve relevantne aspekte poput prijetnji, učinkovitosti mjera i preporuka za poboljšanje. Također se ocjenjuje je li izvještaj pravovremeno dostupan osobama operativno odgovornim za provođenje mjera kibernetičke sigurnosti i osobama u upravljačkom tijelu subjekta, postoji li sustavna arhiva prethodnih izvještaja radi praćenja trendova i sigurnosnih poboljšanja te koliko su preporuke iz izvještaja primijenjene u praksi. Ocjenjuje se pravovremenost izrade izvještaja, njegova upotrebljivost za strateško odlučivanje te usklađenost sa sigurnosnim zahtjevima subjekta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Godišnji izvještaji o kibernetičkoj sigurnosti ne postoje.
2	Postoje osnovni godišnji izvještaji, ali su neformalni i ne pokrivaju sve ključne aspekte.
3	Izvještaji se izrađuju godišnje, ali im nedostaju ključni elementi ili nisu dostupni svim relevantnim osobama.
4	Izvještaji se izrađuju godišnje, sadrže sve ključne elemente i pravovremeno su dostupni svim relevantnim osobama, ali preporuke nisu adekvatno ili precizno definirane.
5	Izvještaji se izrađuju godišnje, sadrže sve ključne elemente i uključuju detaljnu analizu prijetnji, učinkovitosti mjera i adekvatno definirane preporuke te su pravovremeno dostupni svim relevantnim osobama.

Reference:

- **ISO/IEC 27001:2022** (9.1, 9.2, 9.3, 10.1, 10.2, A.5.4)
- **ISO 22301:2019** (9.1, 9.2, 9.3, 10.1, 10.2)
- **ISO/IEC 27005:2022** (8.6)
- **NIST SP 800-53 Rev. 5** (PM-6, PM-9)
- **NIST CSF v2.0** (GV.RM-03, Kategorija GV.OV)

ORG-001: Raspodjela uloga, odgovornosti i obveza

Cilj ove kontrole je uspostaviti jasnu i formalnu strukturu uloga, odgovornosti i obveza vezanih uz sigurnost unutar subjekta, kako bi se smanjio rizik od nesporazuma, preklapanja odgovornosti i nedostatka koordinacije u provedbi sigurnosnih mjera. Dodatno svaki zaposlenik mora biti svjestan svojih zadataka i uloga, što omogućuje bolju usklađenost s poslovnim potrebama, učinkovitiju provedbu sigurnosnih mjera i prilagodbu na promjenjive sigurnosne izazove.

U postupku se provjerava postoji li dokumentacija koja opisuje raspodjelu uloga i obveza razdvajanja pojedinih uloga u pitanjima kibernetičke sigurnosti i jesu li te informacije jasno komunicirane svim relevantnim zaposlenicima koji su uključeni u provedbu sigurnosnih mjera. Dodatno se procjenjuje jesu li uloge revidirane i ažurirane u skladu s poslovnim potrebama i promjenama unutar subjekta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema definirane raspodjele uloga i odgovornosti.
2	Uloge su djelomično definirane, ali nisu formalizirane.
3	Uloge i odgovornosti su u cijelosti definirane i formalno dokumentirane, ali nisu komunicirane relevantnim zaposlenicima koji su uključeni u provedbu sigurnosnih mjera.
4	Uloge i odgovornosti su formalizirane i komunicirane relevantnim zaposlenicima koji su uključeni u provedbu sigurnosnih mjera.
5	Uloge i odgovornosti su jasno definirane, formalizirane, komunicirane relevantnim zaposlenicima koji su uključeni u provedbu sigurnosnih mjera i revidirane i ažurirane u skladu s poslovnim potrebama i promjenama unutar subjekta.

Reference:

- **ISO/IEC 27001:2022** (5.3, A.5.3, A.5.4)
- **ISO 22301:2019** (5.3)
- **ISO/IEC 27005:2022**
- **NIST SP 800-53 Rev. 5** (PM-1, PM-2, RA-1)

ORG-002: Dodjela posebnih i kombiniranih uloga u kibernetičkoj sigurnosti

Ova kontrola osigurava da subjekt prilagodi dodjelu kibernetičkih uloga specifičnim potrebama i veličini subjekta, bilo kroz dedicirane pozicije za kibernetičku sigurnost ili kao dio postojećih radnih zaduženja. Manje organizacije često delegiraju kibernetičke odgovornosti zaposlenicima s postojećim zaduženjima, dok veće mogu zahtijevati poseban tim ili pojedince s posebnim ulogama i isključivom odgovornošću za sigurnost. Prilagodba uloga osigurava efikasno korištenje resursa i veći nadzor nad sigurnosnim mjerama.

U postupku provjere se analizira kako su sigurnosne odgovornosti delegirane unutar subjekta, jesu li dodijeljene uloge prilagođene veličini i potrebama subjekta te postoje li jasno definirane linije odgovornosti za one s kombiniranim ulogama. Dokumentacija o dodjeli uloga i komunikacija s osobljem ključni su faktori koji potvrđuju da svi relevantni zaposlenici razumiju i prihvaćaju svoje odgovornosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Osnovne odgovornosti i uloge u vezi s kibernetičkom sigurnošću nisu dodijeljene.
2	Osnovne odgovornosti i uloge su dodijeljene, ali nisu usklađene s potrebama subjekta.
3	Uloge su dodijeljene i usklađene s potrebama subjekta, ali postoji nejasnoća u vezi s linijama odgovornosti.
4	Uloge su dodijeljene uz jasnu liniju odgovornosti, ali nisu u potpunosti usklađene s veličinom i specifičnosti subjekta.
5	Uloge su dodijeljene uz jasnu liniju odgovornosti i u potpunosti usklađene s veličinom i specifičnosti subjekta.

Reference:

- **ISO/IEC 27001:2022** (5.3, A.5.3, A.5.4)
- **ISO 22301:2019** (5.3)
- **NIST SP 800-53 Rev. 5** (PM-1, PM-2, RA-1)
- **NIST CSF v2.0** (PR.AT-2)

ORG-003: Imenovanje odgovorne osobe za kibernetičku sigurnost na razini subjekta

Kontrola zahtijeva imenovanje dedicirane osobe operativno odgovorne za kibernetičku sigurnost na razini cijelog subjekta i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu. Osoba ima zadatak nadgledanja i koordinacije svih kibernetičkih sigurnosnih mjera unutar subjekta. Imenovanjem odgovorne osobe, subjekt osigurava centralizirano upravljanje sigurnosnim inicijativama i brže odgovaranje na prijetnje, što povećava ukupnu razinu sigurnosti. Također, odgovorna osoba za kibernetičku sigurnost mora imati neometan pristup potrebnim resursima i zaposlenicima zaduženim za provedbu sigurnosnih mjera. Time se omogućuje učinkovito upravljanje sigurnosnim aktivnostima, brza koordinacija i smanjivanje potencijalnih prepreka u implementaciji mjera. Osiguravanjem pravovremenog pristupa, odgovorna osoba može brže reagirati na sigurnosne prijetnje i prilagođavati mjere prema potrebi subjekta.

Provjerom se analizira dokumentacija koja potvrđuje imenovanje odgovorne osobe, kao i jasne definicije njezinih odgovornosti i ovlasti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nije imenovana osoba za kibernetičku sigurnost na razini subjekta.
2	Osoba je imenovana, ali nije formalizirana ni dokumentirana njena uloga.
3	Osoba je formalno imenovana, ali bez definiranih odgovornosti i bez osiguranja adekvatnog pristupa osobama odgovornim za provedbu mjera u subjektu.
4	Osoba je formalno imenovana, odgovornosti su djelomično definirane kao i adekvatni pristup osobama odgovornim za provedbu mjera u subjektu.
5	Osoba je formalno imenovana, odgovornosti su potpuno definirane kao i adekvatni pristup osobama odgovornim za provedbu mjera u subjektu.

Reference:

- **ISO/IEC 27001:2022** (5.3, A.5.3, A.5.4)
- **ISO 22301:2019** (5.3)
- **NIST SP 800-53 Rev. 5** (PM-1, PM-2, RA-1)

ORG-004: Disciplinske mjere za kršenje pravila kibernetičke sigurnosti

Ova kontrola zahtijeva uspostavu i primjenu adekvatnih disciplinskih mjera za zaposlenike u slučaju nepridržavanja pravila kibernetičke sigurnosti. Disciplinske mjere moraju biti usklađene s relevantnim zakonskim propisima i pravnim okvirima, ugovornim obvezama, poslovnim zahtjevima i internim aktima subjekta te prilagođene težini prekršaja i radnom mjestu zaposlenika. Njihova primjena mora uzeti u obzir razinu ozbiljnosti prekršaja i predviđene posljedice za zaposlenike. Sve disciplinske mjere moraju biti formalno dokumentirane i transparentno komunicirane zaposlenicima s ciljem povećanja sigurnosne svijest zaposlenika. Također, subjekt treba redovito evaluirati i prilagođavati definirane mjere kako bi osigurala njihovu usklađenost s regulatornim zahtjevima i poslovnim potrebama.

Provjera usklađenosti uključuje pregled dokumentacije koja definira disciplinske mjere, analizu njihove primjene te usklađenost s pravnim i internim pravilima subjekta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Disciplinske mjere ne postoje.
2	Postoje osnovne smjernice, ali nisu formalizirane ni dosljedno primjenjivane.
3	Formalizirane mjere postoje, ali nisu jasno prilagođene razini prekršaja ili nisu potpuno usklađene sa zakonodavstvom.
4	Disciplinske mjere su formalizirane, ali ne postoji sustavni mehanizam za njihovu redovitu analizu i prilagodbu.
5	Disciplinske mjere se dosljedno primjenjuju, evaluiraju i unaprjeđuju na temelju sustavne analize njihove učinkovitosti i usklađenosti sa zakonskim zahtjevima.

Reference:

- **ISO/IEC 27001:2022** (A.6.4)
- **NIST SP 800-53 Rev. 5** (PS-8)

ORG-005: Implementacija prava pristupa prema načelima poslovne potrebe i minimalnih ovlaštenja

Ova kontrola zahtijeva implementaciju prava pristupa mrežnim i informacijskim sustavima prema dodijeljenim poslovnim zaduženjima zaposlenika. Prava pristupa moraju biti usklađena s načelima „poslovne potrebe“, „minimalno potrebnih ovlaštenja za provedbu zadaća“ te „razdvajanja nadležnosti“. Subjekt mora:

- Definirati prava pristupa prema radnim ulogama i odgovornostima.
- Redovito pregledavati i ažurirati prava pristupa kako bi se uklonile nepotrebne privilegije.
- Osigurati dokumentaciju i nadzor sustava prava pristupa.

Provjera uključuje pregled dokumentacije prava pristupa i evidencija redovitih revizija. Evaluira se usklađenost s načelima „poslovne potrebe“ (*need-to-know)*, „minimalno potrebnih ovlaštenja za provedbu zadaća“ (*least privilege)* te „razdvajanja nadležnosti“ (*segregation of duties*).

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Prava pristupa nisu definirana ni dokumentirana.
2	Prava pristupa su djelomično definirana, ali nisu formalizirana niti sustavno primijenjena.
3	Prava pristupa su definirana i djelomično usklađena s načelima, uz povremene revizije.
4	Prava pristupa su formalizirana i dosljedno primijenjena, usklađena s načelima, redovito revidirana, a revizije su dokumentirane.
5	Prava pristupa su formalizirana i potpuno usklađena s načelima, sustavno nadzirana i revidirana, uz osigurane zamjenske osobe.

Reference:

- **ISO/IEC 27001:2022** (A.5.15, A.5.18, A.8.2)
- **NIST SP 800-53 Rev. 5** (AC-2, AC-5, AC-6, AC-17)

ORG-006: Definiranje i postizanje ciljeva oporavka poslovanja (RPO, RTO, SDO)

Ova kontrola osigurava definiranje, dokumentiranje i postizanje ciljeva oporavka poslovanja, uključujući RTO (*Recovery Time Objectives*), RPO (*Recovery Point Objectives*) i SDO (*Service Delivery Objectives*). Ciljevi moraju biti usklađeni s rezultatima analize utjecaja incidenata na poslovanje (BIA – *Business Impact Analysis*) te integrirani u planove kontinuiteta poslovanja (BCP – *Business Continuity Plan*), planove oporavka od ugroza (DRP – *Disaster Recovery Plan*) i politike pričuvnih kopija, upravljanja sigurnošću lanca opskrbe i sigurnosti sustava. Kontrola obuhvaća redovitu reviziju i ažuriranje ciljeva prema promjenama u poslovnim procesima i procjeni rizika.

Provjera uključuje pregled dokumentacije o RTO, RPO i SDO ciljevima, analizu integracije ovih ciljeva u ključne poslovne procese i sustave, pregled zapisa o revizijama i ažuriranjima ciljeva te konzultacije s odgovornim osobljem kako bi se osiguralo dosljedno provođenje. Također, obuhvaća provjeru povezanosti ciljeva s politikama pričuvnih kopija i upravljanjem kontinuitetom poslovanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ciljevi oporavka poslovanja (RPO, RTO, SDO) nisu definirani niti dokumentirani.
2	Osnovni ciljevi oporavka poslovanja su definirani za manji podskup poslovnih funkcija.
3	Ciljevi oporavka poslovanja su definirani, dokumentirani i djelomično ih je moguće postići, ali nisu redovito revidirani ili ažurirani.
4	Ciljevi oporavka poslovanja su definirani, dokumentirani te je napravljena osnovna analiza i usporedba s mogućnostima subjekta za postizanje istih za ključne poslovne funkcije.
5	Sveobuhvatni ciljevi oporavka poslovanja su definirani, dokumentirani, redovito revidirani i ažurirani te ih je moguće postići za sve ključne poslovne funkcije.

Reference:

- **ISO/IEC 27001:2022** (A.5.29)
- **ISO 22301:2019** (8.2.2, 8.2.3, 8.3.2, 8.4.2, 8.4.4, 8.4.5)
- **NIST SP 800-34 Rev. 1** (3.4)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-9)

ORG-007: Planiranje i dokumentacija aktivnosti kontinuiteta poslovanja (BCP/DRP)

Ova kontrola osigurava razvoj, održavanje i dokumentaciju planova za kontinuitet poslovanja (BCP – *Business Continuity Plan*) i oporavak od katastrofa (DRP – *Disaster Recovery Plan*). Fokusira se na definiranje ključnih elemenata, uključujući uloge i odgovornosti, ključne kontakte, komunikacijske kanale, uvjete aktivacije i deaktivacije s eskalacijskim nivoima, redoslijed postupanja kod oporavka, potrebne resurse te povezanost s postupanjima u slučaju incidenata. Kontrola obuhvaća periodično testiranje planova kroz vježbe, procjenu učinkovitosti i identifikaciju potrebnih poboljšanja temeljenih na rezultatima testiranja. Također uključuje osiguranje povezanosti planova s mrežnim i informacijskim sustavima, redundancijama, pričuvnim kopijama i alternativnim izvorima energije.

Provjera uključuje analizu dokumentacije planova BCP i DRP, pregled zapisa o testiranjima, evaluaciju rezultata vježbi i provedbe poboljšanja, konzultacije s odgovornim osobljem te provjeru povezanosti planova s definiranim resursima, mrežnim i informacijskim sustavima, redundancijama i pričuvnim kopijama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Planovi kontinuiteta poslovanja nisu razvijeni niti dokumentirani.
2	Osnovni planovi su razvijeni, ali nisu sveobuhvatni niti redovito testirani.
3	Planovi su dokumentirani i djelomično testirani, ali nisu ažurirani prema promjenama.
4	Sveobuhvatni planovi su razvijeni, dokumentirani i redovito testirani kroz vježbe.
5	Planovi su potpuno integrirani, automatizirani i kontinuirano ažurirani temeljem vježbi.

Reference:

- **ISO/IEC 27001:2022** (A.5.29)
- **ISO 22301:2019** (8.2.2, 8.2.3, 8.3.2, 8.4.2, 8.4.4, 8.4.5)
- **NIST SP 800-34 Rev. 1** (3.5, 3.6)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-3, CP-4)

EDU-001: Upoznavanje zaposlenika s ključnim odrednicama kibernetičke sigurnosne politike

Ova kontrola osigurava da svi zaposlenici, a posebno osobe odgovorne za provedbu mjera, budu upoznati s ključnim odrednicama kibernetičke sigurnosne politike, posebno u vezi s upravljanjem sigurnosnim rizicima i njihovim potencijalnim utjecajem na usluge i aktivnosti subjekta. Redovite obuke pomažu u razumijevanju rizika i stvaranju kulture sigurnosti unutar subjekta.

U postupku provjere se analizira sadržaj edukacijskih programa usmjerenih na podizanje svijesti o kibernetičkim prijetnjama i važnosti upravljanja rizicima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Zaposlenici nisu upoznati s ključnim elementima politike.
2	Postoji osnovni program edukacije, ali nije formaliziran ili se ne provodi redovito.
3	Edukacija se provodi, ali ne obuhvaća sve potrebne elemente posebno u vezi s upravljanjem sigurnosnim rizicima i njihovim potencijalnim utjecajem na usluge i aktivnosti subjekta ili nije dostupna svim relevantnim zaposlenicima.
4	Edukacija obuhvaća sve potrebne elemente i dostupna je svim relevantnim zaposlenicima.
5	Edukacija je potpuno implementirana i uz sve potrebne elemente provodi se redovito za sve zaposlenike.

Reference:

- **ISO/IEC 27001:2022** (A.5.4, A.6.3)
- **ISO 22301:2019** (7.3)
- **NIST SP 800-53 Rev. 5** (AT-2, AT-3, PM-13)
- **NIST CSF v2.0** (PR.AT-1)

EDU-002: Upoznavanje poslovnih partnera s ključnim odrednicama kibernetičke sigurnosne politike

Ova kontrola osigurava da su poslovni partneri subjekta, poput dobavljača i pružatelja usluga, upoznati s relevantnim dijelovima kibernetičke sigurnosne politike koji utječu na njihovu suradnju sa subjektom. Informiranjem partnera o sigurnosnim očekivanjima, subjekt smanjuje rizik od neusklađenih sigurnosnih praksi koje bi mogle dovesti do incidenata. Ovo također jača međusobno povjerenje i odgovornost između subjekta i njihovih partnera.

Postupkom se provjerava postoje li dokazi o formalnom obavještavanju poslovnih partnera, kao i je li sadržaj koji im se prenosi prilagođen specifičnostima njihovog odnosa sa subjektom. Provjerava se postoje li dokumenti kao što su smjernice, ugovorne klauzule, aneksi ili zapisnici sa sastanka na kojima se prenose očekivanja o ispunjenju sigurnosnih obveza, kao i povratne informacije partnera o razumijevanju tih očekivanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Poslovni partneri nisu informirani o glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose.
2	Informacije se prenose povremeno i nisu formalizirane, primjerice u obliku smjernica, ugovornih odredbi ili zapisnika sa sastanka.
3	Postoji kontinuirana komunikacija, ali ne obuhvaća sve relevantne dijelove politike niti je formalizirana.
4	Informacije se redovito prenose i obuhvaćaju sve relevantne dijelove politike, ali postoje manji nedostaci u dokumentaciji.
5	Informacije su redovito prenesene, obuhvaćaju sve relevantne dijelove politike, i formalizirane su u obliku smjernica, ugovornih odredbi ili zapisnika sa sastanka i prilagođene svakom poslovnom partneru prema njihovoj ulozi.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20, A.5.21)
- **ISO 22301:2019** (7.3)
- **NIST SP 800-53 Rev. 5** (SA-9, SR-3, PS-7)

EDU-003: Edukativne aktivnosti za podizanje svijesti o kibernetičkim sigurnosnim rizicima

Cilj ove kontrole je osigurati redovne edukativne aktivnosti poput radionica i seminara usmjerenih na upravljanje kibernetičkim rizicima i njihovim mogućim utjecajem na poslovanje. Pravilno strukturirane edukacije omogućuju informiranost o trenutnim izazovima i pomažu u održavanju visoke razine sigurnosti unutar subjekta.

Procjenjuje se učestalost i kvaliteta organiziranih edukativnih aktivnosti te analizira koliko su ove aktivnosti usklađene s aktualnim prijetnjama i potrebama subjekta. Također se provjerava dokumentacija o sudjelovanju i povratnim informacijama polaznika kako bi se procijenila učinkovitost edukacija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Edukativne aktivnosti za podizanje svijesti ne postoje.
2	Edukativne aktivnosti za podizanje svijesti postoje, ali nisu formalizirane.
3	Edukativne aktivnosti za podizanje svijesti postoje i formalizirane su, ali ne provode se redovito.
4	Edukativne aktivnosti za podizanje svijesti postoje i formalizirane su te se provode redovito uz povremene nedostatke u prilagodbi trenutnim potrebama subjekta.
5	Edukativne aktivnosti za podizanje svijesti postoje i formalizirane su te prilagođene trenutnim potrebama subjekta i redovito se provode.

Reference:

- **ISO/IEC 27001:2022** (A.5.4, A.6.3)
- **ISO 22301:2019** (7.3)
- **ENISA Interoperable Risk Management Framework**
- **NIST SP 800-53 Rev. 5** (AT-2, AT-3, AT-6)
- **NIST CSF v2.0** (PR.AT-1)

EDU-004: Angažman upravljačkog tijela u sigurnosnim inicijativama

Ova kontrola osigurava da je upravljačko tijelo subjekta aktivno uključeno u aktivnosti kibernetičke sigurnosti kroz redovne edukacije i angažman u sigurnosnim inicijativama. Takva uključenost osigurava da donosioci odluka imaju jasnu sliku o potencijalnim prijetnjama, rizicima i potrebnim mjerama, što omogućava donošenje proaktivnih odluka o sigurnosnim strategijama.

Revizori ispituju dokumentaciju koja pokazuje sudjelovanje upravljačkog tijela u sigurnosnim inicijativama te analizira raspoložive materijale i povratne informacije o angažmanu uprave. Također se procjenjuje kontinuitet edukacija i sudjelovanje uprave u redovnim sigurnosnim sastancima ili radionicama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Upravljačko tijelo nije uključeno u aktivnosti kibernetičke sigurnosti.
2	Upravljačko tijelo povremeno sudjeluje u edukacijama, ali bez redovitih ili formaliziranih aktivnosti.
3	Upravljačko tijelo povremeno sudjeluje u redovnim edukacijama uz formalizirane aktivnosti i uloge.
4	Upravljačko tijelo redovito sudjeluje u aktivnostima, uz manja odstupanja u angažmanu ili pokrivenosti tema.
5	Upravljačko tijelo je potpuno angažirano u redovnim sigurnosnim aktivnostima i donosi strateške odluke temeljene na edukacijama.

Reference:

- **ISO/IEC 27001:2022** (5.3, 6.3)
- **ISO 22301:2019** (5.3, 6.2)
- **ENISA Interoperable Risk Management Framework**
- **NIST SP 800-53 Rev. 5** (PM-3, PM-16)

EDU-005: Upute o procedurama upravljanja rizicima

Kontrola zahtijeva izradu i distribuciju uputa, a na osnovu procesa upravljanja rizicima koje obuhvaćaju sve aspekte upravljanja rizicima. Upute trebaju pružiti korake za identifikaciju, analizu, evaluaciju i obradu rizika, uz objašnjenje konkretnih scenarija i primjera iz poslovne prakse. Upute bi trebale biti prilagođene različitim razinama zaposlenika koji su odgovorni za segmente poslovanja subjekta povezane s rizicima i njihovim povezanim funkcijama unutar subjekta. Poseban fokus treba biti na edukaciji zaposlenika o rizicima koji bi mogli utjecati na dostupnost, povjerljivost, autentičnost, integritet i cjelovitost sustava.

Provjerava se postoje li upute, jesu li redovito ažurirane, jasno strukturirane i lako dostupne zaposlenicima koji su odgovorni za segmente poslovanja subjekta povezane s rizicima. Također, treba ocijeniti u kojoj mjeri zaposlenici razumiju i pridržavaju se uputa kroz individualne intervjue.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Upute o upravljanju rizicima ne postoje.
2	Postoje osnovne upute, ali nisu formalizirane.
3	Upute su formalizirane, ali nisu dostupne svim zaposlenicima koji su odgovorni za segmente poslovanja subjekta povezane s rizicima.
4	Upute su formalizirane i dostupne svim zaposlenicima koji su odgovorni za segmente poslovanja subjekta povezane s rizicima.
5	Upute su potpuno implementirane, prilagođene potrebama zaposlenika, redovito se ažuriraju i dostupne su svim zaposlenicima koji su odgovorni za segmente poslovanja subjekta povezane s rizicima.

Reference:

- **ISO/IEC 27001:2022** (A.5.4, A.6.3)
- **ISO 22301:2019** (6.1, 6.2, 8.2)
- **ISO/IEC 27005:2022**
- **ENISA Interoperable Risk Management Framework**
- **NIST SP 800-53 Rev. 5** (RA-1)
- **NIST CSF v2.0** (PR.AT-1)

EDU-006: Program osposobljavanja zaposlenika o specifičnim mjerama kibernetičke sigurnosti

Ova kontrola zahtijeva uspostavu formalnog i dokumentiranog programa osposobljavanja za zaposlenike čije radne uloge uključuju projektiranje, nadzor, provođenje ili reviziju mjera kibernetičke sigurnosti. Program mora:

- Uključivati upute za sigurno rukovanje mrežnim i informacijskim sustavima.
- Obuhvatiti redovno informiranje o poznatim kibernetičkim prijetnjama.
- Definirati postupanje prilikom incidenata.
- Prilagoditi sadržaj specifičnim potrebama radnih mjesta, poput IT administratora koji moraju imati dodatnu edukaciju o sigurnim konfiguracijama.

Provjera se provodi pregledom dokumentiranog programa, evidencija o sudionicima edukacije i evaluacijom učinkovitosti programa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Program osposobljavanja nije uspostavljen niti dokumentiran.
2	Program je djelomično uspostavljen, ali nije dokumentiran.
3	Program je dokumentiran i djelomično implementiran za sve uloge.
4	Program je u potpunosti implementiran za sve relevantne uloge.
5	Program dokumentiran, u potpunosti implementiran, redovito ažuriran i evaluiran prema potrebama subjekta.

Reference:

- **ISO/IEC 27001:2022** (A.5.2, A.6.3)
- **ISO 22301:2019** (6.2, 7.3, 8.4)
- **NIST SP 800-53 Rev. 5** (AT-3, AT-6, IR-2)
- **NIST CSF v2.0** (PR.AT-1, PR.AT-2)

EDU-007: Program osposobljavanja o osnovnim praksama kibernetičke higijene

Ova kontrola zahtijeva uspostavu, redovitu provedbu i redovno ažuriranje programa podizanja svijesti o osnovnim praksama kibernetičke higijene i prepoznavanju prijetnji. Program mora:

- Obuhvatiti osnovne IT vještine, uključujući sigurno korištenje elektroničke pošte i Interneta.
- Pružiti smjernice o sigurnom korištenju autentifikacijskih sredstava i vjerodajnica.
- Uključivati dokumentirane upute o prijavi i postupanju u slučaju incidenata.

Provjera usklađenosti uključuje pregled dokumentacije programa, evidencije o sudionicima obuke i evaluacije programa od strane zaposlenika te konzultacije s odgovornim osobljem za obuku i sigurnost. Također se provjerava redovitost i prilagodba obuka poslovnim potrebama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Program nije uspostavljen i podizanje svijesti o osnovnim praksama kibernetičke higijene ne postoji.
2	Program nije uspostavljen, ali se podizanje svijesti o osnovnim praksama kibernetičke higijene sporadično provodi u praksi.
3	Program je dokumentiran i provodi se djelomično za sve zaposlenike.
4	Program se redovno provodi za sve relevantne zaposlenike te se mjeri njegova učinkovitost – kroz dokumentirana mjerenja.
5	Program je ažuriran prema trenutnim potrebama i rizicima kojima je subjekt izložen, te se dodatno usavršava temeljem prikupljenih povratnih informacije od zaposlenika.

Reference:

- **ISO/IEC 27001:2022** (A.5.27, A.6.3)
- **ISO 22301:2019** (7.3, 8.4)
- **NIST SP 800-53 Rev. 5** (AT-2)
- **NIST CSF v2.0** (PR.AT-1, PR.AT-2)

EDU-008: Program obuke za odgovor na incidente

Ova kontrola zahtijeva razvoj i provedbu specijalizirane obuke za ključne osobe koje sudjeluju u procesu odgovora na incidente. Program mora uključivati stručno usavršavanje, praktične scenarije, simulacije incidenata i redovite vježbe kako bi se osigurala spremnost sudionika za učinkovito reagiranje. Program obuke treba biti usklađen s kibernetičkom sigurnosnom politikom subjekta i ažuriran na temelju promjenjivih prijetnji i najboljih praksi.

Evaluacija uključuje pregled programa i rasporeda obuke, analizu dokumentacije i povratne informacije sudionika. Također se provjerava učestalost i kvaliteta ažuriranja programa obuke kako bi bila prilagođena novim izazovima u području kibernetičke sigurnosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Program obuke nije uspostavljen.
2	Postoji osnovna razina obuke za odgovor na incidente, ali nije strukturirana niti redovito provedena. Obuhvaća teorijske prezentacije bez praktičnih scenarija ili simulacija. Ne postoji mehanizam za procjenu učinkovitosti obuke ni prikupljanje povratnih informacija.
3	Subjekt provodi dokumentirani program obuke za ključne osobe koje sudjeluju u odgovoru na incidente. Program uključuje osnovno stručno usavršavanje, simulacije i praktične scenarije koji pokrivaju faze odgovora (primjerice prema PICERL modelu).
4	Postoji sveobuhvatan i redovito održavan program obuke usklađen s kibernetičkom sigurnosnom politikom subjekta. Obuka uključuje praktične vježbe. Svi relevantni sudionici obavezno sudjeluju, a program se ažurira na temelju promjena u prijetnjama, novim tehnologijama i lekcijama iz prethodnih incidenata. Povratne informacije se analiziraju i koriste za poboljšanje sadržaja i metoda isporuke.
5	Subjekt ima napredan, integriran i stalno ažuriran program specijalizirane obuke za sve dionike u odgovoru na incidente. Program uključuje razne formate praktičnih vježbi. Evaluacija učinka obuke je metodična, kvantitativna i povezana s unapređenjem performansi tima. Pristup je orijentiran na stalno povećanje spremnosti i otpornosti.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.26, A.5.27, A.6.3, A.6.8)
- **ISO 22301:2019** (8.4, 8.5, 8.6)
- **NIST SP 800-53 Rev. 5** (IR-2, AT-3, CP-4)
- **NIST CSF v2.0** (Kategorija RS.MA)

EDU-009: Sustavi digitalnog učenja za kontinuiranu obuku i certifikaciju

Ova kontrola zahtijeva uspostavu i korištenje sustava za udaljeno digitalno učenje s ciljem kontinuirane obuke i certifikacije zaposlenika u području kibernetičke sigurnosti. Sustav mora omogućiti fleksibilan pristup učenju, praćenje napretka sudionika te integraciju s programima osposobljavanja specifičnim za subjekt. Poseban naglasak stavlja se na upravljanje rizicima i razumijevanje njihovog utjecaja na poslovne procese i pružanje usluga.

Pregled kontrole uključuje evaluaciju funkcionalnosti sustava, kvalitetu sadržaja obuke, relevantnost certifikacija te učestalost i dosljednost korištenja sustava od strane zaposlenika. Također se analizira način prilagodbe sustava specifičnim potrebama subjekta, uključujući tehničku podršku i ažuriranje sadržaja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za udaljeno digitalno učenje nije implementiran.
2	Sustav postoji, ali s ograničenim sadržajem ili tehničkom funkcionalnošću.
3	Sustav omogućuje osnovnu obuku, ali nije namijenjen za kontinuiranu primjenu.
4	Sustav je funkcionalan, uključuje redovita ažuriranja, proširenja i certifikacijske programe.
5	Sustav je potpuno integriran u procese subjekta i osigurava kontinuiranu primjenu.

Reference:

- **ISO/IEC 27001:2022** (7.2, A.6.3)
- **ISO 22301:2019** (7.2)
- **NIST CSF v2.0** (PR.AT-1)

EDU-010: Implementacija testiranja socijalnog inženjeringa i simulacija krađe identiteta

Ova kontrola zahtijeva redovito provođenje testiranja socijalnog inženjeringa i simulacija krađe identiteta (*phishing*) s ciljem identificiranja ranjivosti zaposlenika i poboljšanja njihovih sposobnosti prepoznavanja i odgovora na prijetnje. Aktivnosti uključuju pripremu edukativnih materijala, organizaciju radionica i praktičnih vježbi kako bi se osiguralo razumijevanje sigurnosnih rizika i jačala otpornost zaposlenika na prijetnje.

Prilikom provjere usklađenosti analizira se dokumentacija o provedenim testiranjima, planovima vježbi i povratnim informacijama zaposlenika. Posebna pažnja posvećuje se učestalosti simulacija i njihovoj relevantnosti za poslovne procese subjekta, kao i kontinuiranoj prilagodbi edukativnih materijala na temelju rezultata ovih aktivnosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne provodi se testiranje socijalnog inženjeringa i simulacija *phishinga*.
2	Povremene aktivnosti postoje, ali nisu dokumentirane niti redovite.
3	Aktivnosti su djelomično dokumentirane i provode se redovito.
4	Aktivnosti su u potpunosti dokumentirane i redovite.
5	Aktivnosti su potpuno integrirane u sigurnosne procese subjekta i kontinuirano optimizirane.

Reference:

- **ISO/IEC 27001:2022** (A.6.3)
- **ISO 22301:2019** (8.5)
- **NIST SP 800-53 Rev. 5** (AT-2, CA-8)

EDU-011: Obuka za analizu i upravljanje dnevničkim zapisima

Kontrola osigurava redovitu obuku osoblja za praćenje, analizu i upravljanje dnevničkim zapisima. Program obuke uključuje korištenje alata za detekciju i analizu sumnjivih aktivnosti, tumačenje dnevničkih zapisa te upravljanje sustavima za njihovo bilježenje i pohranu.

Provjera usklađenosti uključuje pregled programa obuke, evidencije sudionika i rezultata evaluacija znanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Obuka za analizu i upravljanje dnevničkim zapisima nije provedena.
2	Provedena je osnovna obuka, ali bez praktičnih elemenata.
3	Obuka uključuje osnovne analitičke alate i upravljanje dnevničkim zapisima.
4	Redovita obuka s praktičnim testovima je provedena.
5	Obuka uključuje napredne analitičke alate i simulacije.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.27, A.5.28, A.6.3)
- **NIST SP 800-53 Rev. 5** (AU-2, AU-6, AU-12, IR-4)
- **NIST CSF v2.0** (DE.AE-2, Kategorija RS.AN)

RES-001: Osiguranje financijskih sredstava za mjere kibernetičke sigurnosti

Ova kontrola osigurava da subjekt ima odgovarajuće financijske resurse za implementaciju mjera upravljanja kibernetičkim sigurnosnim rizicima. Financijska sredstva ključna su za nabavu sigurnosnih alata, provedbu obuka i podršku stručnjacima u održavanju visoke razine zaštite. Redovita godišnja procjena financijskih potreba i prilagodba sredstava ključni su za osiguranje kontinuiteta i učinkovitosti sigurnosnih mjera.

Procjenjuje se dokumentacija o dodijeljenim financijskim sredstvima te prate promjene u financijskom planiranju za aktivnosti vezane uz sigurnost i povećanje otpornosti. Analizira se provodi li subjekt redovitu procjenu financijskih resursa i prilagođava li ih temeljem sigurnosnih potreba i promjena u rizicima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Financijska sredstva za kibernetičku sigurnost nisu osigurana.
2	Financijska sredstva su planirana, ali nisu usklađena s aktualnim potrebama subjekta.
3	Financijska sredstva su usklađena i provodi se djelomična procjena i prilagodba resursa.
4	Provodi se godišnja procjena i djelomična prilagodba financijskih resursa.
5	Financijska sredstva u potpunosti slijede potrebe subjekta, redovito su revidirana i prilagođena trenutnim rizicima i potrebama.

Reference:

- **ISO/IEC 27001:2022** (6.2, 7.1, 8.3)
- **ISO 22301:2019** (6.2, 7.1, 8.3)
- **ISO/IEC 27005:2022**
- **NIST SP 800-53 Rev. 5** (PM-3)

RES-002: Tehnički alati za provedbu mjera upravljanja rizicima

Ova kontrola osigurava dostupnost i primjenu potrebnih tehničkih alata za provedbu mjera zaštite. Alati kao što su antivirusni sustavi, sustavi za otkrivanje upada i alati za praćenje mrežne aktivnosti ključni su za učinkovitu provedbu sigurnosnih mjera i za pravovremenu reakciju na prijetnje. Bez odgovarajućih alata, postoji povećan rizik od ranjivosti i mogućih incidenata. Subjekt mora redovito provoditi procjenu postojećih tehničkih alata i prilagođavati ih sigurnosnim zahtjevima kako bi osigurao njihovu učinkovitost.

U postupku se provjerava jesu li dostupni i funkcionalni odgovarajući tehnički alati koji omogućuju implementaciju sigurnosnih mjera te analiziraju jesu li alati redovito nadograđivani i prilagođeni promjenama u prijetnjama. Analiziraju se specifikacije alata, njihova usklađenost s potrebama subjekta i provode li se redovite nadogradnje i održavanje. Na taj se način procjenjuje koliko su alati učinkoviti i prilagođeni trenutnim sigurnosnim zahtjevima. Također se ispituje vodi li se dokumentacija o godišnjoj procjeni tehničkih alata i kako se na temelju nje donose odluke o nadogradnji i zamjeni zastarjelih rješenja.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Tehnički alati nisu dostupni niti planirani.
2	Postoje osnovni alati, ali nisu redovito održavani ili prilagođeni potrebama.
3	Dostupni su tehnički alati, povremeno su ažurirani, ali njihova funkcionalnost nije u potpunosti usklađena s potrebama subjekta.
4	Alati su funkcionalni, redovito ažurirani, provodi se godišnja procjena njihove učinkovitosti i prilagodba sigurnosnim potrebama, a njihova primjena zadovoljava većinu sigurnosnih potreba subjekta.
5	Tehnički alati su potpuno funkcionalni, redovito ažurirani i usklađeni s potrebama subjekta, uz dokumentirani postupak njihove godišnje evaluacije i prilagodbe.

Reference:

- **ISO/IEC 27002:2022** (A.8.15, A.8.16)
- **NIST SP 800-53 Rev. 5** (SI-3, SI-4, RA-5)
- **NIST CSF v2.0** (Kategorija DE.CM)

RES-003: Ljudski resursi s potrebnim stručnim znanjima

Kontrola osigurava da subjekt ima stručno osoblje za provedbu i nadzor kibernetičke sigurnosti, s odgovarajućim znanjima i vještinama. Kompetentno osoblje je ključno za održavanje i unaprjeđenje mjera sigurnosti, a redovita procjena ljudskih resursa omogućuje subjektu da pravovremeno reagira na potrebe za dodatnom edukacijom ili zapošljavanjem stručnjaka. U slučaju nedostatka stručnjaka, postoji povećan rizik od pogrešaka u provedbi mjera, zakašnjenja u odgovoru ili pak neodgovaranja na incidente.

Ocjenjuju se kvalifikacije i dostupnost osoblja zaduženog za kibernetičku sigurnost te postoje li programi za kontinuiranu edukaciju i profesionalni razvoj. Uz to, ispituju se planovi za osiguranje ljudskih resursa, uključujući postupke za popunjavanje pozicija u slučaju nedostatka kadra, kako bi subjekt imao potrebne vještine za sigurnosne izazove. Analizira se provodi li subjekt godišnju procjenu potrebnih ljudskih resursa i prilagođava li svoje kapacitete sigurnosnim potrebama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji osoblje s potrebnim znanjima za provedbu sigurnosnih mjera.
2	Postoji osnovno osoblje, ali s ograničenim znanjima i vještinama.
3	Osoblje postoji, ali s nedostatnim znanjima ili bez mogućnosti kontinuirane edukacije.
4	Osoblje s potrebnim znanjima postoji, djelomično pokriva sigurnosne potrebe subjekta, povremeno sudjeluje na edukacijama, a provodi se i godišnja procjena resursa.
5	Osoblje s visokim kompetencijama potpuno pokriva sigurnosne potrebe, redovito sudjeluje u edukacijama, a ljudski resursi se procjenjuju i prilagođavaju na temelju sigurnosnih zahtjeva.

Reference:

- **ISO/IEC 27001:2022** (7.2, 7.3, A.6.3)
- **ISO 22301:2019** (7.2, 7.3)
- **NIST SP 800-53 Rev. 5** (AT-3, PM-14)
- **NIST CSF v2.0** (Kategorija PR.AT)

RES-004: Provjera kandidata prije zapošljavanja

Ova kontrola osigurava da subjekt provodi sustavne provjere kvalifikacija i adekvatnosti kandidata prije zapošljavanja, sukladno značaju radnog mjesta, važećim propisima i sigurnosnim zahtjevima. Provjere mogu uključivati provjeru referenci, valjanost certifikata i diploma, pismene i usmene testove te dostavu potvrda o nekažnjavanju za određene pozicije. Subjekt mora definirati jasne kriterije provjere, uskladiti ih s poslovnim i sigurnosnim potrebama te osigurati njihovu proporcionalnost i zakonitost.

Provjerava se postoji li formaliziran proces provjere kandidata prije zapošljavanja te analizira se jesu li definirani jasni kriteriji za provjeru kvalifikacija i sigurnosnih aspekata. Ispituje se primjena tih postupaka u praksi, uključujući dosljednost provođenja provjera za različite razine odgovornosti. Također, analizira se dokumentacija o provedenim provjerama kako bi utvrdili njihovu usklađenost s regulatornim zahtjevima i poslovnim potrebama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne provodi se nikakva provjera adekvatnosti i kvalifikacija kandidata prije zapošljavanja.
2	Provjera se provodi bez jasnih kriterija ili formalne dokumentacije.
3	Postoji definirana procedura provjere, ali nije sustavno primjenjivana ili prilagođena različitim razinama odgovornosti.
4	Provjera se redovito provodi, dokumentirana je i usklađena s poslovnim zahtjevima, ali nema sustavne evaluacije.
5	Sustav provjere adekvatnosti i kvalifikacija potpuno je definiran, redovito se provodi, dokumentiran je te evaluiran i prilagođen rizicima, propisima i poslovnim potrebama.

Reference:

- **ISO/IEC 27001:2022** (A.6.1, A.6.2)
- **NIST SP 800-53 Rev. 5** (PS-3)

RES-005: Implementacija redundancije za mrežne i informacijske sustave

Kontrola zahtijeva uspostavu redundancije za kritične mrežne i informacijske sustave s ciljem osiguravanja njihove dostupnosti čak i u slučaju kvarova. Redundancija može uključivati RAID polja diskova, više podatkovnih centara, redundantne mrežne uređaje i poslužitelje iza sustava za raspodjelu opterećenja. Ovaj proces obuhvaća tehničke analize i planiranje resursa.

Pregledava se tehnička dokumentacija o implementaciji redundancije, rezultati testiranja otpornosti sustava i njihova usklađenost s definiranim zahtjevima. Također se analizira učestalost provjera i ažuriranja ovih sustava.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Redundancija nije implementirana.
2	Redundancija je djelomično implementirana, ali nije dokumentirana.
3	Redundancija je implementirana za dio kritičnih sustava i dokumentirana sukladno potrebama.
4	Redundancija je implementirana za sve kritične sustave i testirana povremeno.
5	Redundancija je potpuno implementirana, dokumentirana i redovito testirana.

Reference:

- **ISO/IEC 27001:2022** (A.5.30)
- **NIST SP 800-53 Rev. 5** (CP-6, CP-7, SC-36)

RES-006: Implementacija redundancije za ključnu imovinu

Redundancija ključne imovine osigurava kontinuitet operacija kroz postojanje rezervnih objekata, opreme i zaliha. Kontrola zahtijeva jasno definiranje ključne imovine i planiranje potrebnih rezervi. Ključni aspekt je dokumentacija koja pokriva procese održavanja i testiranja rezervnih resursa. Naglasak je na optimizaciji raspoloživih sredstava kako bi se smanjio rizik prekida poslovanja. Redovito revidiranje planova redundancije omogućuje njihovu usklađenost s promjenjivim operativnim potrebama i novim rizicima.

Provjerava se dokumentacija koja pokriva planove redundancije, uključujući popise ključne imovine i zaliha. Evaluiraju se metode održavanja rezervnih resursa i njihova dostupnost u slučaju potrebe.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Redundancija za ključnu imovinu nije planirana bez obzira na utvrđenu potrebu.
2	Postoje planovi, ali nisu dokumentirani niti implementirani.
3	Redundancija je djelomično implementirana i dokumentirana.
4	Redundancija je potpuno implementirana za većinu ključne imovine.
5	Redundancija je implementirana i sustavno provjeravana.

Reference:

- **ISO/IEC 27001:2022** (A.5.30)
- **NIST SP 800-53 Rev. 5** (RA-9)

RES-007: Redundancija zaposlenika s nužnim odgovornostima, ovlastima i sposobnostima

Kontrola osigurava da su ključne uloge unutar subjekta pokrivene dodatnim ili zamjenskim osobljem s potrebnim ovlastima i vještinama. Cilj je smanjiti ovisnost o pojedinačnim zaposlenicima. Posebna pažnja posvećuje se procesu obuke zamjenskog osoblja i ažuriranju njihovih kompetencija u skladu s poslovnim potrebama. Planiranje uključuje evaluaciju rizika povezanih s ljudskim resursima i identifikaciju kritičnih uloga koje zahtijevaju zamjensko osoblje.

Analiziraju se procesi za identifikaciju zamjenskog osoblja, planovi obuke i raspodjela uloga. Također se razmatra kako zamjensko osoblje doprinosi kontinuitetu ključnih poslovnih funkcija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nisu definirani zamjenski zaposlenici za ključne uloge.
2	Zamjenski zaposlenici su identificirani, ali nisu obučeni.
3	Zamjenski zaposlenici su djelomično obučeni.
4	Zamjenski zaposlenici su obučeni za sve ključne zadatke.
5	Zamjenski zaposlenici su potpuno osposobljeni i njihova uloga je testirana.

Reference:

- **ISO 22301:2019** (7.2, 8.4.2)
- **NIST SP 800-53 Rev. 5** (AT-3, CP-2, PM-13)

RES-008: Implementacija redundancije za komunikacijske kanale

Redundancija komunikacijskih kanala obuhvaća uspostavu alternativnih sredstava komunikacije za osiguranje neprekidne razmjene informacija. Kontrola uključuje identificiranje kritičnih komunikacijskih kanala i osiguranje rezervnih opcija. Posebna pozornost posvećuje se sigurnosti i otpornosti alternativnih kanala kako bi se spriječili sigurnosni rizici i prekidi u komunikaciji.

Procjenjuje se tehnička dokumentacija o alternativnim komunikacijskim kanalima i njihova usklađenost s definiranim standardima. Pregledavaju se rezultati testiranja funkcionalnosti i planovi za održavanje tih kanala.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nisu definirani alternativni komunikacijski kanali.
2	Alternativni kanali su definirani, ali nisu implementirani.
3	Alternativni kanali su djelomično implementirani.
4	Alternativni kanali su potpuno implementirani i testirani.
5	Alternativni kanali su potpuno funkcionalni i redovito testirani.

Reference:

- **ISO/IEC 27001:2022** (A.5.29, A.5.30)
- **ISO 22301:2019** (8.4.3)
- **NIST SP 800-53 Rev. 5** (CP-8)

RES-009: Implementacija redundancije za ključne komunalne usluge

Ova kontrola osigurava rezervne izvore ključnih komunalnih usluga, uključujući električnu energiju, vodu i grijanje. Cilj je minimizirati rizik prekida usluga koje su kritične za poslovanje. Planiranje redundancije uključuje procjenu dostupnih resursa i ulaganje u rezervne kapacitete poput generatora, spremnika vode i redundanciju infrastrukture. Kontrola također obuhvaća planove za održavanje i testiranje sustava. Svi implementirani sustavi moraju biti redovito provjeravani kako bi se osigurala njihova spremnost za krizne situacije.

Provjeravaju se planovi za osiguranje rezervnih izvora usluga, uključujući tehničke karakteristike i kapacitete. U obzir se uzimaju i učestalost provjera sustava te njihova otpornost na krizne situacije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Redundancija komunalnih usluga nije planirana bez obzira na utvrđenu potrebu.
2	Postoje planovi, ali nisu implementirani.
3	Redundancija je djelomično implementirana.
4	Redundancija je potpuno implementirana i povremeno testirana.
5	Redundancija je implementirana, testirana i redovito održavana.

Reference:

- **ISO/IEC 27001:2022** (A.5.29, A.5.30)
- **ISO 22301:2019** (8.3.4)
- **NIST SP 800-53 Rev. 5** (CP-8)
- **CIS v8** (15.4)

UPR-001: Mehanizmi za sudjelovanje odgovornih osoba u provođenju mjera i promociji kontinuiranog unaprjeđenja kibernetičke sigurnosti

Ova kontrola osigurava da subjekt ima osigurane i uspostavljene mehanizme za sudjelovanje osoba odgovornih za kibernetičku sigurnost u inicijativama i donošenju odluka o sigurnosnim prioritetima. Mehanizmi podrazumijevaju uključenost navedenih osoba u strateške procese, radne skupine i odbore posvećene sigurnosnim pitanjima te transparentan protok informacija između operativnog tima za kibernetičku sigurnost i upravljačkog tijela subjekta. Pravovremena i točna razmjena informacija ključna je za donošenje informiranih odluka i omogućava upravljačkom tijelu da procijeni trenutačno stanje sigurnosnih mjera te podrži inicijative za poboljšanje. Povećana transparentnost komunikacije osigurava bolje usklađivanje ciljeva između operativnog tima i upravljačkog tijela. Primjenom navedenih mehanizama subjekt osigurava redovit angažman osoba odgovornih za sigurnost u procjeni prijetnji, prilagodbi sigurnosnih mjera i poboljšanju postojećih praksi, a njihova aktivna uloga omogućuje bolje razumijevanje sigurnosnih rizika i usklađivanje mjera s poslovnim ciljevima subjekta.

U postupku se provjerava dokumentacija koja potvrđuje sudjelovanje ključnih osoba odgovornih za sigurnost u sastancima i radnim skupinama, učestalost i sadržaj tih sastanaka, te kako se zaključci, sigurnosne odluke i preporuke komuniciraju unutar subjekta. Također analiziraju postoji li transparentna evidencija o odlučivanju i je li osigurana dvosmjerna razmjena informacija (između upravljačkog tijela i operativnog tima i obratno) koja omogućuje prilagodbu sigurnosnih mjera u skladu s operativnim potrebama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Mehanizmi sudjelovanja nisu uspostavljeni.
2	Mehanizmi postoje, ali nisu adekvatno dokumentirani ili ne omogućuju dosljedno sudjelovanje odgovornih osoba i članova upravljačkog tijela.
3	Mehanizmi su uspostavljeni i postoji dokumentacija, ali sudjelovanje nije redovito ili ne postoji redovita razmjena informacija.
4	Mehanizmi su uspostavljeni, postoji dokumentacija, sudjelovanje je redovito i uključuje većinu odgovornih osoba ili članova upravljačkog tijela. Razmjena informacija postoji no nije dokumentirana.
5	Mehanizmi su uspostavljeni, postoji dokumentacija, sudjelovanje je redovito i uključuje većinu odgovornih osoba ili članova upravljačkog tijela te postoji protok informacija koji je dokumentiran.

Reference:

- **ISO/IEC 27001:2022** (5.3, A.5.3, A.5.4)
- **ISO 22301:2019** (6.1)
- **NIST SP 800-53 Rev. 5** (PM-3, PM-12, RA-3)

UPR-002: Politika kontinuiteta poslovanja i planiranje oporavka od kibernetičkih incidenata

Ova kontrola omogućava organizaciji da sustavno pristupi očuvanju poslovanja u slučaju kibernetičkih incidenata ili drugih kriznih situacija koje mogu narušiti redovite poslovne aktivnosti. Razvijanjem i održavanjem politike kontinuiteta poslovanja i upravljanja kibernetičkim krizama, subjekt osigurava strateški okvir za pravovremeno djelovanje u uvjetima izvanrednog stanja. Izradom planova za rad u suženom opsegu tijekom razdoblja oporavka, kao i definiranjem vremenskog okvira i opsega oporavka, organizacija povećava svoju otpornost, smanjuje vrijeme zastoja i sprječava dugotrajne prekide koji mogu utjecati na sigurnost podataka, dostupnost usluga i povjerenje korisnika.

Provjerava se postoji li formalna i ažurirana politika kontinuiteta poslovanja te posebna komponenta koja se odnosi na kibernetičke krize. Analizira se dokumentacija kako bi se utvrdilo jesu li izrađeni konkretni planovi za rad u ograničenom opsegu tijekom faze oporavka, uključujući opis prioriteta, kritičnih funkcija i resursa potrebnih za privremeni rad. Dodatno se provjerava jesu li definirani vremenski okvir i opseg oporavka, uključujući jasno određene ciljeve oporavka (npr. *RTO – Recovery Time Objective*, *RPO – Recovery Point Objective*) za različite poslovne funkcije i sustave. Naglasak je na dokumentiranosti i usklađenosti planova s drugim sustavima upravljanja rizicima i sigurnošću informacija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji politika kontinuiteta poslovanja ni planovi za kibernetičke incidente.
2	Politika ili planovi su djelomično definirani, ali bez jasno definiranog opsega oporavka i vremenskih ciljeva, dokumentacija je nepotpuna ili zastarjela.
3	Postoji osnovna dokumentacija politike i planova s djelomično definiranim prioritetima i vremenskim okvirima, ali nisu testirani niti redovito ažurirani.
4	Politika i planovi su dokumentirani, obuhvaćaju kibernetičke krize, definiraju suženi opseg poslovanja i vremenske ciljeve, ali nisu potpuno integrirani u druge sigurnosne procese.
5	Politika i svi povezani planovi su ažurirani, temeljito dokumentirani, redovito testirani, uključuju jasno definirane RTO i RPO vrijednosti te su potpuno integrirani u sustav upravljanja kontinuitetom poslovanja i odgovorom na incidente.

Reference:

- **ISO/IEC 27001:2022** (A.5.30)
- **ISO/IEC 27002:2022** (5.30)
- **ISO/IEC 22301:2019** (8.2, 8.4, 9.1)

UPR-003: Mehanizam za prijavu sumnjivih događaja i incidenata

Ova kontrola osigurava uspostavu i održavanje jednostavnog mehanizma koji omogućuje zaposlenicima i izravnim dobavljačima prijavu sumnjivih događaja i incidenata. Mehanizam mora biti lako dostupan, siguran i omogućavati pravovremenu prijavu kako bi se incidenti mogli što prije identificirati i riješiti.

Provjera uključuje pregled dokumentacije o postupcima prijave incidenata, analizu implementiranih mehanizama za prijavu, provjeru zapisa o prijavljenim incidentima te konzultacije s osobljem i dobavljačima kako bi se utvrdila informiranost te osigurala funkcionalnost i učinkovitost mehanizma.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji formalizirani mehanizam za prijavu sumnjivih događaja ni incidenata. Zaposlenici i dobavljači ne znaju kome se obratiti ili kako prijaviti sumnjivu aktivnost.
2	Postoji osnovni mehanizam za prijavu incidenata, ali nije dovoljno promoviran, nije siguran, ili nije jasno definiran za sve zaposlenike i dobavljače. Nema formalnog postupka ni dokumentiranog toka prijave.
3	Subjekt ima dokumentiran i funkcionalan mehanizam za prijavu incidenata, koji je dostupan svim zaposlenicima i izravnim dobavljačima. Zaposlenici su informirani o načinu prijave putem interne komunikacije ili materijala za uvođenje u posao.
4	Mehanizam za prijavu je jasno komuniciran, lako dostupan putem više kanala i osigurava siguran prijenos informacija. Postoje standardni obrasci, dokumentacija o postupanju po prijavama te jasno definirane odgovornosti unutar sigurnosnog tima.
5	Subjekt ima centraliziran sustav za prijavu sumnjivih događaja i incidenata, dostupan zaposlenicima, dobavljačima i partnerima. Mehanizam podržava integraciju s mobilnim aplikacijama, zapisima revizijskog praćenja i automatskom kategorizacijom prema prioritetima. Svi prijavljeni slučajevi se strukturirano bilježe.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.26)
- **ISO 22301:2019** (8.4)
- **NIST SP 800-53 Rev. 5** (IR-6)
- **NIST CSF v2.0** (DE.AE-2, RS.MA-2)
- **CIS v8** (17.2, 17.3)

UPR-004: Procjena utjecaja incidenata na kontinuitet poslovanja

Ova kontrola osigurava da subjekt sustavno procjenjuje utjecaje incidenta s potencijalno velikim negativnim učinkom na kontinuitet poslovanja (BIA – *Business Impact Analysis*) makar njihova je percipirana vjerojatnost statistički mala (npr. poplava, potres, veliki kibernetički napada, geopolitičke krize i slično). Procjena uključuje analizu posljedica incidenta na ključne poslovne funkcije, vremenske okvire oporavka te potrebne mjere za minimiziranje prekida poslovanja. Cilj je osigurati pravovremeno donošenje odluka o oporavku i usklađenost mjera odgovora na incidente s poslovnim potrebama.

U postupku se provjera dokumentacija i metodologija procjene utjecaja incidenata na poslovanje, analiziraju primjere stvarnih incidenata i njihovih procjena te ispituju jesu li preporuke i prilagodbe poduzete na temelju provedenih procjena.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema definirane procjene utjecaja incidenata na kontinuitet poslovanja.
2	Provedena je procjena utjecaja incidenata na kontinuitet poslovanja, ali formalni i ponovljiv postupak nije propisan.
3	Metoda procjene utjecaja na poslovanje je definirana i dokumentirana, ali nije redovita (barem godišnja) te ne uključuje sve kritične aspekte poslovanja.
4	Procjena utjecaja na poslovanje se provodi sustavno, dokumentirana je i koristi se za donošenje odluka o projektiranju procesa oporavka.
5	Procjena utjecaja je potpuno integrirana u procese upravljanja incidentima i kontinuitetom poslovanja.

Reference:

- **ISO/IEC 27001:2022** (A.5.25, A.5.30)
- **ISO 22301:2019** (8.2, 8.3, 8.4)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-10, IR-4, RA-3)

UPR-005: Usklađivanje postupanja s incidentima i upravljanja kontinuitetom poslovanja

Ova kontrola osigurava da su postupci odgovora na incidente usklađeni s planovima kontinuiteta poslovanja. Subjekt mora definirati jasne korake za koordinaciju i komunikaciju između timova za upravljanje incidentima i timova za kontinuitet poslovanja kako bi se osigurala pravovremena reakcija i učinkovit oporavak kritičnih sustava. Također, potrebno je provoditi redovite praktične vježbe, testove i simulacije kako bi se osigurala funkcionalnost planova u stvarnim uvjetima.

U postupku se pregledavaju dokumentirane procedure za usklađivanje upravljanja incidentima i kontinuiteta poslovanja, analiziraju postojeće planove i njihove međusobne poveznice te provjeravaju usklađenost kroz provjeru evidencija provedenih testiranja, simulacija i praktičnih vježbi.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Postupanje s incidentima i kontinuitet poslovanja nisu usklađeni niti dokumentirani.
2	Procedure za usklađivanje postoje, ali nisu formalizirane niti redovito testirane.
3	Postupci su definirani i dokumentirani, ali postoje nedostaci u njihovoj koordinaciji ili primjeni uz povremene prilagodbe radi poboljšanja učinkovitosti.
4	Usklađenost postupaka je redovito testirana i dokumentirana kroz simulacije, uz povremene prilagodbe radi poboljšanja učinkovitosti.
5	Postupci su potpuno integrirani, redovito testirani i usklađeni s planovima kontinuiteta, uz jasnu koordinaciju timova.

Reference:

- **ISO/IEC 27001:2022** (A.5.26, A.5.29, A.5.30)
- **ISO 22301:2019** (8.2, 8.3, 8.4)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-4, CP-10, IR-4)
- **NIST CSF v2.0** (ID.BE-5, RS.RP-1, RS.CO-3)

UPR-006: Upravljanje dokumentacijom vezanom za postupanje s incidentima

Ova kontrola osigurava uspostavu i održavanje sveobuhvatne dokumentacije koja se koristi tijekom postupanja s incidentima. Dokumentacija treba uključivati priručnike za odgovor na incidente, grafove eskalacije, kontaktne liste, obrasce za prijavu i izvještaje o incidentima. Kontrola obuhvaća postupke za izradu, pohranu, ažuriranje i zaštitu ove dokumentacije kako bi bila lako dostupna u slučaju incidenta. Poseban naglasak stavlja se na redovito ažuriranje dokumentacije kako bi odražavala promjene u procesima i organizacijskoj strukturi.

Provjera usklađenosti uključuje pregled dokumentacije za postupanje s incidentima, analizu postupaka za izradu i ažuriranje te provjeru zapisa o korištenju dokumentacije tijekom stvarnih incidenata ili provođenja vježbi. Također se provode konzultacije s odgovornim osobljem kako bi se osigurala dostupnost, točnost i dosljedna primjena dokumentacije u postupcima odgovora na incidente.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt nema uspostavljenu dokumentaciju za upravljanje incidentima.
2	Postoji osnovna dokumentacija koja uključuje neke elemente, poput kontakt liste ili jednostavnog obrasca za prijavu incidenta. U praksi se dokumenti rijetko koriste, a zaposlenici nisu sigurni gdje se nalaze niti kada su zadnji put ažurirani.
3	Subjekt ima dokumentaciju za upravljanje incidentima koja uključuje sve ključne elemente. Dokumenti su dostupni tijekom incidenata, ali postoji rizik da neke informacije (npr. kontakti) nisu aktualne. Dokumentacija se koristi u vježbama i stvarnim situacijama, ali ne postoji formalna evidencija korištenja.
4	Subjekt ima sveobuhvatan i aktualan skup dokumenata za odgovor na incidente. Dokumentacija obuhvaća operativne upute, detaljne eskalacijske tokove, kontaktne točke i obrasce za obradu i izvještavanje o incidentima. Dokumenti su sigurno pohranjeni, dostupni tijekom incidenata i integrirani u vježbe. Evidencije o pristupu i korištenju dokumentacije se vode, a odgovorni tim ima jasne zadatke za održavanje točnosti.
5	Subjekt ima centraliziran, digitalno dostupan i integriran sustav za upravljanje dokumentacijom za incidente. Ažuriranja se provode prema definiranim vremenskim okvirima i automatizirano reflektiraju promjene u organizaciji. Redovite vježbe uključuju validaciju dokumentacije, a svaki stvarni incident rezultira pregledom i ažuriranjem relevantnih zapisa. Dokumentacija se koristi ne samo operativno, već i kao alat za unapređenje sigurnosne kulture i sposobnosti organizacije.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.26)
- **ISO 22301:2019** (8.2, 8.3, 8.4, 8.5, 8.6)
- **NIST SP 800-53 Rev. 5** (IR-4, IR-6, IR-8)
- **NIST CSF v2.0** (RC.RP-06)
- **CIS v8** (17.8)

UPR-007: Dodjela uloga za otkrivanje i odgovor na incidente

Ova kontrola osigurava da su definirane i dodijeljene specifične uloge za otkrivanje, analizu i odgovor na incidente kompetentnim zaposlenicima. Uloge trebaju biti jasno opisane, uključujući odgovornosti i ovlasti, te dodijeljene osobama s odgovarajućim znanjem i vještinama. Kontrola također obuhvaća redovitu obuku zaposlenika kako bi bili spremni učinkovito reagirati na incidente.

Provjera usklađenosti uključuje pregled dokumentacije o dodijeljenim ulogama i odgovornostima te analizu kvalifikacija i obuke zaposlenika zaduženih za odgovor na incidente. Također se provjeravaju zapisi o incidentima kako bi se osigurala dosljedna primjena dodijeljenih uloga i provode se konzultacije s odgovornim osobljem kako bi se osigurala jasna podjela odgovornosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Uloge za otkrivanje i odgovor na incidente nisu definirane ni dodijeljene.
2	Neke uloge i odgovornosti za upravljanje incidentima su definirane, ali nisu dovoljno precizne ni sveobuhvatne. Dodjela uloga nije dokumentirana za sve ključne funkcije (otkrivanje, analiza, odgovor). Evidencija o incidentima pokazuje nedosljednu primjenu uloga.
3	Postoji dokumentacija kojom su definirane osnovne uloge za sve ključne faze odgovora na incidente (poput PICERL modela). Osnovna obuka je provedena, ali ne redovito. Dodjela uloga se provodi u praksi, no ne uvijek na strukturiran način. Iz zapisa o incidentima vidljivo je da postoje određena odstupanja u primjeni odgovornosti.
4	Specifične uloge za sve faze odgovora na incidente su jasno definirane, dokumentirane i dodijeljene kvalificiranim osobama. Postoji formalna evidencija o znanjima, certifikatima i radnom iskustvu osoba zaduženih za odgovor na incidente.
5	Subjekt ima potpuno razvijen sustav raspodjele uloga za otkrivanje, analizu i odgovor na incidente (utemeljen na modelima poput PICERL). Svaka uloga ima jasno definirane zadatke, ovlasti, tehničke i organizacijske zahtjeve. Uloge su dodijeljene certificiranim i redovito educiranim zaposlenicima koji sudjeluju u praktičnim vježbama.

Reference:

- **ISO/IEC 27001:2022** (A.5.26, A.5.3, A.6.3)
- **ISO 22301:2019** (8.2, 8.3, 8.4)
- **NIST SP 800-53 Rev. 5** (AT-3, IR-1, IR-4)
- **CIS v8** (17.1, 17.4)

UPR-008: Planovi komunikacije i razvrstavanje incidenata

Ova kontrola osigurava uspostavu planova za komunikaciju tijekom incidenata, uzimajući u obzir kategoriju incidenata prema nacionalnoj taksonomiji. Planovi trebaju definirati postupke za internu eskalaciju, obavještavanje nadležnih tijela i relevantnih sudionika uz korištenje sigurnih komunikacijskih sustava. Kontrola obuhvaća i pravila za korištenje najboljih sigurnosnih praksi u komunikaciji tijekom hitnih situacija.

Provjera usklađenosti uključuje pregled planova komunikacije i procedura za razvrstavanje incidenata, analizu sigurnosnih mjera primijenjenih u komunikacijskim kanalima te testiranje procedura za internu eskalaciju i prijavu incidenata nadležnim tijelima. Također se provode konzultacije s osobljem odgovornim za komunikaciju tijekom incidenata kako bi se osigurala dosljedna primjena planova i sigurnost komunikacija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Planovi komunikacije i razvrstavanje incidenata nisu definirani.
2	Osnovni planovi postoje, ali nisu sveobuhvatni i ne uzimaju u obzir kategorizaciju incidenata.
3	Planovi su definirani i primjenjuju se, ali nisu redovito testirani.
4	Sveobuhvatni planovi su dokumentirani, testirani i uzimaju u obzir nacionalnu taksonomiju.
5	Planovi su potpuno integrirani, ažurirani, redovito testirani kroz simulacije.

Reference:

- **ISO/IEC 27001:2022** (A.5.26, A.5.29)
- **ISO 22301:2019** (8.2, 8.3, 8.4, 8.5, 8.6)
- **NIST SP 800-53 Rev. 5** (IR-4, IR-6, IR-7, IR-8)
- **NIST CSF v2.0** (RS.CO-1, RS.CO-2)
- **CIS v8** (17.2, 17.3, 17.6)

UPR-009: Sustav za vođenje evidencije incidenata

Ova kontrola osigurava uspostavu sustava za vođenje detaljne evidencije svih incidenata. Sustav mora bilježiti informacije o incidentu, tijeku odgovora, eskalaciji i konačnom rješenju. Kontrola uključuje provjeru pravila za vođenje, održavanje, zaštitu i arhiviranje evidencije. Podaci iz evidencije moraju omogućiti provedbu forenzičkih analiza.

Provjera usklađenosti uključuje pregled sustava za vođenje evidencije i zapisa o incidentima, analizu mjera i postupaka za zaštitu i arhiviranje evidencije te provjeru mogućnosti provedbe forenzičkih analiza na temelju evidencije. Također se provode konzultacije s osobljem odgovornim za vođenje evidencije incidenata kako bi se osigurala dosljedna primjena pravila za evidentiranje i arhiviranje incidenata.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za vođenje evidencije incidenata ne postoji ili nije funkcionalan.
2	Postoji osnovna evidencija incidenata, ali je vođena ručno ili u neadekvatnim formatima. Podaci nisu standardizirani, a informacije o tijeku incidenta i eskalaciji su nepotpune. Pravila za zaštitu i arhiviranje podataka nisu formalno definirana.
3	Subjekt koristi strukturirani sustav za vođenje evidencije incidenata, u kojem se bilježe ključne informacije.
4	Postoji centraliziran i standardiziran sustav za vođenje evidencije incidenata, s jasno definiranim poljima, automatiziranim unosima iz povezanih sustava i praćenjem cijelog životnog ciklusa incidenta. Evidencije uključuju sve faze životnog ciklusa incidenta.
5	Subjekt ima automatiziran, skalabilan i sigurnosno zaštićen sustav za vođenje incidentne evidencije, u potpunosti integriran s ostalim sigurnosnim alatima. Svaki incident je dokumentiran s punim audit tragom, vremenskom crtom, vezanim događajima, uključenim sustavima i osobljem.

Reference:

- **ISO/IEC 27001:2022** (A.5.24)
- **ISO 22301:2019** (7.5, 8.3, 8.4, 8.6)
- **NIST SP 800-53 Rev. 5** (IR-4, IR-5, AU-6, AU-7, AU-11)
- **NIST CSF v2.0** (Kategorija DE.AE)
- **CIS v8** (17.4)

UPR-010: Obavještavanje nadležnih tijela o incidentima

Ova kontrola osigurava da subjekt pravovremeno obavještava nadležna tijela, poput nacionalnog CSIRT-a, o incidentima koji mogu ugroziti mrežne i informacijske sustave. Kontrola uključuje provjeru procedura za identifikaciju incidenata, klasifikaciju prema nacionalnoj taksonomiji, provjera pridržavanja rokova za obavještavanje i uspostavu komunikacijskih kanala za prijavu incidenata. Također obuhvaća vođenje evidencije o prijavljenim incidentima i dokumentaciju o poduzetim radnjama.

Provjera uključuje pregled procedura za obavještavanje nadležnih tijela, analizu evidencija o prijavljenim incidentima, provjeru usklađenosti s nacionalnim propisima i rokovima za prijavu incidenata te konzultacije s odgovornim osobljem za upravljanje incidentima. Također se provjerava implementacija klasifikacije incidenata prema nacionalnoj taksonomiji i uspostavljeni planovi komunikacije za hitne slučajeve.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Postupci za obavještavanje nadležnih tijela o incidentima nisu definirani ni dokumentirani.
2	Osnovni postupci za obavještavanje postoje, ali nisu usklađeni s nacionalnim propisima ili taksonomijom.
3	Postupci su definirani i dokumentirani, ali primjena nije dosljedna niti se provode redovite provjere.
4	Sveobuhvatni postupci su definirani, dokumentirani i provode se dosljedno u skladu s propisima.
5	Postupci obavještavanja su automatizirani, redovito se ažuriraju i provode u skladu s najboljim praksama.

Reference:

- **ISO/IEC 27001:2022** (A.5.26, A.5.31)
- **ISO 22301:2019** (7.5, 8.4)
- **NIST SP 800-53 Rev. 5** (IR-6, IR-7)
- **NIST CSF v2.0** (RS.CO-2, RS.CO-3)
- **CIS v8** (17.6)

UPR-011: Pravila trijaže i procjene sumnjivih događaja

Ova kontrola osigurava definiranje i primjenu pravila za trijažu sumnjivih događaja kako bi se odredili prioriteti obrade i analize. Pravila uključuju kriterije za prepoznavanje lažno pozitivnih događaja, procjenu utjecaja na poslovanje i prilagodbu prioriteta obrade kako bi se osigurala učinkovita reakcija na stvarne prijetnje.

Provjera uključuje pregled dokumentacije o pravilima trijaže, analizu zapisa o provedenim trijažama i prioritetima, testiranje učinkovitosti procesa trijaže te konzultacije s osobljem za sigurnost kako bi se osigurala dosljedna primjena pravila.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Pravila trijaže nisu definirana ni dokumentirana.
2	Osnovna pravila trijaže su definirana, ali nisu sveobuhvatna niti se dosljedno primjenjuju. Postoji ograničena dokumentacija.
3	Subjekt ima dokumentirana pravila za trijažu koja uključuju osnovne kriterije za klasifikaciju događaja, prepoznavanje lažno pozitivnih signala i inicijalnu procjenu potencijalnog utjecaja. Trijaža se provodi prema prioritetima temeljenima na vrsti događaja, izvoru i kontekstu.
4	Trijaža je u potpunosti integrirana u proces detekcije i analize sigurnosnih događaja. Pravila su jasno definirana, dokumentirana i usklađena s klasifikacijom imovine, procjenom rizika i poslovnim prioritetima.
5	Subjekt ima automatiziran sustav trijaže, integriran sa SIEM, SOAR ili EDR alatima. Trijažni mehanizmi se redovito testiraju i prilagođavaju na temelju mjerenja učinkovitosti, povratnih informacija sigurnosnog tima i promjena u prijetnjama.

Reference:

- **ISO/IEC 27001:2022** (A.5.24, A.5.25)
- **ISO 22301:2019** (8.6, 9.1)
- **NIST SP 800-53 Rev. 5** (IR-4, IR-5, RA-3)
- **NIST CSF v2.0** (Kategorija RS.AN)
- **CIS v8** (17.4, 17.9)

UPR-012: Provedba simulacijskih vježbi odgovora na incidente

Ova kontrola osigurava redovito provođenje simulacijskih vježbi za odgovor na incidente kako bi se testirala učinkovitost postojećih procedura i planova za postupanje s incidentima. Vježbe uključuju *red teaming*, *table-top* simulacije, *purple teaming* i druge oblike simulacija napada kako bi se identificirale potencijalne slabosti i osigurala spremnost subjekta. Dokumentacija provedbe vježbi mora biti sveobuhvatna i uključivati detaljan opis scenarija, rezultata i preporuka za poboljšanja.

Provjera uključuje analizu dokumentacije o provedenim vježbama, pregled scenarija korištenih tijekom simulacija, evaluaciju rezultata i preporuka iz vježbi te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala primjena naučenih lekcija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Simulacijske vježbe odgovora na incidente nisu planirane ni provedene.
2	Simulacijske vježbe se provode *ad hoc i* bez jasne dokumentacije.
3	Vježbe se provode godišnje, ali ne obuhvaćaju sve ključne scenarije i nisu sveobuhvatno dokumentirane.
4	Redovite simulacijske vježbe provode se godišnje s jasnim scenarijima i sveobuhvatnom dokumentacijom. Rezultati se analiziraju i koriste za poboljšanje procedura.
5	Napredne simulacijske vježbe provode se redovito s različitim scenarijima (*red teaming*, *purple teaming*).

Reference:

- **ISO/IEC 27001:2022** (A.5.27, A.6.3)
- **ISO 22301:2019** (8.5)
- **NIST SP 800-53 Rev. 5** (CP-4, IR-3, IR-8)

UPR-013: Kontinuitet poslovanja i upravljanja krizama

Ova kontrola osigurava razvoj, dokumentiranje, održavanje i implementaciju politika za kontinuitet poslovanja i upravljanje kibernetičkim krizama. Politike moraju definirati kriterije i metode za identificiranje ključnih poslovnih aktivnosti subjekta koji će biti opseg analize i planiranja, kao i organizacijske i tehničke preduvjete za njihovu provedbu. Sam opseg može biti definiran u proizvoljnom dokumentu. Poseban naglasak stavlja se na obaveznost pojedinih koraka radi postizanje otpornosti i odgovora organizacije na krizne situacije.

Provjera uključuje pregled dokumentacije politika kontinuiteta poslovanja i upravljanja krizama, te konzultacije s odgovornim osobljem za krizno upravljanje kako bi se osigurala usklađenost s poslovnim potrebama i sigurnosnim standardima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Politike kontinuiteta poslovanja i upravljanja krizama nisu razvijene niti dokumentirane.
2	Osnovne politike postoje, ali nisu sveobuhvatne niti redovito ažurirane.
3	Politike su dokumentirane i djelomično implementirane, ali nisu testirane niti revidirane.
4	Sveobuhvatne politike su razvijene, dokumentirane, redovito testirane i revidirane.
5	Politike su potpuno integrirane i usklađene s rezultatima procjene rizika.

Reference:

- **ISO/IEC 27001:2022** (A.5.29, A.5.30)
- **ISO 22301:2019**
- **NIST SP 800-53 Rev. 5** (CP-2, CP-4, CP-10, IR-4, PM-8)

UPR-014: Upravljanje informacijama dobivenim od nadležnih tijela

Ova kontrola osigurava definiranje, implementaciju i dokumentiranje procesa za primanje, analizu i korištenje informacija dobivenih od nadležnog CSIRT-a ili drugih nadležnih tijela. Proces uključuje obradu informacija o incidentima, ranjivostima, kibernetičkim prijetnjama i preporučenim mjerama, kako bi se osigurala pravovremena reakcija i sprječavanje dodatnih rizika.

Provjera uključuje pregled dokumentacije procesa upravljanja informacijama, analizu primljenih podataka od nadležnih tijela, procjenu primjene preporučenih mjera te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala učinkovita implementacija.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Procesi za upravljanje informacijama nisu definirani ni implementirani.
2	Osnovni procesi su definirani, ali nisu dosljedno primijenjeni ni dokumentirani.
3	Procesi su djelomično implementirani i dokumentirani, ali nedostaje redovita analiza i evaluacija.
4	Procesi su potpuno implementirani, dokumentirani i redovito evaluirani.
5	Procesi su potpuno integrirani, automatizirani i kontinuirano unapređivani prema dobivenim informacijama.

Reference:

- **ISO/IEC 27001:2022** (A.5.26, A.5.31)
- **ISO 22301:2019** (8.4)
- **NIST SP 800-53 Rev. 5** (CA-2, RA-7)
- **NIST CSF v2.0** (DE.AE-3, RS.CO-3)

UPR-015: Osiguravanje dodatnih kapaciteta tijekom kriznih situacija

Ova kontrola osigurava uspostavu i implementaciju tehničkih i organizacijskih mjera za povećanje kapaciteta tijekom kriznih situacija. To uključuje osiguranje dodatnih resursa, podrške te redundancije kako bi se očuvala razina kibernetičke sigurnosti i osigurala otpornost subjekta na prijetnje.

Provjera uključuje pregled planova za osiguranje dodatnih kapaciteta, analizu korištenih tehničkih i organizacijskih mjera tijekom kriznih situacija, provjeru redundancije te konzultacije s odgovornim osobljem za sigurnost.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Dodatni kapaciteti nisu osigurani ni planirani.
2	Dodatni kapaciteti su planirani, ali nisu dokumentirani.
3	Dodatni kapaciteti su djelomično osigurani, ali nisu sveobuhvatni.
4	Dodatni kapaciteti su osigurani, dokumentirani i testirani kroz vježbe.
5	Dodatni kapaciteti su potpuno integrirani u procese upravljanja krizama i kontinuirano unapređivani.

Reference:

- **ISO/IEC 27001:2022** (A.5.29, A.5.30)
- **ISO 22301:2019** (7.1, 8.4)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-6, CP-7, CP-10, SC-36)

UPR-016: Razvoj i održavanje hodograma aktivnosti oporavka

Ova kontrola osigurava razvoj, dokumentiranje i održavanje hodograma aktivnosti oporavka u okviru DRP-a (*Disaster Recovery Plan*). Hodogram mora obuhvatiti vremenske okvire, ključne međuovisnosti aktivnosti, raspodjelu odgovornosti i potrebne resurse. Također mora osigurati da se aktivnosti oporavka odvijaju pravodobno i u skladu s definiranim RTO-ima (*Recovery Time Objectives*), RPO-ima (*Recovery Point Objectives*) i SDO-ima (*Service Delivery Objectives*).

Provjera uključuje pregled dokumentiranog hodograma aktivnosti oporavka, analizu postupaka za redovito ažuriranje i testiranje hodograma te konzultacije s odgovornim osobljem kako bi se osiguralo da je hodogram usklađen s politikama kontinuiteta poslovanja i oporavka od katastrofa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Hodogram aktivnosti oporavka nije razvijen.
2	Osnovni hodogram postoji, ali nije sveobuhvatan niti redovito ažuriran.
3	Hodogram je razvijen i djelomično ažuriran, ali nije testiran.
4	Hodogram je sveobuhvatan, redovito ažuriran i testiran.
5	Hodogram je potpuno integriran i kontinuirano optimiziran.

Reference:

- **ISO/IEC 27001:2022** (A.5.29, A.5.30)
- **ISO 22301:2019** (8.4, 8.6)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-4, CP-10, IR-4)

UPR-017: Upravljanje ključnim komunalnim uslugama

Ova kontrola osigurava identifikaciju, upravljanje i praćenje ključnih komunalnih usluga koje su nužne za normalan rad mrežnih i informacijskih sustava subjekta. Kontrola uključuje procjenu ovisnosti o komunalnim uslugama, razvoj rezervnih opcija i planova za nastavak poslovanja u slučaju prekida pružanja komunalnih usluga.

Provjera uključuje pregled dokumentacije o ovisnostima o ključnim komunalnim uslugama, analizu rezervnih opcija i postupaka za ublažavanje rizika te konzultacije s odgovornim osobljem za kontinuitet poslovanja kako bi se osigurala učinkovitost mjera upravljanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ovisnosti o ključnim komunalnim uslugama nisu identificirane niti dokumentirane.
2	Osnovna analiza ovisnosti postoji, ali nedostaju rezervne opcije.
3	Ovisnosti su dokumentirane, ali postupci za ublažavanje rizika nisu sveobuhvatni.
4	Ovisnosti su dokumentirane, rezervne opcije osigurane i testirane.
5	Upravljanje ovisnostima je potpuno integrirano i redovito optimizirano.

Reference:

- **ISO 22301:2019** (8.3.4)
- **NIST SP 800-53 Rev. 5** (PE-11)

UPR-018: Utvrđivanje ključnih poslovnih aktivnosti

Ova kontrola osigurava da subjekt prepozna koje su poslovne aktivnosti ključne za održavanje minimalnog funkcionalnog poslovanja i da za njih osigura tehničke i organizacijske preduvjete za nastavak rada u slučaju incidenta. Identifikacijom tih aktivnosti i njihovih ovisnosti, organizacija može planirati i implementirati mjere koje omogućuju kontinuitet najvažnijih funkcija, čak i u uvjetima otežanog rada ili prekida dijela sustava. Time se smanjuje izloženost organizacije dugotrajnim zastojima, gubicima prihoda i narušavanju ugleda, te se doprinosi bržem i učinkovitijem oporavku.

Provjerava se je li subjekt proveo formalnu identifikaciju ključnih poslovnih aktivnosti, uključujući dokumentirani popis procesa, usluga ili funkcija koje su nužne za poslovni kontinuitet. Također se analizira dokumentacija u kojoj su definirani tehnički (npr. dostupnost sustava, komunikacija, infrastruktura) i organizacijski (npr. odgovorne osobe, zamjene, vanjski dobavljači) preduvjeti koji omogućuju nastavak tih aktivnosti u slučaju kibernetičkog incidenta. Poseban naglasak stavlja se na konzistentnost u popisu ključnih poslovnih aktivnosti, kao i na dokumentaciju koja pokazuje kako su ti preduvjeti osigurani ili planirani.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ključne poslovne aktivnosti nisu identificirane; ne postoje tehnički ni organizacijski preduvjeti za njihov nastavak.
2	Aktivnosti su djelomično prepoznate, ali ne postoji dokumentacija o preduvjetima ili su oni nejasno definirani.
3	Postoji dokumentiran popis ključnih aktivnosti, ali preduvjeti su opisani općenito ili nisu usklađeni s planovima kontinuiteta.
4	Ključne aktivnosti i njihovi tehnički i organizacijski preduvjeti su dokumentirani, ali nisu ažurirani.
5	Postoji ažurirana i sveobuhvatna dokumentacija o ključnim poslovnim aktivnostima i svim potrebnim preduvjetima za njihov nastavak, uz osiguranu povezanost s planovima kontinuiteta i redovitim provjerama njihove provedivosti.

Reference:

- **ISO/IEC 22301:2019** (8.2, 8.4, 9.1)
- **NIST SP 800-53 Rev. 5** (CP-2, CP-10, CP-11, PE-17)

NAD-001: Definiranje ključnih sigurnosnih metrika za praćenje kibernetičke sigurnosti uključivo prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika

Ova kontrola osigurava da subjekt definira ključne sigurnosne metrike potrebne za praćenje i procjenu stanja kibernetičke sigurnosti. Ove metrike uključuju pokazatelje poput broja i vrste incidenata, vremena reakcije te postotka usklađenosti s propisanim mjerama. Precizno definirane metrike omogućuju bolji uvid u sigurnosnu situaciju i donošenje informiranih odluka o sigurnosnim poboljšanjima. Prikupljanje informacija poput vremena reakcije i broja incidenata daje subjektu stvarni uvid u sigurnosne performanse.

U postupku se provjerava postoji li dokumentacija o definiranim metrikama, kao i njihova usklađenost s potrebama subjekta. U svrhu ocjenjivanja omogućuju li metrike kontinuirano praćenje stanja kibernetičke sigurnosti, analizira se pokrivaju li svi ključni pokazatelji relevantne prijetnje i potrebe te se provjeravaju sustavi i procesi uspostavljeni za prikupljanje i praćenje podataka temeljem definiranih sigurnosnih metrika uz ocjenjivanje učestalosti i točnosti podataka. Ocjenjuje se kvaliteta i dosljednost analiza sigurnosnih metrika te se ispituju procesi izvještavanja prema relevantnim osobama kroz intervjue.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ključne sigurnosne metrike nisu definirane.
2	Ključne sigurnosne metrike su definirane, ali nisu formalno dokumentirane niti uključuju ključne pokazatelje poput incidenata i vremena reakcije.
3	Ključne sigurnosne metrike su definirane, uključuje sve ključne pokazatelje i formalno su dokumentirane.
4	Ključne sigurnosne metrike su definirane i dokumentirane, uključuju ključne pokazatelje, ali se ne provodi prikupljanje i praćenje podataka temeljem definiranih metrika niti sustavno izvještavanje prema osobama odgovornim za provedbu mjera.
5	Metrike su potpuno definirane i pokrivaju sve ključne pokazatelje u skladu s potrebama subjekta i redovito su ažurirane temeljem provedenog prikupljanja i praćenja podataka uz izvještavanje osoba odgovornih za provedbu mjera.

Reference:

- **ISO/IEC 27001:2022** (9.1, 9.2)

- **ISO 22301:2019** (9.1, 9.2)
- **NIST SP 800-53 Rev. 5** (CA-7, PM-14, SI-4)

NAD-002: Implementacija sustava za nadzor aktivnosti na informacijskim sustavima u stvarnom vremenu

Kontrola osigurava implementaciju naprednih sustava za kontinuirani nadzor stanja kibernetičke sigurnosti. Ti sustavi omogućavaju prikupljanje, konsolidiranje te praćenje ključnih podataka/indikatora, kao što su abnormalne mrežne aktivnosti, neovlašteni pristupi i potencijalno neovlaštene promjene u sustavima, što omogućuje pravovremeno prepoznavanje potencijalnih prijetnji. Uspostavljanjem ovakvih sustava, subjekt može bolje reagirati na incidente i osigurati kontinuiranu zaštitu svojih resursa.

U postupku se provjeravaju sustavi za nadzor s pripadajućom dokumentacijom i analizira razina pokrivenosti sigurnosnih indikatora, kao i učestalost praćenja i ažuriranja sustava. Također procjenjuju se usklađenost nadzora s organizacijskim potrebama i zahtjevima za zaštitu ključnih resursa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustavi za nadzor nisu uspostavljeni.
2	Postoji osnovni sustav nadzora, ali nije prilagođen kontinuiranom praćenju u stvarnom vremenu.
3	Sustav ili sustavi za nadzor su implementirani, ali sigurnosna telemetrija ne pokriva sve ključne informacijske sustave.
4	Sustav ili sustavi za nadzor su funkcionalni, pokrivaju ključne informacijske sustave i postoji uspostavljeni proces praćenja ključnih indikatora.
5	Sustav ili sustavi za nadzor su funkcionalni, pokrivaju sve ključne informacijske sustave te postoji automatizacija koja osigurava bržu i učinkovitiju reakciju na unaprijed definirane sigurnosne događaje.

Reference:

- **ISO/IEC 27001:2022** (A.8.9, A.8.16)
- **ISO/IEC 27002:2022** (8.15, 8.16)
- **NIST SP 800-53 Rev. 5** (SI-4, AU-6, CA-7)
- **NIST CSF v2.0** (Kategorija DE.CM)
- **CIS v8** (Kontrola 8)

NAD-003: Postavljanje automatskih alarma za detekciju prijetnji

Ova kontrola uključuje uspostavljanje automatskih alarma za pravovremenu detekciju i reakciju na potencijalne sigurnosne prijetnje. Automatski alarmi, koji se aktiviraju u slučaju otkrivanja neobičnih aktivnosti ili odstupanja u sigurnosnim pokazateljima, omogućuju brzo reagiranje na moguće incidente. Time se značajno smanjuje vrijeme potrebno za identifikaciju prijetnji i poduzimanje mjera zaštite.

U postupku provjere analizira se konfiguracija automatskih alarma i provjerava se jesu li oni usklađeni s glavnim sigurnosnim prijetnjama za subjekt. Dodatno se ispituje kako su alarmi prilagođeni u kontekstu specifičnih pokazatelja rizika te postoji li dokumentacija o njihovim učincima u prošlim slučajevima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt nema uspostavljene automatske alarme za detekciju sigurnosnih prijetnji.
2	Automatski alarmi su uspostavljeni u pojedinim sustavima, ali nisu centralizirani niti sveobuhvatni. Aktiviraju se samo za osnovne tipove prijetnji (npr. *brute force* napad), dok veći dio aktivnosti ostaje nepokriven. Konfiguracija alarma nije usklađena s procjenom rizika ni s imovinom visoke kritičnosti. Postoji djelomična dokumentacija.
3	Subjekt koristi automatske alarme u sklopu SIEM, EDR ili sličnih sigurnosnih sustava, koji su konfigurirani da prepoznaju uobičajene sigurnosne prijetnje i anomalije. Alarmni pragovi su definirani prema poznatim sigurnosnim pokazateljima, a sustav je povezan s inicijalnim oblicima reakcije. Postoji dokumentacija o konfiguraciji i dnevnički zapisi (*logovi*) o aktiviranim alarmima.
4	Automatski alarmi su kontekstualno postavljeni i usklađeni s rizicima, kritičnom imovinom i poslovnim procesima. Konfiguracija uključuje dinamičko praćenje ponašanja korisnika, sustava i mrežnog prometa. Postoji redovita evaluacija učinkovitosti, evidencija o aktivacijama alarma i njihove povezanosti s detektiranim incidentima.
5	Subjekt koristi automatizirane, adaptivne i kontekstualne alarme temeljene na analizi ponašanja u stvarnom vremenu i naprednim detekcijskim mehanizmima (poput analize ponašanja, modela strojnog učenja u SOAR/SIEM alatima i ostalim). Alarmi su direktno integrirani u mehanizme automatskog odgovora (poput izolacije krajnjih točaka). Postoji formalni proces kontinuiranog unaprjeđenja sustava alarmiranja.

Reference:

- **NIST SP 800-53 Rev. 5** (PL-8)
- **NIST CSF v2.0** (Kategorija DE.CM)

NAD-004: Korištenje nadzornih ploča (*dashboarda*) za praćenje sigurnosnih indikatora

Korištenje nadzornih ploča (*dashboarda*) omogućava operativnim timovima i upravljačkom tijelu brz i jasan pregled ključnih sigurnosnih indikatora u stvarnom vremenu. Nadzorne ploče olakšavaju identifikaciju trendova i anomalija, što omogućava pravovremenu reakciju na prijetnje. Vizualizacija podataka putem nadzornih ploča također poboljšava razumijevanje trenutnog stanja sigurnosti i omogućava brže donošenje odluka.

U postupku provjere se analiziraju i ispituju implementirane nadzorne ploče, uključujući pokrivenost ključnih pokazatelja i način prezentacije podataka. Dodatno se procjenjuje funkcionalnost nadzornih ploča i prilagodba za potrebe tima, kako bi se omogućio brz pregled sigurnosnih informacija i olakšala detekcija rizika.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nadzorne ploče za praćenje sigurnosnih indikatora nisu uspostavljene.
2	Postoji osnovna nadzorna ploča, ali nije usklađena s ključnim sigurnosnim pokazateljima.
3	Nadzorne ploče su implementirane, ali ne uključuju sve ključne pokazatelje ili nisu redovito ažurirane.
4	Nadzorne ploče su funkcionalne, lako dostupne i pokrivaju glavne pokazatelje, uz manje nedostatke u ažuriranju ili prilagodbi.
5	Nadzorne ploče su potpuno funkcionalne, redovito ažurirane i omogućavaju jasan pregled svih ključnih pokazatelja.

Reference:

- **NIST SP 800-53 Rev. 5** (PL-9)
- **NIST CSF v2.0** (Kategorija RS.AN)

NAD-005: Filtriranje pristupa zlonamjernim web stranicama

Ova kontrola osigurava primjenu mehanizama koji sprječavaju ili otkrivaju pristup poznatim ili sumnjivim zlonamjernim web stranicama. Filtriranje se može provoditi putem liste zabranjenih kategorija ili domena (*blacklist*) ili liste dozvoljenih kategorija ili domena (*whitelist*), ovisno o procjeni rizika i poslovnim potrebama subjekta. Kontrola također obuhvaća ažuriranje lista i praćenje učinkovitosti filtriranja uz primjenu odgovarajućih politika filtriranja na mrežnoj opremi ili sigurnosnim alatima.

Provjera usklađenosti uključuje pregled konfiguracija filtriranja, analizu ažuriranih lista dozvoljenih/zabranjenih domena te testiranje mehanizama za blokiranje zlonamjernih web stranica. Provjera također uključuje konzultacije s odgovornim osobljem za sigurnost mreže uz analizu politika filtriranja web prometa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Mehanizmi za filtriranje nisu implementirani.
2	Osnovni mehanizmi filtriranja postoje, ali se ažuriraju reaktivno.
3	Filtriranje je implementirano ručno koristeći javno dostupne liste zabranjenih kategorija ili domena i web stranica.
4	Filtriranje je implementirano koristeći sustave koji samostalno održavaju filter liste.
5	Implementirano je napredno filtriranje s automatskom detekcijom i analizom sadržaja.

Reference:

- **ISO/IEC 27001:2022** (A.8.16, A.8.23)
- **ISO/IEC 27002:2022** (8.16, 8.23)
- **NIST SP 800-53 Rev. 5** (SC-7, SC-44, SI-3, SI-4)
- **NIST CSF v2.0** (Kategorija DE.CM)
- **CIS v8** (9.2, 9.3)

NAD-006: Ograničavanje javno izloženih servisa

Ova kontrola osigurava identifikaciju i ograničavanje servisa koji su izloženi javno putem Interneta. Servisi poput web stranica, elektroničke pošte, VPN-a, RDP-a, SSH-a i drugih trebaju biti analizirani i ograničeni prema potrebi poslovanja i procjeni rizika.

Provjera usklađenosti uključuje pregled popisa javno izloženih servisa, analizu politika ograničavanja pristupa te provjeru tehničkih konfiguracija sustava.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema identifikacije ili ograničavanja javno izloženih servisa.
2	Postoji djelomična identifikacija izloženih servisa bez aktivnog ograničavanja.
3	Identifikacija izloženih servisa provedena je, ali ograničavanje je nedosljedno.
4	Izloženost servisa je identificirana i ograničena prema poslovnim potrebama.
5	Sustavna identifikacija i ograničavanje izloženih servisa uz kontinuirani nadzor.

Reference:

- **ISO/IEC 27001:2022** (A.8.12, A.8.16)
- **ISO/IEC 27002:2022** (8.12, 8.16)
- **NIST SP 800-53 Rev. 5** (AC-3, AC-4, SC-7)
- **NIST CSF v2.0** (DE.CM-7)

NAD-007: Implementacija principa nultog povjerenja (*Zero Trust*)

Kontrola osigurava primjenu principa nultog povjerenja u mrežnom pristupu što je posebno primjereno u više otvorenim okruženjima ili onima koje koriste javni oblak, pri čemu se svi korisnici i uređaji smatraju nepouzdanim dok se ne verificiraju. Primjenjuju se mehanizmi za provjeru identiteta korisnika s više faktora i granuliranu kontrolu pristupa mrežnim resursima.

Provjera usklađenosti uključuje pregled politike nultog povjerenja, analizu implementiranih kontrola za provjeru identiteta i autorizacije te konzultacije s mrežnim administratorima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt uopće ne primjenjuje pristup nultog povjerenja čak ni na javno dostupnim sustavima.
2	Neki elementi principa nultog povjerenja (npr. višefaktorska autentifikacija, kriptiranje komunikacije ili prepoznavanje uređaja) se koriste na javno dostupnim servisima, ali nisu dio strukturiranog pristupa. Primjenjuju se samo za određene sustave ili korisnike (primjerice administratore).
3	Subjekt je uspostavio temeljne principe nultog povjerenja za javno dostupne servise (kako vlastite tako i one u oblaku). Provodi se višefaktorska autentifikacija korisničkog identiteta te prepoznavanje pristupnog uređaja. Međutim, kontrole nisu ujednačene u cijeloj organizaciji, a pristup i dalje nije kontekstualan (npr. ne prati se lokacija korisnika, status uređaja ili rizik pristupa).
4	Pristup nultog povjerenja je formalno usvojen i dokumentiran u strategiji, implementiran za sve javno izložene i kritične sustave te se dodatno primjenjuje za sve korisnike jednako. Koriste se kontrole pristupa temeljene na identitetu, stanju pristupnog uređaja i kontekstu (npr. vrijeme pristupa, geografska lokacija ili ponašanje korisnika).
5	Subjekt ima potpuno implementiran i integriran model nultog povjerenja s drugim sustavima kako bi se mogla provjeriti ažurnost i sigurnost pristupnog uređaja tijekom procesa autentifikacije. Model se bez iznimke koristi i za sve vanjske korisnike. Nema implicitnog povjerenja – svaki pristup mora biti višestruko verificiran u trenutku pristupa. Princip nultog povjerenja je dio sigurnosne arhitekture i kulture organizacije.

Reference:

- **ISO/IEC 27001:2022** (A.8.2)
- **ISO/IEC 27002:2022** (8.2)
- **NIST SP 800-53 Rev. 5** (AC-3, AC-6)
- **NIST SP 800-207** (Poglavlje *Zero Trust Architecture*)
- **CIS v8** (6.7)

NAD-008: Sigurni mrežni protokoli za prijenos podataka

Ova kontrola osigurava korištenje sigurnih mrežnih protokola kao što su HTTPS, sFTP, SSH, te drugih protokola koji omogućavaju kriptiranje i zaštitu kritičnih podataka tijekom prijenosa. Subjekt je dužan redovito provjeravati konfiguracije mrežnih protokola i osigurati ažuriranje na sigurne inačice.

Provjera usklađenosti uključuje pregled konfiguracija mrežnih protokola, analizu dnevničkih zapisa prijenosa podataka i konzultacije s odgovornim osobljem za mrežnu sigurnost kako bi se potvrdila primjena sigurnih protokola.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Koriste se nesigurni mrežni protokoli ili nesigurne inačice uobičajenih protokola.
2	Sigurni protokoli su implementirani, ali nisu dosljedno primjenjivani ili svojom konfiguracijom i javnom dostupnošću povećavaju površinu napada na organizaciju.
3	Korištenje sigurnih protokola je definirani interni standard, ali nema redovite provjere.
4	Sigurni protokoli su uniformno implementirani i redovito se provjeravaju te ažuriraju.
5	Primjena sigurnih protokola je potpuno integrirana uz automatizirani proces provjere i nadzor korištenja.

Reference:

- **ISO/IEC 27001:2022** (A.8.12)
- **ISO/IEC 27002:2022** (8.12)
- **NIST SP 800-52** (Poglavlje *Guidelines for the Selection and Use of Transport Layer Security (TLS)*)
- **NIST SP 800-53 Rev. 5** (SC-13)
- **NIST CSF v2.0** (PR.DS-02)
- **CIS v8** (3.10, 4.6)

NAD-009: Filtriranje nepoželjnog mrežnog prometa

Ova kontrola osigurava definiranje i primjenu metoda za filtriranje nepoželjnog mrežnog prometa kako bi se smanjio rizik od kibernetičkih prijetnji. To uključuje upotrebu odgovarajućih alata za praćenje i analizu mrežnog prometa, otkrivanje i sprječavanje napada (primjerice IDS/IPS), sigurnosnih politika i drugih rješenja za filtriranje prometa. Kontrola uključuje redovito ažuriranje pravila filtriranja, automatizirano prepoznavanje i blokiranje sumnjivih aktivnosti te dokumentiranje postupaka za upravljanje mrežnim prometom. Poseban naglasak stavlja se na analizu učinkovitosti filtriranja i prilagodbu sigurnosnih politika prema novim prijetnjama.

Provjera uključuje pregled konfiguracija sustava, analizu ažuriranih pravila filtriranja i blokiranja, testiranje učinkovitosti filtriranja, te konzultacije s mrežnim administratorima o postupcima za upravljanje prometom. Također se provodi evaluacija dokumentiranih procedura i analiza reakcija na detektirane prijetnje.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije u dijelu koji se tiče automatskog blokiranja sumnjivih aktivnosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Filtriranje nepoželjnog mrežnog prometa nije implementirano.
2	Implementirano osnovno filtriranje bez redovitog ažuriranja pravila.
3	Filtriranje s redovitim ažuriranjem pravila, ali bez automatiziranog blokiranja.
4	Automatizirano filtriranje s redovitim ažuriranjem i osnovnim blokiranjem sumnjivog prometa.
5	Napredno filtriranje s automatskom analizom anomalija, blokiranjem prijetnji i redovitim testiranjem.

Reference:

- **ISO/IEC 27001:2022** (A.8.21, A.8.23)
- **ISO/IEC 27002:2022** (8.21, 8.23)
- **NIST SP 800-53 Rev. 5** (SI-4, AC-4)
- **NIST CSF v2.0** (Kategorija DE.CM)
- **CIS v8** (9.2, 9.3)

NAD-010: Implementacija UEBA sustava za analizu ponašanja korisnika

Ova kontrola osigurava implementaciju sustava za naprednu analizu ponašanja korisnika (*User and Entity Behavior Analytics – UEBA*) radi identifikacije neuobičajenih ili sumnjivih aktivnosti na mrežnim i informacijskim sustavima. UEBA sustavi koriste algoritme strojnog učenja i analize podataka kako bi otkrili odstupanja od uobičajenih obrazaca ponašanja korisnika i sustava. Implementacija uključuje konfiguriranje sustava, redovito ažuriranje modela ponašanja i integraciju s ostalim sigurnosnim sustavima.

Provjera uključuje pregled konfiguracije UEBA sustava, analizu izvještaja o detektiranim anomalijama, provjeru učinkovitosti sustava kroz simulacije prijetnji te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala točnost detekcija i pravovremena reakcija na otkrivene prijetnje.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	UEBA sustav nije implementiran.
2	Implementiran je osnovni UEBA sustav bez redovitog ažuriranja modela ponašanja.
3	UEBA sustav je implementiran i ažurira se, ali ne prepoznaje sve relevantne anomalije.
4	Implementiran je UEBA sustav s naprednom detekcijom anomalija i redovitim ažuriranjem modela.
5	UEBA sustav je potpuno integriran, optimiziran i automatiziran s visokom točnošću detekcije anomalija.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (SI-4, CA-7)
- **NIST CSF v2.0** (Kategorija DE.AE)
- **CIS v8** (10.7)

NAD-011: Integracija alata za automatizirano otkrivanje i odgovor na incidente

Ova kontrola osigurava implementaciju i integraciju specijaliziranih alata za automatizirano otkrivanje i odgovor na incidente (IDR, EDR, XDR, NDR[1]) s postojećim sigurnosnim kontrolama i procesima. Kontrola uključuje pravilno podešavanje alata za prepoznavanje sumnjivih događaja, postavljanje prioriteta i pravila trijaže te osiguranje da alati automatski generiraju upozorenja i odgovaraju na incidente kako bi se spriječilo preopterećenje informacijama i smanjila mogućnost propuštanja značajnih prijetnji, odnosno kako bi se pravovremeno obradili ključni događaji.

Provjera uključuje pregled implementacije i konfiguracije alata za automatizirano otkrivanje i odgovor na incidente, analizu pravila za trijažu sumnjivih događaja, testiranje učinkovitosti automatskih odgovora, pregled zapisa o detekciji i odgovoru te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala učinkovita integracija s postojećim sigurnosnim kontrolama.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije u dijelu koji se tiče automatskog odgovora na incidente.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt ne koristi alate za automatizirano otkrivanje i odgovor na incidente.
2	Odabrani alati su implementirani, ali samo na ograničen broj sustava i bez potpune integracije s drugim sigurnosnim kontrolama.
3	Subjekt koristi jedan ili više alata za otkrivanje i odgovor na incidente koji su djelomično integrirani s procesima detekcije, trijaže i odgovora. Pravila za prepoznavanje sumnjivih događaja su definirana, a automatska upozorenja generiraju se na temelju poznatih uzoraka prijetnji.
4	Alati su implementirani i integrirani u sigurnosnu infrastrukturu. Pravila za trijažu i prioritetne odgovore su usklađena s klasifikacijom imovine, rizicima i poslovnim prioritetima. Automatizacija uključuje više faza odgovora, uključujući prikupljanje forenzičkih podataka, automatsko otvaranje incidenata i početnu izolaciju. Alati se redovito ažuriraju prema novim prijetnjama i povezani su s drugim sigurnosnim mehanizmima (primjerice SIEM, SOAR). Postoje formalni procesi evaluacije učinkovitosti sustava i redovita izvješća o djelovanju alata.

[1] **IDR** (*Incident Detection and Response*), **EDR** (*Endpoint Detection and Response*), **XDR** (*Extended Detection and Response*), **NDR** (*Network Detection and Response*)

5	Subjekt koristi napredno integrirani sigurnosni ekosustav temeljen na IDR/EDR/XDR/NDR rješenjima s potpuno automatiziranim odgovorom i orkestracijom (npr. putem SOAR platforme). Automatizirani odgovori uključuju blokiranje, izolaciju, deaktivaciju računa, obavještavanje korisnika i pokretanje predefinirani postupaka (engl. *playbook*). Subjekt ima iznimno visoku razinu pripravnosti, s minimalnim rizikom od preopterećenja informacijama.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (IR-4, IR-5, SI-4, AU-13, CA-7)
- **NIST CSF v2.0** (DE.CM-3, RS.AN-1)
- **CIS v8** (13.7, 13.8, 13.11)

NAD-012: Sustavi za prikupljanje i analizu dnevničkih zapisa

Ova kontrola osigurava implementaciju sustava za prikupljanje, analizu i čuvanje sigurnosno relevantnih dnevničkih zapisa s kritičnih mrežnih i informacijskih sustava. Sustavi moraju omogućiti bilježenje aktivnosti, uključujući pristup, izmjene korisničkih prava i sigurnosne događaje, te omogućiti forenzičke analize s ciljem otkrivanja i reagiranja na incidente. Period čuvanja zapisa definira se sukladno procjeni rizika i kapacitetima za pohranu, s minimalnim trajanjem od 90 dana, gdje je tehnički izvedivo.

Provjera uključuje analizu konfiguracije sustava za bilježenje zapisa, pregled uzoraka zapisa te konzultacije s odgovornim timovima kako bi se osigurala usklađenost sa zahtjevima mjere i primjena dobrih praksi u pohrani podataka.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustavi za prikupljanje sigurnosno relevantnih zapisa nisu implementirani.
2	Prikupljanje sigurnosno relevantnih zapisa je ograničenog opsega bez jasno definiranih kriterija što se prikuplja i koliko se čuva, a analize ili uvidi u podatke se ne provode.
3	Sustavi za prikupljanje sigurnosno relevantnih zapisa pokrivaju ključne sustave i ključne sigurnosne događaje.
4	Sustavi za prikupljanje sigurnosno relevantnih zapisa pokrivaju sve ključne sustave i tipove događaja, omogućuju korelaciju i osnovne analize.
5	Sustavi za prikupljanje sigurnosno relevantnih zapisa su potpuno integrirani u svakodnevne operativne poslove kibernetičke sigurnosti, optimizirani su i podržavaju napredne analize i forenziku događaja.

Reference:

- **ISO/IEC 27001:2022** (A.8.15)
- **ISO/IEC 27002:2022** (8.15)
- **NIST SP 800-53 Rev. 5** (AU-2, AU-3, AU-4, AU-6, AU-9, SI-4)
- **NIST CSF v2.0** (DE.AE-3)
- **CIS v8** (8.4, 8.5)

NAD-013: Sinkronizacija vremena između sustava

Ova kontrola osigurava da svi mrežni i informacijski sustavi subjekta imaju sinkronizirano vrijeme putem pouzdanog izvora. Sinkronizacija vremena ključna je za korelaciju dnevničkih zapisa između različitih sustava i omogućavanje točne analize događaja.

Provjera usklađenosti obuhvaća pregled konfiguracije sinkronizacije vremena na mrežnim i informacijskim sustavima te provjeru dosljednosti vremenskih oznaka u dnevničkim zapisima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustavi nemaju međusobno sinkronizirano vrijeme.
2	Sinkronizacija vremena implementirana je samo na ograničenom broju sustava.
3	Sinkronizacija vremena primijenjena je na svim ključnim sustavima, ali postoje odstupanja.
4	Sinkronizacija vremena primijenjena je na svim sustavima bez značajnih odstupanja.
5	Sinkronizacija vremena potpuno je implementirana na svim mrežnim i informacijskim sustavima.

Reference:

- **ISO/IEC 27001:2022** (A.8.17)
- **ISO/IEC 27002:2022** (8.17)
- **NIST SP 800-53 Rev. 5** (SC-45)
- **CIS v8** (8.4)

NAD-014: Godišnji pregled i ažuriranje mjera zaštite mreže

Ova kontrola osigurava provođenje godišnjeg pregleda svih tehničkih i organizacijskih mjera zaštite mreže kako bi se osigurala njihova učinkovitost i relevantnost. Proces uključuje analizu trenutnih prijetnji, ranjivosti i promjena u poslovnom okruženju, kao i dokumentiranje i odobravanje predloženih promjena od strane odgovornih osoba. Ažuriranje mjera treba biti u skladu s najboljim praksama i novim sigurnosnim zahtjevima.

Provjera usklađenosti uključuje pregled dokumentacije o provedenim godišnjim pregledima, analiza prijedloga za ažuriranje mjera zaštite te konzultacije s odgovornim osobama kako bi se potvrdila pravovremena implementacija promjena.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Godišnji pregled mjera zaštite mreže se ne provodi.
2	Godišnji pregled je proveden, ali bez dokumentiranih rezultata.
3	Pregled je proveden s dokumentiranim rezultatima i prijedlozima za poboljšanje, ali bez ažuriranja mjera.
4	Redoviti godišnji pregled s dokumentiranim rezultatima i djelomičnim ažuriranjem mjera zaštite.
5	Godišnji pregled proveden s dokumentiranim rezultatima i potpunim ažuriranjem mjera zaštite u skladu s novim prijetnjama.

Reference:

- **ISO/IEC 27001:2022** (9)
- **ISO 22301:2019** (9)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (CA-2, CA-7, RA-3, SI-4)
- **NIST CSF v2.0** (Kategorija ID.RA)

NAD-015: Zaštita i integritet dnevničkih zapisa

Ova kontrola osigurava primjenu mjera za zaštitu dnevničkih zapisa od neovlaštenog pristupa, izmjena i manipulacija. Dnevnički zapisi moraju biti pohranjeni u sigurnim sustavima s redovitim sigurnosnim kopijama.

Provjera uključuje pregled konfiguracije kriptiranja podataka u prijenosu i kontrole pristupa sustavima za upravljanje dnevničkim zapisima. Pregled sigurnosnih kopija i analiza sustava za praćenje integriteta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Zaštita dnevničkih zapisa nije implementirana.
2	Implementirane su osnovne mjere zaštite zapisa na izvorišnim sustavima.
3	Dnevnički zapisi su zaštićeni prebacivanjem na središnju kontroliranu lokaciju.
4	Kopije dnevničkih zapisa su zaštićene strožom kontrolom pristupa nego na izvorišnom sustavu.
5	Implementirani su mehanizmi koji onemogućuju promjenu kopija dnevnički zapisa ili obavještavaju u slučaju pokušaja.

Reference:

- **ISO/IEC 27001:2022** (A.8.13, A.8.15)
- **ISO/IEC 27002:2022** (8.13, 8.15)
- **NIST SP 800-53 Rev. 5** (AU-9, AU-10, AU-11, SC-13)
- **NIST CSF v2.0** (Kategorija PR.DS)
- **CIS v8** (8.1, 8.3)

NAD-016: Centralizirana pohrana i analiza dnevničkih zapisa

Ova kontrola osigurava centraliziranu pohranu sigurnosno relevantnih dnevničkih zapisa s mrežnih i informacijskih sustava subjekta. Dnevnički zapisi trebaju se kontinuirano ili u intervalima ne duljima od 24 sata kopirati na centralizirani sustav koji omogućuje pretragu, analizu i zaštitu od neautoriziranog pristupa i izmjena. Centralizirani sustav treba imati mogućnosti prepoznavanja anomalija, detekcije incidenata i generiranja upozorenja o sumnjivim događajima. Proces treba uključivati provjeru ispravnosti bilježenja zapisa i minimalizaciju lažno pozitivnih i lažno negativnih događaja.

Provjera usklađenosti obuhvaća pregled dokumentacije o centraliziranom sustavu za bilježenje zapisa, analizu konfiguracije sustava, provjeru mehanizama za prepoznavanje anomalija te ispitivanje putem simulacija ili testnih događaja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Centralizirani sustav za pohranu dnevničkih zapisa nije implementiran.
2	Dnevnički zapisi se centralno pohranjuju, ali nisu zaštićeni od neautoriziranog pristupa ili izmjena
3	Implementirana je centralizirana pohrana s osnovnom zaštitom i mogućnošću pretrage zapisa.
4	Centralizirani sustav omogućava analizu dnevničkih zapisa i prepoznavanje anomalija.
5	Sustav je potpuno integriran, s naprednom analizom, prepoznavanjem incidenata i generiranjem upozorenja.

Reference:

- **ISO/IEC 27001:2022** (A.8.15)
- **ISO/IEC 27002:2022** (8.15)
- **NIST SP 800-53 Rev. 5** (AU-2, AU-3, AU-12)
- **NIST CSF v2.0** (DE.AE-3)
- **CIS v8** (8.9)

INV-001: Definiranje pravila i odgovornosti za upravljanje imovinom

Pravila i odgovornosti za upravljanje programskom i sklopovskom imovinom ključni su za osiguranje sigurnosti i učinkovitog nadzora imovine. Ova kontrola obuhvaća definiranje specifičnih zaduženja i zadataka, uključujući način klasifikacije imovine, upravljanje inventarom i postupke za održavanje. Postavljanjem jasnih pravila subjekt izbjegava nejasnoće u upravljanju i povećava odgovornost ključnih osoba. Subjekt treba dokumentirati sve odgovornosti i osigurati da su relevantne informacije dostupne dionicima.

Provjerava se je li subjekt jasno definirao i dokumentirao pravila za upravljanje imovinom, uključujući postupke za klasifikaciju, vođenje inventara i održavanje. Posebno se ispituje usklađenost pravila s poslovnim ciljevima i sigurnosnim zahtjevima. Analizira se jesu li zaduženja za upravljanje imovinom jasno dodijeljena te jesu li informacije o odgovornostima dostupne relevantnim dionicima. Također, ocjenjuje se postojanje mehanizama za praćenje provedbe pravila i eventualnih ažuriranja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Pravila i odgovornosti nisu definirani.
2	Pravila su definirana, ali nisu formalizirana.
3	Pravila su formalizirana, ali povremeno ažuriranje ili komunikacija nedostaje.
4	Pravila su formalizirana i ažurirana, s manjim nedostacima u dokumentaciji.
5	Pravila su potpuno definirana, ažurirana i jasno komunicirana svim relevantnim osobama.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.10)
- **ISO/IEC 27002:2022** (5.9, 5.10)
- **NIST CSF v2.0** (Kategorija ID.AM)
- **CIS v8** (1.1)

INV-002: Klasifikacija imovine i podataka prema kritičnosti

Kategorizacija te klasifikacija imovine i podataka prema kriterijima kritičnosti omogućuje subjektu da primjeni diferencirane sigurnosne mjere u skladu s njihovom važnosti za poslovanje. Klasifikacija obuhvaća različite vrste imovine i podataka, uključujući poslovne aplikacije, infrastrukturu, javno dostupne servise, kao i skupove podataka poput osobnih podataka i poslovnih tajni.

Pregledava se jesu li kriteriji za klasifikaciju imovine i podataka prema kritičnosti jasno definirani i dokumentirani. Analiziraju se popisi kategorija imovine i podataka kako bi se utvrdilo je li klasifikacija provedena dosljedno i uključuje li sve relevantne elemente, poput poslovnih aplikacija, infrastrukture i osjetljivih podataka.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Klasifikacija imovine i podataka prema kritičnosti nije provedena.
2	Osnovna klasifikacija imovine i podatka prema kritičnosti postoji, ali nije formalno dokumentirana ili ažurirana.
3	Klasifikacija imovine i podatka je formalizirana, ali nije dosljedna.
4	Klasifikacija imovine i podatka je sveobuhvatna i ažurirana, uz manje nedostatke u dokumentaciji.
5	Klasifikacija imovine i podatka je potpuno definirana, dokumentirana i redovito ažurirana u skladu s poslovnim i sigurnosnim zahtjevima.

Reference:

- **ISO/IEC 27001:2022** (A.5.10, A.5.12, A.5.13)
- **ISO/IEC 27002:2022** (5.10, 5.12, 5.13)
- **NIST SP 800-53 Rev. 5** (MP-3, RA-2, RA-3)
- **NIST CSF v2.0** (ID.AM-05)

INV-003: Definiranje kriterija za identifikaciju kritične imovine

Kritična imovina mora biti jasno identificirana na temelju unaprijed definiranih kriterija. Ovi kriteriji uključuju aspekte poput dostupnosti, povjerljivosti i cjelovitosti podataka. Također, važno je uzeti u obzir značaj imovine za poslovanje i potencijalne posljedice njenog ugrožavanja. Subjekt može uspostaviti smjernice koje omogućuju standardizaciju identifikacije kritične imovine. Cilj nije samo popisivanje sustava, već osiguranje da svaki kritični element dobije odgovarajuću razinu pažnje i zaštite.

Provjerava se dokumentacija o kriterijima za identifikaciju kritične imovine kako bi se utvrdilo jesu li jasno definirani i primjenjivi na različite vrste imovine. Posebna pažnja posvećuje se aspektima poput dostupnosti, povjerljivosti, cjelovitosti i poslovnog značaja. Analizira se popis kritične imovine radi usklađenosti s definiranim kriterijima i utvrđuje jesu li ključni elementi pravilno identificirani za primjenu odgovarajuće razine zaštite.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Kriteriji za identifikaciju kritične imovine nisu definirani.
2	Kriteriji su postavljeni, ali nisu formalizirani niti prilagođeni.
3	Kriteriji su formalizirani, ali nisu dovoljno detaljni ili ažurirani.
4	Kriteriji su detaljni i redovito se ažuriraju, uz manje nedostatke u provedbi.
5	Kriteriji su potpuno definirani, formalizirani i redovito ažurirani te obuhvaćaju sve aspekte.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.12)
- **ISO/IEC 27002:2022** (5.9, 5.12)
- **NIST SP 800-53 Rev. 5** (RA-2, RA-3)

INV-004: Dokumentacija, revizija i ažuriranje inventara kritične imovine

Inventar kritične imovine služi kao osnovni alat za upravljanje i zaštitu ključnih resursa subjekta. Ovaj inventar obuhvaća sve važne informacije o imovini, uključujući popis ključnih mrežnih i informacijskih sustava, identifikatore imovine (npr. inventurni brojevi), lokaciju, odgovornu osobu ili organizacijsku jedinicu. Dokumentacija mora biti ažurirana i prilagođena promjenama u poslovnim potrebama, rizicima i tehnološkim zahtjevima. Osim vođenja detaljne evidencije, subjekt mora osigurati redovitu reviziju inventara kako bi provjerio točnost podataka, identificirao nove sustave i uklonio zastarjele.

Provjera usklađenosti uključuje pregled inventara i dokumentacije inventara, analizu dosljednosti ažuriranja i provjeru provedenih revizija. Posebna pažnja posvećuje se točnosti podataka o imovini, uključenim odgovornim osobama te evidenciji ažuriranja i usklađenosti s poslovnim potrebama. Također se ispituje u kojoj mjeri dokumentacija inventara podržava operativno upravljanje i procese sigurnosnog nadzora odnosno je li dokumentacija organizirana tako da omogućuje brzo prepoznavanje i reakciju na sigurnosne incidente ili tehničke probleme.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Inventar kritične imovine nije dokumentiran, ne postoji definirani postupak vođenja evidencije niti ažuriranja.
2	Inventar je nepotpun, nesustavno vođen, bez jasnih kriterija ažuriranja ili revizije.
3	Inventar je dokumentiran i sadrži ključne informacije, ali ažuriranje i revizije nisu sustavno provedene ili imaju značajne nedostatke.
4	Inventar je ažuriran i obuhvaća većinu kritičnih sustava, provode se redovite revizije, uz povremene nedostatke u dokumentaciji ili ažuriranju.
5	Inventar je potpuno ažuriran, detaljno dokumentiran i obuhvaća sve kritične elemente, uz redovite revizije i prilagodbu sigurnosnim i poslovnim potrebama.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.12, A.5.13)
- **ISO/IEC 27002:2022** (5.9, 5.12, 5.13)
- **NIST SP 800-53 Rev. 5** (CM-8)
- **NIST CSF v2.0** (Kategorija ID.AM)
- **CIS v8** (1.1)

INV-005: Upravljanje inventarom mrežnih i informacijskih sustava

Ova kontrola osigurava da subjekt vodi sveobuhvatan, ažuran i strukturiran inventar odnosno popis i pregled svih mrežnih i informacijskih sustava, tj. svih resursa koje subjekt koristi u pružanju svojih usluga s ciljem razumijevanja sigurnosne arhitekture sustava, kategorizacije prema funkcionalnim ulogama i optimizaciju mjera zaštite.

Provjera usklađenosti uključuje pregled dokumentacije inventara, njene strukture i ažuriranosti popisa mrežnih i informacijskih sustava, analizu kategorizacije sustava prema njihovom značaju i sigurnosnim zahtjevima, pregled dokumentacije o jasno dodijeljenim odgovornostima i lokaciji za sve stavke inventara uključujući i vanjske pružatelje usluga, provjeru dosljedne primjene jedinstvenih identifikatora, provjeru kako se inventar prilagođava poslovnim potrebama i sigurnosnim rizicima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Popis mrežnih i informacijskih sustava ne postoji.
2	Popis sustava postoji, ali nije potpun, formaliziran niti redovito ažuriran, te podaci o odgovornim osobama i lokacijama su nesustavno evidentirani.
3	Inventar je dokumentiran i obuhvaća kritične sustave, ali redovito ažuriranje i kategorizacija nisu formalno definirani, što dovodi do nedostataka u podacima.
4	Inventar je redovito ažuriran i obuhvaća većinu mrežnih i informacijskih sustava, uz manje nedostatke u dokumentaciji i analizi usklađenosti s poslovnim potrebama i sigurnosnim zahtjevima.
5	Inventar je sveobuhvatan i potpuno dokumentiran, redovito i sustavno ažuriran te uključuje kategorizaciju, segmentaciju, odgovorne osobe i povezanost s poslovnim potrebama.

Reference:

- **ISO/IEC 27001:2022** (A.5.9)
- **ISO/IEC 27002:2022** (5.9)
- **NIST SP 800-53 Rev. 5** (CM-8, PM-5, PM-7)
- **NIST CSF v2.0** (Kategorija ID.AM)
- **CIS v8** (1.1)

INV-006: Upravljanje korištenjem kritične imovine izvan prostora subjekta

Ova kontrola osigurava da subjekt jasno identificira koja se kritična programska i sklopovska imovina koristi izvan njezinih prostora i uspostavi odgovornosti za njeno čuvanje, korištenje i vraćanje. Identifikacija treba uključivati vrstu imovine, lokaciju njezina korištenja i svrhu korištenja, dok definirane odgovornosti trebaju obuhvatiti jasno dodijeljene zadatke, procedure kontrole i zahtjeve za vraćanje imovine. Cilj je smanjiti rizike povezane s gubitkom, krađom ili zlouporabom te omogućiti donošenje informiranih odluka o upravljanju takvom imovinom odnosno prepoznati imovinu koja je izložena povećanim rizicima zbog korištenja izvan sigurnosnog okruženja subjekta.

Analizira se dokumentacija o korištenju kritične imovine izvan prostora subjekta kako bi se utvrdilo jesu li jasno evidentirani vrsta imovine, lokacija i svrha njezina korištenja uz analizu jasnoće dodijeljenih odgovornosti i definiranih procedura za čuvanje, korištenje i vraćanje imovine. Procjenjuje se jesu li provedene redovite analize uz evaluaciju učestalosti ažuriranja podataka i prilagodbe sigurnosnih mjera u skladu s promjenama u poslovnim potrebama te omogućuju li donošenje informiranih odluka o upravljanju rizicima povezanim s takvom imovinom.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Korištenje kritične imovine izvan prostora subjekta se ne evidentira.
2	Postoji evidencija, ali nisu dokumentirani svi ključni podaci niti formalizirane odgovornosti.
3	Identifikacija i odgovornosti su formalizirane, te se provodi evidencija imovine koja se koristi izvan prostora subjekta ali povremeno nedostaju ključni podaci ili redovita ažuriranja.
4	Identifikacija je ažurirana i obuhvaća većinu imovine, a odgovornosti su jasno definirane, uz manje proceduralne nedostatke.
5	Korištenje kritične imovine izvan prostora subjekta uz definirane odgovornosti je potpuno identificirano, dokumentirano i redovito ažurirano, a proces upravljanja je usklađen sa sigurnosnim politikama ili se imovina subjekta ne koristi izvan prostora subjekta.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.11, A.5.20)
- **ISO/IEC 27002:2022** (5.9, 5.11, 5.20)

INV-007: Proširenje inventara i kategorizacija imovine manje kritičnosti

Ova kontrola zahtijeva proširenje postojećeg inventara kritične imovine kako bi uključivao programsku i sklopovsku imovinu manje kritičnosti te njezinu kategorizaciju unutar klasifikacijskog sustava subjekta. Proširenjem inventara subjekt dobiva širu sliku o resursima koji, iako manje kritični, mogu utjecati na sigurnost kritične imovine, dok kategorizacija omogućuje preciznije upravljanje rizicima i primjenu specifičnih sigurnosnih mjera. Subjekt treba definirati jasne kategorije imovine manje kritičnosti, primjerice testne sustave, aplikacije za podršku ili infrastrukturu koja nije dio kritičnog operativnog okruženja. Kategorizacija mora biti usuglašena s postojećim klasifikacijskim sustavom, kako bi se osigurala dosljednost u upravljanju inventarom i sigurnosnim mjerama.

Provjerava se je li subjekt proširio inventar kako bi uključio programsku i sklopovsku imovinu manje kritičnosti. Analizira se kategorizacije imovine, uključujući usklađenost s postojećim klasifikacijskim sustavom. Provjerava se dokumentacija o novim kategorijama i načinima njihovog integriranja u proces upravljanja inventarom, odnosno kako su ti resursi identificirani i dodani u inventar te jesu li uzeti u obzir njihovi potencijalni rizici.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Inventar ne uključuje imovinu manje kritičnosti, niti je uspostavljena kategorizacija.
2	Postoji djelomičan popis takve imovine s kategorizacijom, ali nije formaliziran niti ažuriran.
3	Inventar je formaliziran, a kategorizacija uspostavljena, ali nedostaju ključne informacije ili ažuriranja.
4	Inventar i kategorizacija su ažurirani i obuhvaćaju većinu manje kritične imovine.
5	Inventar je potpuno proširen, kategorizacija je jasno definirana i usklađena s poslovnim i sigurnosnim potrebama, a podaci se redovito ažuriraju i omogućavaju sveobuhvatnu procjenu rizika.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.12)

- **ISO/IEC 27002:2022** (5.9, 5.12)
- **NIST CSF v2.0** (Kategorija ID.AM)
- **CIS v8** (1.1)

INV-008: Ažuriranje inventara kritične imovine kroz proces nabave ili automatizaciju

Ova kontrola osigurava da se inventar kritične imovine redovito ažurira putem jednog od dva pristupa:

a) Integracija s procesom nabave, pri čemu se svaka nova programska ili sklopovska imovina, uključujući zamjene postojećih resursa, evidentira u inventaru, ili

b) Automatizacija ažuriranja, gdje tehnički mehanizmi onemogućuju uvođenje imovine u upotrebu bez istovremenog ažuriranja inventara.

Implementacijom jednog od ova dva pristupa smanjuje se rizik od neusklađenosti između stvarnog stanja i dokumentacije te se osigurava pravovremeno ažuriranje podataka o kritičnoj imovini. Cilj je eliminirati mogućnost da se nova imovina koristi bez odgovarajuće evidencije u inventaru.

Provjerava se dokumentacija i primjena procesa/postupaka ažuriranja inventara kroz proces nabave imovine te provjeravaju postoje li formalizirani i jasni postupci koji osiguravaju dosljednost evidencije i obvezuju li odgovorne osobe ili timove da ažuriraju inventar prilikom svake nabave. Provjerava se dokumentacija o nabavama kako bi se utvrdilo prati li je ažuriranje relevantnih podataka, uključujući identifikatore, lokaciju i odgovorne osobe. Ako je implementirana automatizacija, analiziraju se tehnički mehanizmi koji sprječavaju izmjene imovine bez ažuriranja inventara, uključujući generiranje upozorenja ili blokiranje aktivnosti kada ažuriranje inventara izostane. Također se procjenjuje koliko je automatizacija integrirana s procesima implementacije i održavanja te kako doprinosi smanjenju rizika ljudske pogreške i dosljednom praćenju imovine.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ažuriranje inventara nije integrirano s nabavom niti je automatizirano.
2	Postoje osnovne smjernice za ažuriranje inventara, ali nisu formalizirane niti dosljedno primijenjene kroz nabavu ili automatizaciju.
3	Ažuriranje inventara je formalizirano kroz proces nabave ili automatizaciju, ali povremeno dolazi do odstupanja ili tehničkih poteškoća.
4	Ažuriranje inventara provodi se redovito kroz proces nabave ili automatizirane mehanizme, uz manje tehničke ili nedostatke u dokumentaciji.

5	Ažuriranje je potpuno integrirano u proces nabave ili automatizirano i integrirano s poslovnim procesima, sustavno i redovito se provodi te dokumentira.

Reference:

- **ISO/IEC 27001:2022** (A.5.9)
- **ISO/IEC 27002:2022** (5.9)
- **NIST SP 800-53 Rev. 5** (CM-8, PM-5)
- **NIST CSF v2.0** (ID.AM-01, ID.AM-02, ID.AM-04)
- **CIS v8** (1.1, 2.1, 2.4)

INV-009: Fizička identifikacija i označavanje imovine

Subjekt mora implementirati sustave za fizičku identifikaciju i označavanje imovine koja se koristi za obradu podataka. Označavanje treba biti jasno, trajno i omogućiti jednostavno prepoznavanje imovine u svakodnevnim operacijama. Cilj ove kontrole je osigurati da je sva imovina jasno označena kako bi se olakšalo upravljanje i smanjila mogućnost gubitka ili zlouporabe. Prilikom označavanja potrebno je koristiti standardizirane metode koje odgovaraju potrebama subjekta, uključujući kodiranje imovine putem naljepnica, bar kodova ili *RFID* oznaka.

Pregledava se implementacija sustava za fizičku identifikaciju i označavanje imovine kako bi se utvrdilo jesu li metode označavanja, poput naljepnica, bar kodova ili *RFID* oznaka, jasno definirane i standardizirane. Provjerava se dokumentacija o korištenim metodama i njihovoj primjeni na relevantnu imovinu. Također se ocjenjuje koliko označavanje olakšava upravljanje imovinom i smanjuje rizik od gubitka ili zlouporabe u svakodnevnim operacijama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Fizička identifikacija i označavanje nisu uspostavljeni.
2	Postoji osnovni sustav označavanja, ali nije formaliziran niti ažuriran.
3	Sustav označavanja je formaliziran, ali povremeno dolazi do propusta u označavanju ili održavanju oznaka.
4	Označavanje je ažurirano i provodi se dosljedno, uz manje nedostatke.
5	Sustav označavanja je potpuno uspostavljen, formaliziran, prilagođen potrebama subjekta i automatiziran korištenjem tehnologija poput *IoT* i *RFID*.

Reference:

- **ISO/IEC 27001:2022** (A.5.9, A.5.10, A.5.12, A.5.13)
- **ISO/IEC 27002:2022** (5.9, 5.10, 5.12, 5.13)
- **NIST SP 800-53 Rev. 5** (PE-22)
- **CIS v8** (2.1, 3.7)

POD-001: Identifikacija kritičnih podataka na temelju kriterija rizika i značaja

Kontrola osigurava identifikaciju kritičnih podataka prema jasno definiranim kriterijima koji uključuju zahtjeve za dostupnost, povjerljivost, cjelovitost i autentičnost podataka. Identifikacija mora uzeti u obzir i rizike povezane s podacima te njihov značaj za kontinuitet poslovanja subjekta. Kroz dosljednu identifikaciju, subjekt dobiva bolji uvid u osjetljive skupove podataka i osigurava usklađenost svojih sigurnosnih mjera s razinom rizika i poslovnim zahtjevima.

Provjerava se jesu li podaci identificirani na način koji odražava njihov značaj za kontinuitet poslovanja i povezane rizike. Također se analizira u kojoj mjeri identifikacija doprinosi boljem upravljanju osjetljivim skupovima podataka i prilagodbi sigurnosnih mjera razini identificiranih rizika.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne provodi se identifikacija kritičnih podatka.
2	Identifikacija je provedena djelomično, bez formalne dokumentacije.
3	Identifikacija je formalizirana, ali nije uzeta u obzir procjena rizika.
4	Identifikacija je sveobuhvatna i ažurirana, procjena rizika je uzeta u obzir, ali podatci nisu kategorizirani.
5	Identifikacija je sveobuhvatna, ažurirana i podatci su kategorizirani.

Reference:

- **ISO/IEC 27001:2022** (A.5.12)
- **ISO/IEC 27002:2022** (5.12)
- **NIST SP 800-53 Rev. 5** (RA-2, RA-3, RA-9)
- **NIST CSF v2.0** (ID.AM-05)
- **CIS v8** (3.2, 3.7)

POD-002: Sigurno pohranjivanje pričuvnih kopija

Ova kontrola osigurava sigurno pohranjivanje pričuvnih kopija podataka kako bi se zaštitila njihova povjerljivost, cjelovitost i dostupnost. Obuhvaća primjenu odgovarajućih fizičkih kontrola (kao što je ograničenje pristupa) i logičkih kontrola (kao što je kriptiranje), uz osiguranje da su pričuvne kopije pohranjene na sigurnim lokacijama udaljenima od primarnih sustava kako bi se smanjio rizik od katastrofa. Kontrola također uključuje definiranje procesa redovitog testiranja valjanosti i integriteta pričuvnih kopija.

Provjera uključuje pregled dokumentacije o procesima pohranjivanja pričuvnih kopija, analizu fizičkih i logičkih sigurnosnih kontrola na lokacijama gdje su pohranjene pričuvne kopije, provjeru rezultata testiranja valjanosti i integriteta pričuvnih kopija, kao i konzultacije s odgovornim osobljem kako bi se osigurala dosljedna primjena definiranih sigurnosnih mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurnosne kontrole za pričuvne kopije nisu uspostavljene ni dokumentirane.
2	Osnovne fizičke i logičke kontrole su uspostavljene, ali nisu sveobuhvatne.
3	Kontrole su definirane i primijenjene, ali nisu redovito testirane.
4	Sveobuhvatne kontrole su definirane, dokumentirane i redovito testirane.
5	Sigurnosne kontrole su potpuno integrirane i automatizirane uz kontinuirani nadzor.

Reference:

- **ISO/IEC 27001:2022** (A.8.13)
- **ISO/IEC 27002:2022** (8.13)
- **NIST SP 800-53 Rev. 5** (CP-9, SC-28)
- **NIST CSF v2.0** (PR.DS-01, PR.DS-11)
- **CIS v8** (Kontrola 11)

POD-003: Definiranje pravila za korištenje prijenosnih medija

Ova kontrola zahtijeva definiranje pravila koja uređuju korištenje prijenosnih medija za pohranu kritičnih podataka. Pravila moraju jasno navesti dopuštenu svrhu korištenja, sigurnosne zahtjeve (npr. onemogućavanje izvršenja programskog koda) i postupke za redovite provjere prijenosnih medija. Cilj je osigurati da su svi prijenosni mediji korišteni na siguran način te isključivo za poslovne svrhe. Pravila također trebaju obuhvatiti kada je potrebna obveza korištenja kriptiranja za pohranu osjetljivih podataka i automatizirane provjere na prisutnost malicioznih sadržaja, čime se smanjuje rizik od sigurnosnih incidenata.

Provjeravaju se dokumentirana pravila za korištenje prijenosnih medija kako bi se utvrdilo uključuju li jasno definirane svrhe korištenja, sigurnosne zahtjeve i postupke za redovite provjere. Analizira se je li obveza korištenja kriptiranja i automatiziranih provjera na prisutnost malicioznih sadržaja pravilno dokumentirana i primijenjena.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Pravila za korištenje prijenosnih medija nisu definirana.
2	Pravila su djelomično definirana, ali nisu formalizirana ili usklađena s praksama subjekta.
3	Pravila su formalizirana, ali nisu potpuno prilagođena rizicima ili potrebama subjekta.
4	Pravila su formalizirana i ažurirana, uz povremene nedostatke u pokrivanju svih sigurnosnih aspekata.
5	Pravila su potpuno definirana, dokumentirana i prilagođena poslovnim potrebama te redovito ažurirana.

Reference:

- **ISO/IEC 27001:2022** (A.7.10, A.8.10, A.8.12)
- **ISO/IEC 27002:2022** (7.10, 8.10, 8.12)
- **NIST SP 800-53 Rev. 5** (MP-2, MP-4, MP-5, SC-28)
- **NIST CSF v2.0** (Kategorija PR.DS)
- **CIS v8** (3.9, 10.3, 10.4)

POD-004: Automatizirana provjera prijenosnih medija na prisutnost malicioznih sadržaja

Kontrola zahtijeva implementaciju automatiziranih sustava za provjeru prijenosnih medija na prisutnost malicioznih sadržaja prije njihove upotrebe unutar subjekta. Takva provjera smanjuje rizik od unošenja zlonamjernog softvera u mrežu i osigurava da se prijenosni mediji koriste u skladu sa sigurnosnim standardima.

Procjenjuje se implementacija automatiziranih sustava za provjeru prijenosnih medija kako bi se utvrdilo omogućuju li detekciju malicioznih sadržaja prije njihove upotrebe. Ispituje se ažurnost i prilagodba sustava suvremenim prijetnjama te jesu li procedure za postupanje jasno definirane i dokumentirane.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Automatizirane provjere prijenosnih medija nisu uspostavljene.
2	Postoji osnovna provjera, ali nije u potpunosti automatizirana niti formalizirana.
3	Automatizirane provjere su uspostavljene, ali nisu prilagođene trenutnim prijetnjama.
4	Sustavi su ažurirani i pokrivaju većinu sigurnosnih potreba, uz manje tehničke nedostatke.
5	Sustavi za automatizirane provjere su potpuno funkcionalni, ažurirani i prilagođeni potrebama subjekta.

Reference:

- **ISO/IEC 27001:2022** (A.8.7, A.8.12)
- **ISO/IEC 27002:2022** (8.7, 8.12)
- **NIST SP 800-53 Rev. 5** (MP-7, SI-3, SI-44)
- **NIST CSF v2.0** (PR.IR-03)
- **CIS v8** (13.7)

POD-005: Implementacija procedura za sigurno zbrinjavanje podataka i uređaja

Subjekt mora uspostaviti detaljne procedure za sigurno zbrinjavanje podataka i uređaja koji sadrže kritične informacije. Ove procedure trebaju uključivati metode trajnog brisanja podataka, fizičkog uništavanja uređaja i sigurno zbrinjavanje elektroničkog otpada u skladu s najboljim praksama i zakonskim standardima. Sigurno zbrinjavanje treba biti dokumentirano i nadzirano kako bi se osigurala usklađenost s internim politikama i spriječio potencijalni gubitak osjetljivih podataka tijekom zbrinjavanja.

Procjenjuje se jesu li procedure za sigurno zbrinjavanje podataka i uređaja jasno definirane te uključuju metode poput trajnog brisanja podataka, fizičkog uništavanja uređaja i pravilnog zbrinjavanja elektroničkog otpada (nakon prethodnog brisanja podataka). Pregledava se dokumentacija o provedenim postupcima kako bi se utvrdila njihova usklađenost s internim politikama i pravilima dobre prakse.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Procedure za sigurno zbrinjavanje nisu definirane.
2	Postoje osnovne procedure, ali nisu formalizirane ili usklađene s najboljim praksama.
3	Procedure su formalizirane, ali povremeno dolazi do nedostatka u njihovoj primjeni ili dokumentiranju.
4	Procedure su ažurirane i primjenjuju se dosljedno, uz manje nedostatke u dokumentaciji.
5	Procedure su potpuno formalizirane i prilagođene potrebama subjekta.

Reference:

- **ISO/IEC 27001:2022** (A.8.10, A. 8.12)
- **ISO/IEC 27002:2022** (8.10, 8.12)
- **NIST SP 800-53 Rev. 5** (MP-6, MP-7, SC-28)
- **NIST CSF v2.0** (Kategorija PR.DS)
- **CIS v8** (3.5)

POD-006: Siguran prijevoz uređaja i medija koji sadrže kritične podatke

Cilj ove kontrole je uspostaviti tehničke mjere i postupke za osiguranje sigurnog prijevoza uređaja i medija koji sadržavaju kritične podatke. Kompenzacijske mjere, poput korištenja sigurnih spremnika ili izvanrednog nadzora prijevoza, trebaju se koristiti za jednokratne situacije. Za uređaje koji se često prevoze ili mobilne uređaje, kontrola zahtijeva implementaciju trajnih sigurnosnih rješenja poput kriptiranja medija za pohranu. Osim tehničkih mjera, potrebno je dokumentirati sve aktivnosti vezane uz prijevoz i osigurati pridržavanje internih sigurnosnih smjernica.

Ispituje se jesu li uspostavljeni postupci za osiguranje sigurnog prijevoza uređaja i medija koji sadrže kritične podatke, uključujući korištenje sigurnih spremnika i trajnih sigurnosnih rješenja poput kriptiranja. Pregledava se dokumentacija o aktivnostima prijevoza kako bi se utvrdilo jesu li pravilno evidentirane i usklađene s internim sigurnosnim smjernicama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Siguran prijevoz nije uspostavljen niti dokumentiran.
2	Postoje osnovne mjere za osiguranje prijevoza, ali nisu formalizirane.
3	Mjere za siguran prijevoz su formalizirane, ali povremeno dolazi do tehničkih ili proceduralnih nedostataka.
4	Mjere za siguran prijevoz primjenjuju se dosljedno, uz manje tehničke poteškoće.
5	Siguran prijevoz je potpuno formaliziran, integriran s tehničkim rješenjima i redovito revidiran.

Reference:

- **ISO/IEC 27001:2022** (A.7.10)
- **ISO/IEC 27002:2022** (7.10)
- **NIST SP 800-53 Rev. 5** (MP-5)
- **NIST CSF v2.0** (PR.DS-02)

POD-007: Odobrenje za iznošenje imovine i podataka izvan prostora subjekta

Ova kontrola zahtijeva da iznošenje programske i sklopovske imovine ili podataka izvan prostorija subjekta bude moguće samo uz odobrenje odgovornih osoba. Proces odobravanja treba biti strogo definiran uz dokumentiranje svih aktivnosti.

Provjerava se proces odobravanja iznošenja programske i sklopovske imovine ili podataka izvan prostorija subjekta uz dokumentiranje svih aktivnosti. Analizira se jesu li odgovorne osobe uključene u svaki korak procesa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Postupak odobravanja iznošenja imovine nije uspostavljen.
2	Postoji postupak, ali nije formaliziran.
3	Postupak je formaliziran, ali nije u skladu sa sigurnosnim zahtjevima.
4	Postupak se provodi dosljedno, uz manje proceduralne nedostatke.
5	Postupak je integriran u sigurnosne procese i redovito revidiran ili su poduzete propisane tehničke mjere.

Reference:

- **ISO/IEC 27001:2022** (A.7.10)
- **ISO/IEC 27002:2022** (7.10)
- **NIST SP 800-53 Rev. 5** (MP-5, AC-20)
- **CIS v8** (3.1

RIZ-001: Procjena rizika za kritičnu imovinu temeljem fizičkih prijetnji

Ova kontrola zahtijeva provedbu procjene rizika povezanih s fizičkim prijetnjama za kritičnu imovinu, poput poplava, požara, kvarova, krađa i fizičkog oštećenja imovine. Proces uključuje identifikaciju prijetnji, analizu njihove vjerojatnosti i utjecaja te određivanje razine rizika za svaku prijetnju. Dokumentacija mora sadržavati opis prijetnji, ocjene rizika i predložene mjere za njihovo ublažavanje.

Kako bi se procjena smatrala zadovoljavajućom, potrebno je osigurati da su identificirane sve značajne fizičke prijetnje te da je dokumentacija usklađena sa standardima sigurnosti. Procjena se verificira kroz analizu procesa, dostupnost evidencija i intervjue s odgovornim osobama uključenima u provedbu.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema provedene procjene rizika za fizičke prijetnje.
2	Osnovna procjena obuhvaća samo dio fizičkih prijetnji.
3	Procjena uključuje većinu fizičkih prijetnji, ali bez potpune dokumentacije.
4	Detaljna procjena s dokumentacijom svih relevantnih fizičkih prijetnji.
5	Procjena se redovno ažurira i prilagođava prema novim rizicima.

Reference:

- **ISO/IEC 27001:2022** (6.1)
- **ISO 22301:2019** (6.1)
- **NIST SP 800-53 Rev. 5** (RA-3, PE-14)
- **NIST CSF v2.0** (ID.RA-05)

RIZ-002: Procjena rizika za kritičnu imovinu temeljem kibernetičkih prijetnji

Ova kontrola usredotočena je na procjenu rizika koji proizlaze iz kibernetičkih prijetnji, uključujući ugrožavanje povjerljivosti, integriteta, autentičnosti ili dostupnosti podataka i usluga. Proces uključuje analizu generalnih i čestih ranjivosti sustava te identifikaciju mogućih vektora napada. Rezultati procjene moraju obuhvaćati razvrstavanje prijetnji prema prioritetima i preporuke za ublažavanje utvrđenih rizika, a sve u skladu s metodologijom upravljanja rizicima koju je subjekt uspostavio.

Dokumentacija procjene mora biti potpuna i sadržavati jasne informacije o metodologiji, identificiranim prijetnjama te zaključke o razini rizika. Valjanost procjene potvrđuje se pregledom dokumenata i provjerom konzistentnosti podataka s postojećom metodologijom i načinima obrada rizika, njihove re-evaluacije te prihvaćanja rezidualnih rizika.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema provedene procjene kibernetičkih prijetnji.
2	Procjena identificira osnovne ranjivosti, ali ne uključuje prijetnje.
3	Procjena obuhvaća osnovne prijetnje i ranjivosti, ali nije potpuna.
4	Sveobuhvatna procjena s dokumentacijom kibernetičkih prijetnji.
5	Redovita procjena uz ažuriranje prema novim prijetnjama.

Reference:

- **ISO/IEC 27001:2022** (6.1)
- **ISO 22301:2019** (6.1)
- **NIST SP 800-53 Rev. 5** (RA-3)
- **NIST CSF v2.0** (ID.RA-05)

RIZ-003: Procjena rizika od trećih strana za kritičnu imovinu subjekta

Kontrola pokriva procjenu rizika povezanih s trećim stranama koje imaju utjecaj na sigurnost kritične imovine subjekta. Analiza uključuje pregled ugovorenih usluga, sigurnosnih standarda i praksi pružatelja usluga te identifikaciju mogućih slabosti što čini podlogu za procjenu rizika. Poseban fokus stavlja se na ovisnosti o ključnim dobavljačima i njihove potencijalne ranjivosti koje mogu utjecati na otpornost subjekta, njegov kontinuitet poslovanja ili sigurnost podatka.

Potrebno je osigurati da procjena rizika ukoliko je moguće uključuje specifične mjere prilagodbe ugovora, definiranje SLA-ova (*Service-level Agreement*) i uvođenje dodatnih sigurnosnih zahtjeva. Evaluacija kontrolira konzistentnost analiza s ugovornim obvezama i sigurnosnim smjernicama. Ukoliko subjekt ugovora standardnu uslugu za koju je nemoguće mijenjati uvjete korištenja ili SLA preostali rizik to mora odražavati te može biti prihvaćen.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Rizici od trećih strana za kritičnu imovinu subjekta nisu procijenjeni.
2	Dokumentirana procjena rizika obuhvaća samo ugovore s najkritičnijim trećim stranama.
3	Dokumentirana procjena rizika uključuje većinu trećih strana za kritičnu imovinu i osnovne sigurnosne zahtjeve.
4	Dokumentirana i detaljna procjena rizika uključuje sve treće strane za kritičnu imovinu uz usklađenost sa sigurnosnim zahtjevima.
5	Uz dokumentiranu i detaljnu procjenu rizika koja uključuje sve treće strane i sigurnosne zahtjeve, provodi se i redovito praćenje i ažuriranje procjene rizika trećih strana za kritičnu imovinu.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20)
- **ISO/IEC 27001:2022** (5.19, 5.20)
- **ISO 22301:2019** (6.1, 6,2)
- **NIST SP 800-53 Rev. 5** (RA-3)
- **CIS v8** (15.2)

RIZ-004: Dokumentacija identificiranih rizika i odgovora na rizike

Ova kontrola zahtijeva izradu i održavanje dokumentacije koja bilježi sve identificirane rizike te definirane odgovore na njih odnosno mjere njihove obrade. Dokumentacija mora uključivati detaljan opis rizika, njihovu razinu (vjerojatnost i utjecaj), kao i predložene tehničke, organizacijske ili operativne mjere za smanjenje ili uklanjanje rizika, u skladu s usvojenom metodologijom upravljanja rizicima.

Kako bi se osigurala usklađenost, dokumentacija mora biti formalno strukturirana i redovito ažurirana. Ova se kontrola provjerava kroz pregled dostupne dokumentacije, evaluaciju njene ažurnosti te kroz razgovore s osobama odgovornim za upravljanje rizicima kako bi se potvrdilo razumijevanje i praktična primjena mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema dokumentacije identificiranih rizika ili mjera odgovora na njih.
2	Dokumentacija postoji, ali je nepotpuna i ne ažurira se redovito.
3	Dokumentacija sadrži većinu ključnih rizika i osnovne odgovore.
4	Dokumentacija uključuje sve relevantne rizike i detaljne odgovore.
5	Dokumentacija je potpuno ažurirana i koristi se za donošenje odluka.

Reference:

- **ISO/IEC 27001:2022** (6.1, 6.2, 8.1, 8.2)
- **ISO 22301:2019** (6.1, 6.2, 6.3, 8.1, 8.2)
- **NIST SP 800-53 Rev. 5** (RA-3, PM-9)
- **NIST CSF v2.0** (Kategorija ID.RA)

RIZ-005: Prioritizacija mjera upravljanja rizicima

Ova kontrola osigurava strukturirani proces prioritizacije mjera upravljanja rizicima, uzimajući u obzir razinu izloženosti rizicima, vjerojatnost njihovog nastanka i ozbiljnost njihovih posljedica. Prioritizacija mora uzeti u obzir i širi društveni, gospodarski, međusektorski ili prekogranični utjecaj rizika.

Ova kontrola provjerava se pregledom kriterija prioritizacije, analize donošenja odluka te evaluacijom mjera koje su provedene u skladu s prioritetima. Važno je da dokumentacija pokazuje konzistentan i transparentan proces odlučivanja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema definiranog procesa prioritizacije mjera upravljanja rizicima.
2	Osnovna prioritizacija temelji se na dijelu kriterija, ali nije formalna.
3	Prioritizacija se temelji na većini kriterija, ali nedostaju dokumentirani postupci.
4	Formalna prioritizacija svih mjera uz dokumentaciju postupaka.
5	Prioritizacija je u potpunosti transparentna i redovito se ažurira.

Reference:

- **ISO/IEC 27001:2022** (6.1, 6.2, 8.1, 8.2)
- **ISO 22301:2019** (6.1, 6.2, 6.3, 8.1, 8.2)
- **NIST SP 800-53 Rev. 5** (RA-3, PM-9)
- **NIST CSF v2.0** (ID.RA-06)

RIZ-006: Metode za analizu i procjenu rizika

Ova kontrola zahtijeva implementaciju formaliziranih i detaljnih metoda za analizu i procjenu rizika, odnosno definiranje metodologije upravljanja rizicima, usmjerenih na dosljedno identificiranje, kvantifikaciju, ocjenjivanje prijetnji i ranjivosti koje utječu na kontinuitet poslovnih procesa i imovinu subjekta. Metode moraju uključivati definirane kriterije za procjenu vjerojatnosti događaja i utjecaja, sustave rangiranja te jasno određene procedure za dokumentiranje nalaza i preporuka.

Kako bi se osigurala usklađenost, metode moraju biti dokumentirane i usklađene s postojećim zahtjevima, standardima i smjernicama. Njihova učinkovitost procjenjuje se kroz pregled dokumentiranih analiza rizika, konzistentnost primijenjenih metoda te njihov učinak na donošenje poslovnih odluka.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje metode za analizu, procjenu i obradu rizika.
2	Metode postoje, ali nisu dokumentirane.
3	Metode su dokumentirane, ali se ne primjenjuju dosljedno.
4	Metode se dosljedno primjenjuju.
5	Metode se u potpunosti primjenjuju i usklađene su s postojećim standardima i smjernicama.

Reference:

- **ISO/IEC 27001:2022** (6, 8)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (6, 8)
- **NIST SP 800-53 Rev. 5** (RA-3)
- **NIST CSF v2.0** (ID.RA-04, ID.RA-05)

RIZ-007: Redovito izvještavanje o rizicima

Ova kontrola osigurava uspostavljanje sustava redovitog izvještavanja o identificiranim rizicima, promjenama u procjenama i predloženim mjerama ublažavanja. Izvještaji moraju biti strukturirani i sadržavati ključne informacije kao što su pregled postojećih rizika, nova saznanja, predložene mjere te preporuke za daljnje postupanje.

Sustav izvještavanja mora osigurati da se relevantni dionici pravovremeno obavijeste o ključnim informacijama, omogućujući donošenje informiranih odluka. Procjena učinkovitosti ove kontrole provodi se kroz pregled izvještaja, konzistentnost dostave relevantnim dionicima te praćenje implementacije predloženih mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema uspostavljenog sustava za redovito izvještavanje o rizicima.
2	Izvještavanje se provodi neredovito ili na *ad-hoc* osnovi.
3	Redoviti izvještaji pokrivaju većinu ključnih rizika i dostupni su većini relevantnih dionika.
4	Struktura i sadržaj izvještaja potpuno zadovoljavaju poslovne potrebe i dostupni su svim dionicima.
5	Izvještaji su dosljedni, ažurirani i potpuno integrirani u procese donošenja odluka.

Reference:

- **ISO/IEC 27001:2022** (6, 8, 9.3)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (6, 8, 9.3)
- **NIST SP 800-53 Rev. 5** (RA-3, RA-7, PM-9)
- **NIST CSF v2.0** (ID.RA-06, ID.RA-08))

RIZ-008: Procjena rizika za imovinu manje kritičnosti

Ova kontrola zahtijeva provedbu procjene rizika za imovinu manje kritičnosti kako bi se utvrdio njen utjecaj na sigurnost kritične imovine. Procjena se provodi po istoj metodologiji, a treba uključivati identifikaciju prijetnji, analizu potencijalnih posljedica i prijedloge mjera zaštite za svaku grupu ili kategoriju, u skladu s uspostavljenom metodologijom upravljanja rizicima. *Procjena rizika za imovinu manje kritičnosti može biti sadržana u osnovnoj procjeni rizika za kritičnu imovinu (RIZ-002)*.

Provjerava se dokumentacija o provedenim procjenama i obradama rizika za imovinu manje kritičnosti kako bi se utvrdilo jesu li prijetnje jasno identificirane, posljedice adekvatno analizirane i predložene mjere zaštite relevantne za svaku kategoriju. Ispituje se učestalost procjena i njihova povezanost s procjenom rizika za kritičnu imovinu. Također se ocjenjuje koliko su rezultati procjena korišteni za proaktivno upravljanje sigurnosnim prijetnjama i smanjenje potencijalnih ranjivosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema provedene procjene rizika.
2	Procjena rizika je provedena, ali nije potpuna i ne pridržava se metodologije.
3	Procjena rizika je provedena i pridržava se metodologije, ali nije potpuna.
4	Provedena je sveobuhvatna procjena rizika s pripadajućom dokumentacijom, a sukladno propisanoj metodologiji.
5	Procjena rizika se redovno provodi s pripadajućom dokumentacijom, a sukladno propisanoj metodologiji uz ažuriranje prema novim prijetnjama.

Reference:

- **ISO/IEC 27001:2022** (6, 8)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (6, 8)
- **NIST SP 800-53 Rev. 5** (RA-2, RA-3)
- **NIST CSF v2.0** (Kategorija ID.RA)

RIZ-009: Održavanje i upravljanje registrom identificiranih rizika

Ova kontrola zahtijeva uspostavljanje, održavanje i redovito ažuriranje registra rizika koji sadrži detaljne informacije o svim prepoznatim rizicima, koji je u skladu s uspostavljenom metodologijom upravljanja rizicima, a o sadržaju registra identificiranih rizika potrebno je sustavno informirati relevantne poslovne segmente. Registar mora uključivati opis rizika, procjenu njihove vjerojatnosti i potencijalnog utjecaja, kao i trenutni status te poduzete mjere za upravljanje rizicima i re-evaluaciju vjerojatnosti i utjecaja nakon primjene mjere, odgovornu osobu za primjenu mjere, rok primjene mjere i način verifikacije da je mjera primijenjena. Cilj je osigurati da svi relevantni podaci budu jasno strukturirani i lako dostupni ključnim dionicima.

Učinkovitost kontrole provjerava se pregledom sadržaja i ažuriranosti registra rizika, analizira se povijest promjena kako bi se utvrdila njegova sveobuhvatnost, dosljednost i točnost. Također, osigurava se da registar odgovara poslovnim potrebama i da je u skladu s metodologijom upravljanja rizicima. Dodatno se provjerava postoje li učinkoviti mehanizmi za pravovremeno informiranje poslovnih segmenata putem intervjua s odgovornim osobama kako bi se potvrdila usklađenost s definiranim procesima. Također se analizira dokumentacija o distribuciji informacija, zapisnici sastanaka i izvještaji koji osiguravaju informiranost svih relevantnih dionika, te se provode razgovori s odgovornim osobama kako bi se potvrdila svijest o sadržaju registra i poduzetim mjerama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Registar rizika nije uspostavljen.
2	Registar postoji, ali nije sveobuhvatan ili se ne ažurira redovito.
3	Registar je sveobuhvatan, ali sadrži sporadične propuste u ažuriranju i informiranje se provodi *ad hoc*.
4	Registar je potpuno ažuriran i uključuje sve relevantne podatke, a o promjenama se informira većina dionika.
5	Registar se redovito ažurira, u potpunosti integriran i koristi se za strateško donošenje odluka.

Reference:

- **ISO/IEC 27001:2022** (6, 8)
- **ISO/IEC 27005:2022**

- **ISO 22301:2019** (6, 8)
- **NIST SP 800-53 Rev. 5** (RA-3, PM-9)

RIZ-010: Mjere ublažavanja rizika prije implementacije novih rješenja ili značajnih promjena

Ova kontrola osigurava da se prije implementacije nadogradnji, sigurnosnih unaprijeđena, novih tehnologija, rješenja ili usluga, poduzimaju odgovarajuće unaprijed definirane i nove mjere ublažavanja rizika. Poduzete mjere trebaju biti razmjerne identificiranim prijetnjama i ranjivostima, osiguravati da promjene ne povećavaju rizik ili uvode dodatne ranjivosti ili nestabilnosti te su dokumentirane u skladu s internim smjernicama subjekta ovisno o vrsti promjene, a sve u skladu s usvojenom metodologijom upravljanja rizicima.

Valjanost kontrole provjerava se kroz pregled poduzetih mjera, njihovu primjenjivost na identificirane rizike te konzultacije s odgovornim osobama. Također se ocjenjuje učinkovitost mjera u smanjenju izloženosti rizicima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji proces za ublažavanje rizika prije implementacije novih rješenja. Rizici nisu identificirani ili ostaju bez odgovora ili se mjere poduzimaju reaktivno i neformalno.
2	Mjere ublažavanja se povremeno poduzimaju. Neke mjere se primjenjuju na temelju iskustva ili preporuke sigurnosnog tima, ali bez jasne veze s konkretnim rizicima. Učinkovitost mjera nije evaluirana, a komunikacija s odgovornim osobama nije strukturirana.
3	Postoji formalna obveza primjene unaprijed definiranih mjera ublažavanja rizika ili definiranja novih mjera u slučaju novih okolnosti no njihova primjena ovisi o konkretnim okolnostima pojedinog slučaja. Mjere su razmjerne većini identificiranih rizika.
4	Subjekt ima standardiziran i dokumentiran proces ublažavanja rizika koji se sustavno provodi sukladno internim smjernicama na način da postoje zapis o provedenim promjena i provedenim mjera.
5	Mjere ublažavanja rizika su sastavni dio procesa uvođenja promjena. Odluka o implementaciji se ne donosi dok se sve ključne mjere ne poduzmu i ne potvrdi njihova primjenjivost. Provodi se testiranje efikasnosti mjera, a učinkovitost se redovito ocjenjuje i koristi u strategijama upravljanja rizikom.

Reference:

- **ISO/IEC 27001:2022** (6, 8)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (6, 8)
- **NIST SP 800-53 Rev. 5** (CM-4, SA-3, SI-2, SR-5)
- **NIST CSF v2.0** (ID.RA-07)

RIZ-011: Softverski alati za procjenu i praćenje rizika

Ova kontrola provjerava implementaciju naprednih softverskih alata za procjenu i praćenje rizika kako bi se omogućila detaljna analiza prijetnji, identifikacija ranjivosti i praćenje incidenata u stvarnom vremenu. Alati moraju podržavati automatizirano prikupljanje i analizu podataka, generiranje izvještaja s preporukama za ublažavanje rizika te njihovu integraciju u proces upravljanja rizicima unutar subjekta. Također, potrebno je osigurati redovito ažuriranje i evaluaciju alata kako bi ostali učinkoviti u prepoznavanju novih prijetnji i prilagodbi poslovnim potrebama.

Učinkovitost kontrole provjerava se pregledom instaliranih alata, evaluacijom njihove funkcionalnosti te analizom usklađenosti s potrebama subjekta. Revizija uključuje i provjeru povijesti ažuriranja, testiranje učinkovitosti alata te konzultacije s odgovornim osobama kako bi se osiguralo da se dobiveni rezultati koriste u procesu donošenja odluka i planiranju sigurnosnih mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema implementiranih softverskih alata za procjenu i praćenje rizika.
2	Implementirani alati imaju ograničenu funkcionalnost ili nisu u upotrebi.
3	Alati su u upotrebi, ali ne obuhvaćaju sve ključne funkcionalnosti ili se rezultati ne integriraju dosljedno u procese upravljanja rizicima.
4	Alati su potpuno implementirani, redovito se koriste, ažuriraju i evaluiraju.
5	Alati su potpuno funkcionalni, ažurirani, evaluirani i u potpunosti integrirani u procese donošenja odluka, planiranja sigurnosnih mjera i strateškog upravljanja rizicima.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (RA-5, SI-3, SI-4)
- **NIST CSF v2.0** (ID.RA-01)
- **CIS v8** (7.1, 7.5, 7.6)

RIZ-012: Integracija upravljanja kibernetičkim rizicima u upravljanje rizicima poslovanja (ERM)

Ova kontrola zahtijeva integraciju upravljanja kibernetičkim rizicima u širi okvir upravljanja rizicima na razini poslovanja subjekta (ERM). Subjekt mora osigurati da kibernetički rizici budu formalno identificirani, procijenjeni i integrirani u postojeće procese upravljanja rizicima, zajedno s drugim vrstama rizika koji mogu utjecati na poslovne ciljeve subjekta. Ova integracija omogućuje dosljedno, sveobuhvatno i učinkovito upravljanje rizicima, čime se osigurava usklađenost s poslovnim ciljevima i strateškim prioritetima subjekta.

Provjera valjanosti uključuje pregled dokumentacije koja sadrži politike, procedure i evidencije integracije kibernetičkih rizika u ERM proces. Posebna pažnja posvećuje se povezanosti s poslovnim ciljevima, sposobnosti prilagodbe promjenjivim okolnostima te usklađenosti sa standardima i smjernicama za upravljanje rizicima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Kibernetički rizici nisu prepoznati niti integrirani u ERM proces.
2	Kibernetički rizici su identificirani, ali nisu formalno integrirani.
3	Rizici su djelomično integrirani u ERM proces, ali postoje nedostaci.
4	Rizici su potpuno integrirani i usklađeni s ERM procesom.
5	Rizici su u potpunosti integrirani, ažurirani i redovito evaluirani u sklopu ERM-a.

Reference:

- **ISO/IEC 27001:2022** (6, 8, A.5.8, A.5.21)
- **ISO/IEC 27005:2022**
- **ISO 22301:2019** (6, 8)
- **NIST SP 800-53 Rev. 5** (PM-9)
- **NIST CSF v2.0** (GV.RM-03)

RIZ-013: Procjena rizika zbog neprimjenjivanja sigurnosnih zakrpa

Kontrola osigurava procjenu rizika povezanih s neprimjenjivanjem sigurnosnih zakrpa, uključujući analizu kritičnosti i izloženosti sustava, ozbiljnosti otkrivenih ranjivosti te trenutnog stanja kibernetičke sigurnosti. Subjekt mora dokumentirati razloge za neprimjenjivanje zakrpa i definirati dodatne mjere za ublažavanje rizika, kao što su izolacija sustava i implementacija privremenih sigurnosnih pravila.

Navedena procjena rizika nije sastavni dio godišnje procjene rizika ili registara identificiranih rizika, već predstavlja kratku i ciljanu aktivnost procjene potencijalnih negativnih učinaka zbog ne primjene sigurnosnih zakrpa koja se može dokumentirati kroz redovne zapise koji nastaju u procesu upravljanja ranjivostima.

Provjera uključuje analizu dokumentacije o procjeni rizika, pregled definiranih mjera za ublažavanje rizika i konzultacije s odgovornim osobama za upravljanje sigurnosnim procedurama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Razlozi za neprimjenu zakrpa nisu identificirani, a pripadajući rizici nisu procijenjeni niti dokumentirani.
2	Postoje jasni iskustveni ili slični razlozi za neprimjenu pojedinih zakrpa te postoji djelomična, ne nužno dokumentirana procjena rizika, ali nedostaju mjere za ublažavanje.
3	Razlozi za neprimjenu pojedinih zakrpa su dokumentirani, a rizici procijenjeni te definiraju osnovne mjere za ublažavanje potencijalnih negativnih učinaka.
4	Uspostavljen je sustavni proces provjere, testiranja i planske primjene sigurnosnih zakrpa što uključuje i procjenu rizika od ne primjene istih te definiranje mjera za ublažavanje.
5	Uspostavljen je sustavni proces koji osigurava naknadnu identifikaciju i implementaciju eventualno neprimijenjenih zakrpa te ranjivosti sustava.

Reference:

- **ISO/IEC 27001:2022** (A.8.8)
- **NIST SP 800-53 Rev. 5** (SI-2, RA-5, CM-3)
- **CIS v8** (2.2)

RIZ-014: Pravila sigurnosti lanca opskrbe

Ova kontrola osigurava razvoj, dokumentiranje, održavanje i implementaciju pravila sigurnosti lanca opskrbe. Pravila trebaju definirati minimalne sigurnosne zahtjeve za različite vrste izravnih dobavljača i pružatelja usluga, uključujući specifične zahtjeve za opskrbu IKT proizvodima, sustavima i uslugama. Proces provjere sigurnosti dobavljača uključuje procjenu rizika, definiranje odgovornosti i ovlasti te redovite provjere usklađenosti s utvrđenim pravilima. Pravila trebaju biti prilagođena specifičnim vrstama dobavljača, kao što su dobavljači komercijalne opreme, dobavljači softvera po narudžbi, pružatelji usluga računalstva u oblaku ili održavanja sustava.

Provjera uključuje pregled dokumentacije pravila sigurnosti lanca opskrbe, specifičnih pravila za različite vrste dobavljača, analizu procesa provjere dobavljača i pružatelje usluga, evidenciju o provedenim procjenama i konzultacije s odgovornim osobljem kako bi se osigurala dosljedna primjena pravila.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Pravila sigurnosti lanca opskrbe nisu definirana.
2	Pravila sigurnosti lanca opskrbe su djelomično definirana, ne obuhvaćaju sve vrste izravnih dobavljača, ali se ne primjenjuju.
3	Pravila sigurnosti lanca opskrbe su definirana, dokumentirana, obuhvaćaju sve izravne dobavljače, ali nisu dosljedno implementirana niti ažurirana.
4	Sveobuhvatna pravila sigurnosti lanca opskrbe su definirana, dokumentirana i primijenjena za sve izravne dobavljače i pružatelje usluga ovisno o kategoriji.
5	Sveobuhvatna pravila sigurnosti lanca opskrbe su definirana, dokumentirana, primijenjena za sve izravne dobavljače i pružatelje usluga ovisno o kategoriji, redovito su ažurirana i uključuju kontinuiranu provjeru dobavljača i pružatelja usluga uz redovne provjere usklađenosti.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20, A.5.21)
- **ISO/IEC 27002:2022** (5.19, 5.20, 5.21)
- **ISO 22301:2019** (8.1)
- **NIST SP 800-53 Rev. 5** (SR-3, SR-5, SA-9)
- **CIS v8** (15.2, 15.3, 15.4)

RIZ-015: Identifikacija i registar izravnih dobavljača i pružatelja usluga

Ova kontrola osigurava identifikaciju svih izravnih dobavljača i pružatelja usluga, uključujući one povezane s IKT uslugama, sustavima ili proizvodima. Kontrola također obuhvaća uspostavu i održavanje ažuriranog registra dobavljača koji uključuje relevantne informacije kao što su kontaktne točke, popis usluga, sustava ili proizvoda koje subjekt izravno nabavlja te status procjene rizika za svakog dobavljača.

Provjera revizora obuhvaća pregled dokumentacije o identifikaciji, analizu ažuriranosti registra i postupaka za ažuriranje procjena, provjeru informacija o pristupu kritičnoj imovini te konzultacije s odgovornim osobljem za upravljanje lancem opskrbe i sigurnosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Izravni dobavljači nisu identificirani.
2	Postoji popis izravnih dobavljača, ali nije dokumentiran u formi registra.
3	Postoji registar izravnih dobavljača, ali nije potpun niti se ažurira.
4	Postoji registar izravnih dobavljača i redovito se ažurira.
5	Postoji registar izravnih dobavljača i redovito se ažurira te je potpuno implementiran u proces upravljanja lancem opskrbe i integriran s procesom procjene rizika.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20, A.5.21, A.5.22)
- **ISO/IEC 27002:2022** (5.19, 5.20, 5.21, 5.22)
- **ISO 22301:2019** (8.1)
- **NIST SP 800-53 Rev. 5** (SR-3, SR-6, SA-9, RA-3)
- **NIST CSF v2.0** (ID.RA-10)
- **CIS v8** (Kontrola 15)

RIZ-016: Sigurnosni zahtjevi u ugovorima sa izravnim dobavljačima ili pružateljima usluga

Kontrola osigurava definiranje i implementaciju sigurnosnih zahtjeva u ugovorima o poslovnoj suradnji odnosno o nabavi i pružanju usluga s izravnim dobavljačima i pružateljima usluga. Sigurnosni zahtjevi trebaju uključivati sigurnosne klauzule poput povjerljivosti podataka, ugovaranje pružanja upravljanih usluga ili upravljanih sigurnosnih usluga sa ključnim ili važnim subjektima, obveze obavještavanja o incidentima koji mogu utjecati na subjekta , odredbu o pravu zahtijevanja provedbe revizije kibernetičke sigurnosti ili pravu na dokaz o provedenoj reviziji, upravljanje ranjivostima, ili certifikate te zahtjeve o mogućem podugovaranju i sigurnosnim zahtjevima za podugovaratelje kao i odredbe o obvezama izravnog dobavljača ili pružatelja usluga pri isteku ili raskidu ugovornog odnosa (npr. postupanje sa podacima). Sigurnosni zahtjevi mogu uključivati odredbe o osposobljavanju ili certifikatima.

Provjera usklađenosti obuhvaća pregled ugovora i analizu ugovorenih sigurnosnih zahtjeva, provjeru evidencija o prijavljenim incidentima od strane dobavljača i upravljanju ranjivostima te konzultacije s odgovornim osobljem za ugovorne odnose i sigurnost. Ukoliko subjekt ugovara standardnu uslugu za koju je nemoguće mijenjati uvjete korištenja ili SLA, u postupku revizije taj preostali rizik to mora odražavati te može biti prihvaćen.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurnosni zahtjevi nisu definirani u ugovorima sa izravnim dobavljačima ili pružateljima usluga.
2	Osnovni sigurnosni zahtjevi su definirani u ugovorima sa izravnim dobavljačima ili pružateljima usluga, ali nisu primijenjeni sukladno ugovoru ili nisu primijenjeni na sve izravne dobavljače ili pružatelje usluga.
3	Osnovni sigurnosni zahtjevi su definirani u ugovorima sa izravnim dobavljačima ili pružateljima usluga, ali su djelomično primijenjeni na pojedine izravne dobavljače ili pružatelje usluga ili samo djelomično u dijelu ugovorenih sigurnosnih zahtjeva.
4	Osnovni sigurnosni zahtjevi su definirani u ugovorima sa izravnim dobavljačima ili pružateljima usluga i u cijelosti su primijenjeni na sve izravne dobavljače ili pružatelje usluga i u skladu sa ugovorenim sigurnosnim zahtjevima.
5	Osnovni sigurnosni zahtjevi su definirani u ugovorima sa izravnim dobavljačima ili pružateljima usluga i u cijelosti su primijenjeni na sve izravne dobavljače ili pružatelje usluga te u skladu sa ugovorenim sigurnosnim zahtjevima. Ugovoreni sigurnosni zahtjevi se provjeravaju i prema potrebi ažuriraju.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20, A.5.21)

- **ISO/IEC 27002:2022** (5.19, 5.20, 5.21)
- **ISO 22301:2019** (8.1)
- **NIST SP 800-53 Rev. 5** (SR-3, SR-6, SA-9, RA-3)
- **CIS v8** (15.2, 15.4)

RIZ-017: Redoviti nadzor i revizija sigurnosti ključnih lanca opskrbe IKT uslugama, sustavima ili proizvodima

Ova kontrola osigurava redoviti nadzor, reviziju, evaluaciju i poboljšanje sigurnosti lanaca opskrbe IKT uslugama, sustavima ili proizvodima. Revizija se provodi pri svakom novom ugovaranju, najmanje svake dvije godine, nakon incidenata povezanog s predmetnom uslugom ili značajnih promjena u sigurnosnim zahtjevima ili stanju kibernetičke sigurnosti. Proces uključuje provjeru svih ugovorenih sigurnosnih zahtjeva, identifikaciju odstupanja, analizu odstupanja kroz provođenje procjene rizika radi pravovremenog otklanjanja nedostataka, a potrebne mjere poduzeti kako bi se osigurala usklađenost s ugovorenim sigurnosnim zahtjevima. Kontrola sigurnosnih zahtjeva trebala bi obuhvatiti sve ugovorima definirane sigurnosne zahtjeve.

Provjera uključuje pregled dokumentacije o provedenim revizijama, evidencije o identificiranim odstupanjima, zapise o provedenim procjenama rizika i konzultacije s odgovornim osobljem za upravljanje i sigurnost lanca opskrbe.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Redoviti nadzor i revizija sigurnosti ključnih lanca opskrbe nisu uspostavljeni.
2	Revizije i nadzor se provode neredovito ili nisu dokumentirane.
3	Revizije i nadzor se provode redovito, ali ne uključuju provjeru svih sigurnosnih zahtjeva niti procjenu rizika.
4	Revizije i nadzor se provode redovito i uključuju provjeru svih sigurnosnih zahtjeva uz djelomičnu procjenu rizika.
5	Revizije i nadzor se provode redovito i uključuju provjeru svih sigurnosnih zahtjeva i potpuno su integrirani s procesima upravljanja rizicima.

Reference:

- **ISO/IEC 27001:2022** (9, A. 5.19, A.5.21, A.5.22)
- **ISO/IEC 27002:2022** (5.19, 5.21, 5.22)
- **ISO 22301:2019** (8.1, 9)
- **NIST SP 800-53 Rev. 5** (SR-3, SR-4, SR-6, CA-7)
- **CIS v8** (15.5, 15.6)

RIZ-018: Kriteriji i sigurnosni zahtjevi za odabir dobavljača i pružatelja usluga

Ova kontrola osigurava definiranje i primjenu kriterija i sigurnosnih zahtjeva za odabir i ugovaranje izravnih dobavljača i pružatelja usluga, s naglaskom na ključne dobavljače u lancu opskrbe IKT uslugama, sustavima ili proizvodima. Kriteriji uključuju sposobnost dobavljača da provede sigurnosne zahtjeve subjekta, razinu rizika, razinu kritičnost IKT usluga, sustava ili proizvoda te toleranciju rizika. Kontrola također uključuje redovitu procjenu i ažuriranje kriterija sukladno promjenama u sigurnosnim potrebama i rizicima uz diversifikaciju izvora opskrbe kako bi se smanjila ovisnost o pojedinom dobavljaču. Za procjenu rizika uzimaju se u obzir koordinirane procjena rizika od relevantnih europskih tijela.

Provjera uključuje pregled i analizu dokumentacije o kriterijima i sigurnosnim zahtjevima za odabir dobavljača, pregled i analizu ugovora o suradnji s dobavljačima, procjenu rizika povezanih s dobavljačima te konzultacije s odgovornim osobljem za sigurnost i nabavu.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Kriteriji i sigurnosni zahtjevi za odabir dobavljača nisu definirani.
2	Osnovni kriteriji postoje, ali nisu sveobuhvatni niti redovito ažurirani.
3	Kriteriji i sigurnosni zahtjevi su definirani i primjenjuju se za neke dobavljače, ali bez detaljne procjene rizika.
4	Sveobuhvatni kriteriji su definirani, dokumentirani, uključuju procjenu rizika i redovito se ažuriraju i primjenjuju za sve ključne dobavljače.
5	Kriteriji su potpuno integrirani s procesima upravljanja rizicima i uključuju kontinuirano praćenje i evaluaciju dobavljača.

Reference:

- **ISO/IEC 27001:2022** (A.5.19, A.5.20)
- **ISO/IEC 27002:2022** (5.19, 5.20)
- **ISO 22301:2019** (8.1)
- **NIST SP 800-53 Rev. 5** (SR-5, SR-6, RA-3)
- **CIS v8** (15.2, 15.5)

RIZ-019: Procjena rizika geografske lokacije

Ova kontrola osigurava da subjekt uzme u obzir rizike povezane s fizičkom lokacijom svojih informacijskih resursa, uključujući podatkovne centre, komunikacijsku infrastrukturu i druge ključne točke. Geografski rizici, poput onih vezanih uz seizmičku aktivnost, poplave ili druge prirodne prijetnje, mogu imati ozbiljan utjecaj na raspoloživost i pouzdanost sustava. Dokumentiranom procjenom rizika temeljenom na relevantnim podacima (npr. potresne zone, podaci o poplavama i sl.), omogućuje se planiranje zaštitnih mjera, pravovremena reakcija i donošenje informiranih odluka o lokaciji infrastrukture, čime se povećava ukupna otpornost sustava na fizičke prijetnje.

Provjerava se postoji li dokumentirana procjena rizika geografske lokacije koja koristi dostupne podatke, primjerice seizmičke karte, povijesne podatke o poplavama, požarima i drugim relevantnim prijetnjama za područje na kojem se nalazi ključna infrastruktura. Dodatno se analizira je li procjena provedena sustavno te u kojoj je mjeri uključena u širu procjenu rizika i planove kontinuiteta poslovanja. Naglasak je na dokumentiranju izvora podataka, identificiranih prijetnji i načinu na koji su ti podaci korišteni za donošenje zaključaka o riziku. Ukoliko je trošak redundantnog podatkovnog centra veći od mogućih gubitaka u slučaju njegova korištenja osobe odgovorne za upravljanje mjerama mogu sukladno procesu upravljanja rizicima prihvatiti rizik – koji onda mora biti adekvatno dokumentiran.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Rizici geografske lokacije nisu razmatrani; ne postoji nikakva dokumentacija ili analiza.
2	Rizici su usmeno prepoznati, ali ne postoji formalna dokumentacija ni korištenje konkretnih izvora podataka.
3	Postoji osnovna dokumentirana procjena, ali se ne temelji na pouzdanim podacima (npr. korišteni su opći opisi).
4	Procjena je dokumentirana i temelji se na relevantnim izvorima podataka, ali nije uključena u druge sigurnosne procese.
5	Procjena je dokumentirana, koristi konkretne podatke (npr. seizmičke karte), redovito se ažurira i integrirana je u sveobuhvatno upravljanje rizicima i kontinuitet poslovanja.

Reference:

- **ISO/IEC 27001:2022** (A.7.5)
- **ISO/IEC 27002:2022** (7.5)
- **NIST SP 800-53 Rev. 5** (CP-2, PM-9)

DID-001: Uspostava i upravljanje jedinstvenim digitalnim identitetima

Ova kontrola zahtijeva uspostavu sustava za kreiranje i upravljanje jedinstvenim digitalnim identitetima za sve korisnike mrežnih i informacijskih sustava. Digitalni identiteti moraju biti povezani s jedinstvenim osobama kako bi se osigurala odgovornost za aktivnosti provedene s tim identitetima. Subjekt mora:

- Osigurati da svaki korisnik posjeduje jedinstven digitalni identitet, gdje je tehnički moguće.
- Voditi evidencije o korisnicima i njihovim digitalnim identitetima.

Provjera uključuje pregled dokumentacije sustava digitalnih identiteta, uključujući evidencije o korisnicima i promjenama identiteta. Također se evaluira sustav praćenja i nadzora kako bi se osiguralo da su svi identiteti jedinstveni i povezani s odgovarajućim korisnicima. Procjenjuje se redovitost provođenja revizija i uklanjanja nepotrebnih identiteta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za upravljanje digitalnim identitetima nije uspostavljen.
2	Jedinstveni digitalni identiteti su kreirani, ali evidencija nije dosljedna.
3	Sustav postoji i djelomično prati promjene u identitetima.
4	Sustav u potpunosti prati, dokumentira i nadzire sve promjene.
5	Sustav je optimiziran i integriran u širi sustav upravljanja rizicima, te se provjeravaju mehanizmi automatizacije upravljanja identitetima.

Reference:

- **ISO/IEC 27001:2022** (A.5.16)
- **ISO/IEC 27002:2022** (5.16)
- **NIST SP 800-53 Rev. 5** (IA-2, IA-4, AC-2)
- **NIST CSF v2.0** (PR.AA-01)
- **CIS v8** (5.1, 5.3)

DID-002: Uvođenje kompenzacijskih mjera za dijeljene digitalne identitete

Ova kontrola zahtijeva dokumentaciju i implementaciju kompenzacijskih mjera za korištenje dijeljenih digitalnih identiteta. Subjekt mora:

- Definirati uvjete pod kojima su dijeljeni identiteti dopušteni.
- Voditi evidenciju o korisnicima dijeljenih identiteta, uključujući vrijeme korištenja.
- Uspostaviti mehanizme za praćenje aktivnosti i osigurati odgovornost.

Provjera uključuje pregled dokumentacije koja definira uvjete za korištenje dijeljenih identiteta, kao i zapisa aktivnosti povezanih s njima. Procjenjuje se učinkovitost kompenzacijskih mjera i sustava praćenja te provjerava evidencije o odobrenjima i korištenju dijeljenih identiteta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Kompenzacijske mjere za dijeljene identitete nisu uspostavljene.
2	Definirani su uvjeti, ali implementacija je nepotpuna.
3	Kompenzacijske mjere su dokumentirane i djelomično implementirane.
4	Sustav za praćenje dijeljenih identiteta u potpunosti je operativan.
5	Sustav je optimiziran i evaluiran prema sigurnosnim standardima.

Reference:

- **ISO/IEC 27001:2022** (A.5.17)
- **ISO/IEC 27002:2022** (5.17)
- **NIST SP 800-53 Rev. 5** (IA-2, AC-2)
- **CIS v8** (5.1)

DID-003: Pravovremena promjena i ukidanje digitalnih identiteta

Ova kontrola osigurava pravovremenu promjenu i ukidanje digitalnih identiteta korisnika mrežnih i informacijskih sustava u skladu s organizacijskim i poslovnim promjenama. Sustav upravljanja identitetima mora omogućiti promptno ukidanje identiteta koji više nisu potrebni, uz detaljnu dokumentaciju svih promjena u pravima pristupa. Redovita revizija prava pristupa osigurava prilagodbu trenutnim potrebama subjekta, smanjuje rizik od neovlaštenog pristupa i doprinosi zaštiti kritičnih podataka.

Provjera kontrole uključuje pregled dokumentacije procesa upravljanja digitalnim identitetima, uključujući evidencije o dodjeli, promjeni i ukidanju prava pristupa. Evaluacija obuhvaća analizu pravovremenosti provedenih promjena i procjenu njihove usklađenosti s internim politikama i poslovnim potrebama, uz konzultacije s odgovornim osobama kako bi se potvrdila dosljedna primjena procesa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za promjenu i ukidanje identiteta nije implementiran.
2	Sustav postoji, ali ne osigurava pravovremenu promjenu ili ukidanje.
3	Sustav djelomično osigurava pravovremene promjene i evidencije.
4	Sustav redovito prati, dokumentira i ukida nepotrebne identitete.
5	Sustav je optimiziran i potpuno integriran s poslovnim procesima.

Reference:

- **ISO/IEC 27001:2022** (A.5.16, A.5.18)
- **ISO/IEC 27002:2022** (5.16, 5.18)
- **NIST SP 800-53 Rev. 5** (AC-2, PS-4)
- **CIS v8** (5.3, 6.2)

DID-004: Integracija sustava za upravljanje ljudskim potencijalima i digitalnim identitetima

Ova kontrola zahtijeva integraciju sustava za upravljanje ljudskim potencijalima sa sustavima za upravljanje digitalnim identitetima i pravima pristupa mrežnom i informacijskom sustavu. Cilj je osigurati pravovremenu dodjelu i ukidanje prava pristupa temeljem sigurnosnih načela poput „poslovne potrebe," „najmanje privilegije" i „razdvajanja nadležnosti." Prava pristupa trebaju biti prilagođena potrebama korisnika i trećih strana, uz ograničenje opsega i trajanja ovlasti.

Evidencija aktivnosti mora uključivati registar dodijeljenih prava po korisnicima, evidentiranje promjena i korištenje zapisa o pristupu. Pregled uključuje analizu integracije sustava, procjenu točnosti i pravovremenosti upravljanja pravima te provjeru pridržavanja sigurnosnih načela u upravljanju pravima pristupa.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za upravljanje digitalnim identitetima nije integriran sa sustavom upravljanja ljudskim potencijalom.
2	Djelomična integracija, ali bez pravovremenog ažuriranja prava pristupa.
3	Sustavi su integrirani, ali nije usklađen sa sigurnosnim načelima.
4	Sustavi su integrirani, usklađeni s sigurnosnim načelima, uz nedosljednosti u evidencijama.
5	Sustavi su integrirani, prava pristupa su ažurirana i evidentirana.

Reference:

- **ISO/IEC 27001:2022** (A.5.16)
- **ISO/IEC 27002:2022** (5.16)
- **NIST SP 800-53 Rev. 5** (AC-2, PS-4, IA-4)
- **CIS v8** (5.6, 6.1, 6.2)

DID-005: Upravljanje pravima pristupa trećih strana

Ova kontrola zahtijeva specifične mjere za upravljanje pravima pristupa trećih strana, uključujući dobavljače i pružatelje usluga. Prava pristupa trebaju biti ograničena po opsegu i trajanju te dokumentirana u skladu s načelima „poslovne potrebe“ i „najmanje privilegije“.

Evaluacija uključuje pregled ugovora, evidencije dodijeljenih prava i revizije aktivnosti trećih strana kako bi se osigurala usklađenost sa sigurnosnim politikama subjekta.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Upravljanje pravima trećih strana nije implementirano.
2	Postoje osnovna pravila za upravljanje pristupom trećih strana, ali njihova primjena nije dosljedna. Ugovori rijetko uključuju sigurnosne zahtjeve za pristup, a prava se često dodjeljuju na neodređeno vrijeme.
3	Subjekt ima uspostavljene kontrole za upravljanje pristupom trećih strana. Prava pristupa se dodjeljuju temeljem poslovne potrebe, a dokumentiraju se u centraliziranoj evidenciji. Pristupi su vremenski ograničeni, ali se ponekad produljuju bez ažurirane procjene.
4	Prava pristupa trećih strana su strogo ograničena, dokumentirana i vremenski definirana. Dodjela prava temelji se na načelima „najmanje privilegije“ i „need-to-know“, a svi zahtjevi za pristup prolaze kroz formalno odobravanje. Pristupi se redovito revidiraju. Sustav revizije omogućava brzo ukidanje pristupa pri završetku poslovnog odnosa ili promjeni ugovora.
5	Subjekt ima potpuno automatiziran sustav za upravljanje pravima pristupa trećih strana, koji je integriran s ugovornim, tehničkim i sigurnosnim sustavima. Svi pristupi su kontekstualno kontrolirani, vremenski ograničeni i automatski deaktivirani nakon isteka ugovora ili završetka zadatka. Sustav podržava izvještavanje i automatsko generiranje upozorenja o odstupanjima.

Reference:

- **ISO/IEC 27001:2022** (A.5.20, A.8.2, A.8.3, A.8.5)
- **ISO/IEC 27002:2022** (5.20, 8.2, 8.3, 8.5)
- **ISO 22301:2019** (8.1)
- **NIST SP 800-53 Rev. 5** (AC-2, AC-3, AC-6)
- **NIST CSF v2.0** (PR.AA-01)
- **CIS v8** (6.1, 6.2, 6.6, 6.8)

DID-006: Nadzor i revizija aktivnosti korisnika sustava

Ova kontrola zahtijeva implementaciju sustava za evidentiranje aktivnosti korisnika mrežnog i informacijskog sustava. Svi sustavi moraju biti u mogućnosti evidentirati vrijeme i korisnika koji je sustavu pristupao te ukoliko je moguće lokaciju pristupa. U slučaju sustava u oblaku subjekt treba imati adekvatna prava da može vidjeti pripadne dnevničke zapise ili iste prebaciti u svoj sustav.

Provjerava se prikupljanje zapisa o vremenu i lokaciji (geografska lokacija, IP adresa ili nešto drugo) pristupa korisnika s pripadajućim identifikatorima korisnika (korisničko ime, ID, uloga i ostali), te zapisi o aktivnostima tokom aktivnih sesija. Ukoliko subjekt koristi rješenja u oblaku, također se provjerava može li subjekt pristupiti pripadajućim dnevničkim zapisima – te je li moguć pristup samo osnovnim podacima ili i detaljnim aktivnostima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt ne posjeduje mogućnosti uvida u zapise pristupa.
2	Subjekt posjeduje mogućnosti uvida u zapise pristupa samo za neke sustave.
3	Zapisi o pristupu na sve sustave postoje i sadržavaju dovoljne informacije za eventualnu analizu uslijed sigurnosnog incidenta.
4	Subjekt ima pohranjene zapise o pristupu sustavima te posjeduje znanje za analizu istih za slučaj sigurnosnog incidenta.
5	Subjekt koristi zapise o pristupu njemu kritičnom sustavu za analizu i automatsko prepoznavanje mogućih napada.

Reference:

- **ISO/IEC 27001:2022** (A.5.28, A.8.15, A.8.16)
- **ISO/IEC 27002:2022** (5.28, 8.15, 8.16)
- **NIST SP 800-53 Rev. 5** (AC-2, AC-7, AU-2, AU-6, AU-12)
- **NIST CSF v2.0** (DE.AE-02)
- **CIS v8** (8.1, 8.2, 8.5, 8.11)

DID-007: Višefaktorska autentifikacija (MFA)

Ova kontrola osigurava implementaciju višefaktorske autentifikacije (MFA – *Multi-Factor Authentication*) za kritične mrežne i informacijske sustave koji su više izloženi potencijalnim kibernetičkim napadima. MFA kombinira više faktora autentifikacije, poput nečega što korisnik zna (lozinka ili PIN), nečega što korisnik posjeduje (token ili pametni telefon) i nečega što korisnik jest (biometrija poput otiska prsta ili prepoznavanja lica). Poseban naglasak stavlja se na primjenu MFA za privilegirane korisničke račune, administrativne pristupe te sustave s kritičnim podacima. Kontrola također uključuje edukaciju korisnika o pravilnoj uporabi MFA metoda te provođenje sigurnosnih mjera za zaštitu faktora autentifikacije od kompromitacije.

Provjera usklađenosti obuhvaća analizu dokumentacije o MFA konfiguraciji, testiranje funkcionalnosti autentifikacijskih metoda te konzultacije s osobljem odgovornim za njihovu implementaciju kako bi se potvrdila učinkovitost i dosljednost provedbe.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Višefaktorska autentifikacija (MFA) nije nigdje implementirana.
2	MFA je implementirana sporadično na određenim sustavima bez jasnih pravila te postoje mnogi izuzeti korisnici.
3	MFA je implementirana na kritičnim sustavima i za većinu privilegiranih korisničkih računa, ali postoje izuzetci.
4	MFA je implementirana na svim kritičnim sustavim i privilegiranim korisničkim računima.
5	MFA je implementirana na svim kritičnim sustavima i za sve korisničke račune te postoje mehanizmi za detekciju i otkrivanje izuzetaka.

Reference:

- **ISO/IEC 27001:2022** (A.8.5)
- **ISO/IEC 27002:2022** (8.5)
- **NIST SP 800-53 Rev. 5** (IA-2, IA-5)
- **CIS v8** (6.3, 6.4, 6.5)

DID-008: Autorizacija korištenja mrežnih resursa

Kontrolom se osigurava da samo ovlašteni korisnici ili uređaji mogu pristupiti mrežnim resursima. Autorizacija se temelji na provjerenim digitalnim identitetima, a u slučajevima kada to nije moguće, koristi se fizička lokacija za kontrolu pristupa.

Usklađenost ove kontrole provodi se pregledom pripadnih politika, analizom evidencija o pristupima mreži i testiranjem mehanizama autorizacije kako bi se osigurala primjena pravila za ovlašteni pristup.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Autorizacija korištenja mrežnih resursa nije implementirana
2	Autorizacija je implementirana isključivo kontrolom pristupa fizičkoj lokaciji.
3	Autorizacija je implementirana provjerom digitalnih identiteta korisnika ili uređaja.
4	Autorizacija je implementirana provjerom digitalnih identiteta korisnika i uređaja.
5	Autorizacija je implementirana provjerom digitalnih identiteta korisnika i pristupnog uređaja te potpuno integrirana s naprednim provjerama kao što je geografska lokacija ili rizično ponašanje korisnika.

Reference:

- **ISO/IEC 27001:2022** (A.7.1, A.8.2, A.8.3)
- **ISO/IEC 27002:2022** (7.1, 8.2, 8.3)
- **NIST SP 800-53 Rev. 5** (AC-2, AC-3)
- **CIS v8** (6.1)

DID-009: Vlasništvo nad ulogama i odobravanje prava pristupa

Ova kontrola osigurava da su definirane uloge vlasnika aplikacija odnosno korisnika s privilegiranim pravima pristupa, a koji su odgovorni za odobravanje korisničkih prava. Svaka uloga mora imati pridruženog vlasnika koji odobrava dodjelu prava, a svi postupci dodjele, izmjene i ukidanja prava moraju biti dokumentirani. Subjekt mora voditi evidenciju o tome tko je odobrio prava i osigurati usklađenost svih postupaka s politikom kontrole pristupa.

Usklađenost ove kontrole provodi se pregledom dokumentacije o ulogama i odgovornostima vlasnika, analizom zapisa o dodjeli prava te konzultacijom s odgovornim osobljem za upravljanje korisničkim pravima i digitalnim identitetima.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Uloge vlasnika nisu definirane, a proces dodjele prava nije dokumentiran.
2	Uloge vlasnika su djelomično definirane, dokumentacija je nepotpuna.
3	Uloge vlasnika su definirane i dokumentirane, ali postupci nisu dosljedni.
4	Sve uloge vlasnika i postupci dodjele prava su jasno definirani i dokumentirani.
5	Uloge vlasnika su potpuno integrirane s procesima kontrole pristupa.

Reference:

- **ISO/IEC 27001:2022** (A.8.2)
- **NIST SP 800-53 Rev. 5** (AC-2)

DID-010: Upravljanje i politike korištenja privilegiranih računa

Ova kontrola osigurava definiranje, implementaciju i nadzor politika za upravljanje privilegiranim korisničkim računima i administratorskim pravima. Pravila moraju uključivati kreiranje specifičnih administratorskih računa, individualizaciju i ograničavanje administratorskih privilegija, primjenu snažne provjere autentičnosti (primjerice metoda višefaktorske autentifikacije) te ograničenje korištenja privilegiranih računa isključivo za administraciju sustava.

Provjera usklađenosti uključuje pregled dokumentacije o politikama i procedurama za upravljanje privilegiranim računima, analizu zapisa o korištenju privilegiranih računa, provjeru implementacije snažne provjere autentičnosti te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala dosljedna primjena pravila.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Privilegirani računi koriste se bez nadzora, često su dijeljeni među više korisnika i nemaju tehnička ograničenja u pogledu svrhe korištenja. Ne postoji formalno definirana politika za upravljanje privilegiranim računima.
2	Postoji osnovna politika upravljanja privilegiranim računima, ali nije obvezujuća niti se sustavno provodi. Neki računi su individualizirani, no i dalje se koriste generički ili zajednički privilegirani pristupi.
3	Subjekt ima dokumentiranu politiku za upravljanje privilegiranim računima koja uključuje individualizaciju korisničkih identiteta, ograničenje pristupa prema poslovnim potrebama te osnovnu implementaciju višefaktorske autentifikacije. Privilegirani računi se koriste isključivo za svrhe administracije, a pristup se bilježi kroz dnevničke zapise. Postoje periodične revizije korištenja privilegiranih računa.
4	Politike za upravljanje privilegiranim računima su jasno definirane, primijenjene i redovito nadzirane. Svi privilegirani računi su individualizirani, vremenski ograničeni i tehnički ograničeni na zadatke administracije. Djelovanje privilegiranih korisnika se bilježi i nadzire kroz sustav evidencije. Revizije se provode na redovnoj osnovi, a rezultati se koriste za ažuriranje pristupnih prava i politika.
5	Pravila su potpuno integrirana s automatiziranim nadzorom, uključuju snažnu sustavnu provjeru autentičnosti i redovitu reviziju aktivnosti.

Reference:

- **ISO/IEC 27001:2022** (A.8.2)
- **ISO/IEC 27002:2022** (8.2)
- **NIST SP 800-53 Rev. 5** (AC-6)
- **CIS v8** (5.4, 6.5, 6.8)

DID-011: Dinamička kontrola pristupa temeljena na riziku

Ova kontrola osigurava implementaciju dinamičke kontrole pristupa koja se prilagođava procjeni rizika u stvarnom vremenu. Prilikom provjere autentičnosti i autorizacije, sustav analizira čimbenike kao što su lokacija korisnika, uređaj, vrijeme pristupa i obrasci aktivnosti te dinamički određuje razinu pristupa ili zahtijeva dodatne korake provjere autentičnosti.

Provjera uključuje pregled konfiguracija sustava za dinamičku kontrolu pristupa, analizu pravila za procjenu rizika, testiranje scenarija dinamičkog pristupa te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala pravilna implementacija i prilagodba sigurnosnih mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Dinamička kontrola pristupa nije implementirana.
2	Implementirana je osnovna dinamička kontrola, ali se ne temelji na procjeni rizika.
3	Dinamička kontrola pristupa se temelji na nekoliko čimbenika rizika, ali nije dosljedno primjenjiva.
4	Dinamička kontrola pristupa je implementirana s redovitom procjenom rizika.
5	Napredna dinamička kontrola pristupa potpuno integrirana s procjenom rizika u stvarnom vremenu.

Reference:

- **ISO 27001:2022** (6.1, A.5.15, A.5.18)
- **NIST SP 800-53 Rev. 5** (AC-2)
- **CIS v8** (10.7)

SKM-001: Primjena EPP/EDR rješenja

Kontrola osigurava implementaciju alata za otkrivanje i odgovor na prijetnje na krajnjim točkama (EPP/EDR) u skladu s procjenom rizika i tehničkim mogućnostima sustava. Alati trebaju omogućiti detekciju, analizu i automatski odgovor na kibernetičke prijetnje u stvarnom vremenu. Poseban naglasak stavlja se na postavljanje prikladne razine automatizacije odgovora, edukaciju osoblja za upravljanje EPP/EDR alatima te integraciju tih alata s ostalim sigurnosnim sustavima subjekta.

Provjera usklađenosti uključuje analizu postavljenih EPP/EDR sustava, dokumentaciju o njihovoj konfiguraciji, pregled evidencija o detektiranim prijetnjama i reakcijama te evaluaciju učinkovitosti alata kroz simulacije napada i testiranja.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	EPP/EDR rješenja nisu implementirana.
2	EPP/EDR rješenja su implementirana na ograničenom broju krajnjih točaka bez prilagodbe te bez uspostavljenog procesa nadzora, trijaže i odgovora.
3	EPP/EDR rješenja su implementirana na kritičnim krajnjim točkama te postoji mehanizam obavještavanja u slučaju sigurnosnih događaja na krajnjim točkama ili ukoliko EPP/EDR rješenja nisu implementirana na svim kritičnim krajnjim točkama, one točke na kojima nisu implementirana moraju biti logički izolirane.
4	EPP/EDR rješenja su implementirana na svim relevantnim krajnjim točkama te je uspostavljen osnovni proces, nadzora, trijaže i odgovara na sigurnosne događaje ili one točke na kojima nisu implementirana EPP/EDR rješenja moraju biti logički izolirane.
5	EPP/EDR rješenja su u potpunosti implementirana na svim relevantnim krajnjim točkama, uspostavljen je proces upravljanja sa sigurnosnim događajima uz primjenu automatizacije integrirani s automatiziranim odgovorima, a ukoliko neke krajnje točke nisu pokrivene EPP/EDR rješenjima iste su logički izolirane od ostalih.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (SI-3, SI-4)
- **NIST CSF v2.0** (Kategorija DE.CM)
- **CIS v8** (13.7, 13.8)

SKM-002: Implementacija osnovnog antivirusnog alata na radnim stanicama i poslužiteljima

Ova kontrola osigurava implementaciju osnovnog antivirusnog alata na svim radnim stanicama i poslužiteljima subjekta kako bi se osigurala osnovna razina zaštite od zlonamjernog softvera. Antivirusni alati moraju uključivati redovito ažuriranje definicija zlonamjernog softvera (ukoliko su temeljeni na definicijama), automatsku detekciju i uklanjanje prijetnji. Subjekt je odgovoran za osiguranje dosljednog upravljanja ovim alatima putem centraliziranog sustava, gdje je to tehnički izvedivo, uključujući redovitu provjeru stanja alata na svim radnim stanicama i poslužiteljima.

Provjera usklađenosti uključuje pregled sustava za upravljanje antivirusnim alatima, dokumentacije ažuriranja definicija zlonamjernog softvera te može uključivati provođenje nasumičnih testova kako bi se osiguralo da alati pravilno funkcioniraju.

Kontrola se primjenjuje na OT sustave ovisno o procjeni rizika implementacije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Antivirusni alat nije implementiran.
2	Antivirusni alat je sporadično implementiran na podskupa radnih stanica i poslužitelja te povremeno ažuriran.
3	Antivirusni alat je uniformno implementiran uz manje objašnjive iznimke, redovito se ažurira, ali nije centralno upravljan.
4	Antivirusni alat je centralno upravljan, a sve iznimke su jasno vidljive i opravdane.
5	Uspostavljen je sustav koji osigurava da se antivirusni alat uniformno implementira na svakom novom računalu te se sva kasnija odstupanja detektiraju i rješavaju u najkraćem mogućem roku.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (SI-3, SI-4)
- **CIS v8** (10.1)

SKM-003: Primjena sigurnosnih zakrpa i upravljanje ranjivostima

Ova kontrola osigurava uspostavu procesa za pravovremenu i cjelovitu primjenu sigurnosnih zakrpa na programskoj i sklopovskoj imovini. Proces uključuje preuzimanje zakrpa iz pouzdanih izvora, njihovo testiranje u kontroliranom okruženju kako bi se osigurala stabilnost sustava te primjenu u skladu s definiranim prioritetima i procedurama. Poseban naglasak stavlja se na procjenu rizika, trijažu i dokumentaciju odluka vezanih uz primjenu sigurnosnih zakrpa. Kontrola također zahtijeva usklađivanje s procedurama za upravljanje promjenama kako bi se osigurala konzistentnost i pouzdanost sustava.

Provjera uključuje pregled dokumentacije o primjeni zakrpa, evidencija o testiranju i preuzimanju zakrpa, analizu razloga za neprimjenjivanje zakrpa te konzultacije s timovima za upravljanje promjenama i sigurnosnim procedurama. Provjera uključuje i analizu alternativnih mjera poduzetih u slučajevima gdje zakrpe nisu primijenjene.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurnosne zakrpe nisu primijenjene niti je uspostavljen proces upravljanja ranjivostima.
2	Sigurnosne zakrpe se primjenjuju povremeno i bez dokumentiranog procesa i testiranja, a razlozi za izuzetke nisu obrazloženi u zapisima procesa.
3	Postoji ustaljeni proces primjene zakrpa koji uključuje osnovnu procjenu rizika i trijažu, ali nedostaju dosljedno testiranje i dokumentacija.
4	Uspostavljen je sustavni proces provjere, testiranja i planske primjene sigurnosnih zakrpa što uključuje jasnu prioritizaciju po informacijskim sustavima te generiranje jasno pisanog traga o provedbi procesa.
5	Uspostavljeni proces upravljanja ranjivostima osigurava i povratni mehanizam provjere te izvještavanje o stupnju ažurnosti sustava a time i mogućnost za unaprjeđenje procesa.

Reference:

- **ISO/IEC 27001:2022** (A.8.8, A.8.19)
- **ISO/IEC 27002:2022** (8.8, 8.19)
- **NIST SP 800-53 Rev. 5** (SI-2)
- **CIS v8** (7.1, 7.2, 7.3, 7.7)

SKM-004: Provjera ranjivosti

Kontrola osigurava provođenje provjera ranjivosti na svim mrežnim i informacijskim sustavima kako bi se identificirale nepravilnosti, poput neprimijenjenih sigurnosnih zakrpa ili nepravilnih konfiguracija. Subjekt mora definirati učestalost provjera na temelju procjene rizika, a rezultati skeniranja trebaju biti prioritetno obrađeni i evidentirani. Poseban naglasak stavlja se na kritičnu imovinu te integraciju rezultata provjera u šire procese upravljanja ranjivostima.

Provjera usklađenosti uključuje pregled rezultata provjera ranjivosti, dokumentacije o učestalosti provjera, analiza postupaka za obradu rezultata te konzultacije s odgovornim timovima za sigurnost.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Provjere ranjivosti se ne provode.
2	Provjere ranjivosti provode se povremeno, ali bez dokumentacije ili analize rezultata.
3	Provjere ranjivosti provode se redovito, ali se rezultati ne koriste za poboljšanje sigurnosti sustava.
4	Provjere ranjivosti provode se redovito, rezultati su dokumentirani i prioritetno obrađeni.
5	Provjere ranjivosti su automatizirane, rezultati se koriste za kontinuirano unaprjeđenje sigurnosti.

Reference:

- **ISO/IEC 27001:2022** (A.8.8)
- **ISO/IEC 27002:2022** (8.8)
- **NIST SP 800-53 Rev. 5** (RA-5)
- **CIS v8** (7.1, 7.5, 7.6)

SKM-005: Sigurnosna testiranja mrežnih i informacijskih sustava

Kontrola osigurava, temeljem procjene rizika, redovita sigurnosna testiranja mrežnih i informacijskih sustava, uključujući penetracijske testove, *red teaming* i druge vrste provjera. Cilj je otkriti ranjivosti u implementaciji i konfiguraciji sustava te koristiti rezultate za unaprjeđenje sigurnosnih politika i praksi. Subjekt je odgovoran za definiranje učestalosti i opsega testiranja na temelju procjene rizika, uz obaveznu dokumentaciju svih rezultata i poduzetih mjera.

Provjera usklađenosti uključuje pregled dokumentacije o sigurnosnim testovima, analizu rezultata testiranja i poduzetih mjera te konzultacije s timovima za sigurnost mrežnih i informacijskih sustava.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurnosno testiranje se ne provodi bez obzira na utvrđenu potrebu.
2	Sukladno procjeni rizika, sigurnosno testiranje provodi se povremeno, ali bez jasnog plana ili prioritizacije rezultata.
3	Subjekt ima plan sigurnosnog testiranja temeljen na procjeni rizika, uključujući penetracijske testove za kritične sustave. Testovi se provode periodično (npr. jednom godišnje), dokumentirani su, a rezultati se analiziraju i koriste za osnovne korektivne mjere.
4	Sigurnosna testiranja su integrirana u sigurnosni plan organizacije, provode se redovito, obuhvaćaju sve kritične sustave i uključuju razne metode (penetracijski testovi, konfiguracijske provjere, testovi fizičkog pristupa itd.). Rezultati su detaljno dokumentirani i povezani s politikama, a sve identificirane ranjivosti imaju planove sanacije.
5	Testiranja su planirana prema kritičnosti sustava i prijetnjama iz *threat intelligencea*, a rezultati se koriste za proaktivno poboljšanje arhitekture, konfiguracija i sigurnosnih politika. Svi rezultati se dokumentiraju, mjere se učinkovitosti sanacije i izvještaji su dostupni upravi. Testiranja su usmjerena na otpornost, a ne samo na sukladnost.

Reference:

- **ISO/IEC 27001:2022** (A.8.8)
- **ISO/IEC 27002:2022** (8.8)
- **NIST SP 800-53 Rev. 5** (RA-5, CA-8)
- **CIS v8** (Kontrola 18)

SKM-006: Upravljanje konfiguracijom mrežnih i informacijskih sustava

Ova kontrola osigurava uspostavu, dokumentiranje, provedbu i kontinuirani nadzor sigurnosnih konfiguracija za mrežne i informacijske sustave. Kontrola uključuje definiranje sigurnosnih konfiguracijskih postavki za svu sklopovsku i programsku imovinu, vanjske usluge i mreže. Također obuhvaća praćenje promjena, reviziju konfiguracija i ažuriranje sigurnosnih postavki tijekom cijelog životnog ciklusa sustava.

Provjera usklađenost uključuje pregled dokumentacije konfiguracijskih postavki, analizu zapisa o promjenama, provjeru procesa nadzora i konzultacije s odgovornim osobljem za upravljanje konfiguracijama.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje definirane sigurnosne konfiguracije. Sustavi se postavljaju prema zadanim (*default*) postavkama, bez sigurnosnog pregleda. Promjene konfiguracija nisu dokumentirane.
2	Postoje djelomične sigurnosne smjernice za konfiguraciju pojedinih sustava (npr. vatrozid, operacijski sustavi), ali nisu obuhvaćene sve vrste ključne imovine. Promjene se ponekad bilježe, ali bez standardiziranog procesa ili revizije. Dokumentacija o konfiguracijama je nepotpuna i neažurirana.
3	Postoje formalno definirane sigurnosne konfiguracije za većinu sustava, uključujući vanjske usluge i mrežne uređaje. Postoji osnovna dokumentacija i sustav za praćenje promjena. Revizija konfiguracija se provodi periodično.
4	Postoji centraliziran proces upravljanja sigurnosnim konfiguracijama, uz dokumentirane standarde za sve vrste imovine i usluga. Svi sustavi imaju definirane sigurne konfiguracije koje se primjenjuju pri inicijalnom postavljanju. Revizije se provode redovito, a postoji i proces eskalacije za neodobrene promjene.
5	Subjekt koristi automatizirane alate za upravljanje sigurnosnim konfiguracijama (SCM) koji su integrirani s procesima promjena, nadzora i otkrivanja ranjivosti. Sve sigurnosne postavke su standardizirane, verzionirane i primjenjive kroz cijeli životni ciklus sustava, uključujući razvoj, test i produkciju. Konfiguracije se kontinuirano nadziru u stvarnom vremenu.

Reference:

- **ISO/IEC 27001:2022** (A.8.9)
- **ISO/IEC 27002:2022** (8.9)
- **NIST SP 800-53 Rev. 5** (CM-2, CM-3, CM-6)
- **CIS v8** (4.1, 4.2, 4.6)

SKM-007: Upravljanje promjenama mrežnih i informacijskih sustava

Ova kontrola osigurava uspostavu, dokumentiranje, provedbu i kontinuirani nadzor procedura za upravljanje promjenama u mrežnim i informacijskim sustavima. Procedure obuhvaćaju planirane i neplanirane promjene, promjene konfiguracija te hitne promjene. Kontrola uključuje definiranje zahtjeva za podnošenje i odobravanje promjena, procjenu rizika povezanih s promjenama, testiranje promjena prije implementacije, provođenje reverznih postupaka (*rollback*) i jasno definiranje odgovornosti. Poseban naglasak stavlja se na osiguranje da su svi relevantni zaposlenici i uključene treće strane upoznati s procedurama i da se one dosljedno primjenjuju.

Provjera uključuje pregled dokumentacije o procedurama za upravljanje promjenama, analizu zapisa o provedenim promjenama, procjenu rizika povezanih s promjenama, pregled postupaka za hitne promjene te konzultacije s odgovornim osobljem za sigurnost i održavanje sustava.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji formalna procedura za upravljanje promjenama. Promjene se provode *ad hoc*, bez odobrenja, procjene rizika ili dokumentacije.
2	Postoje osnovne procedure za neke vrste promjena, ali nisu dokumentirane u cijelosti niti se primjenjuju dosljedno. Promjene se često uvode bez potpune procjene rizika, a hitne promjene se ne razlikuju od redovnih u smislu kontrole. Dokumentacija se vodi djelomično, a odgovornosti nisu jasno definirane.
3	Subjekt ima dokumentirane procedure za upravljanje promjenama, koje uključuju osnovnu klasifikaciju promjena. Većina promjena zahtijeva odobrenje i ima plan provođenja reverznih postupaka. Zaposlenici su upoznati s procedurama, ali se iste ne nadziru. Dokumentacija o provedenim promjenama postoji, ali nije uvijek potpuna.
4	Upravljanje promjenama je sustavno, formalno i redovito primjenjivano. Sve promjene – planirane, hitne i konfiguracijske – prolaze kroz definiran postupak podnošenja, odobravanja, procjene rizika i testiranja. Postoje jasni planovi provođenja reverznih postupaka, standardni obrasci, alati za dokumentiranje i reviziju. Posebna procedura definira uvjete za hitne promjene.
5	Subjekt koristi automatizirani sustav za upravljanje promjenama (poput ITSM alat) u kojem je cijeli proces od zahtjeva do zatvaranja promjene dokumentiran i nadziran. Svaka promjena uključuje automatiziranu procjenu rizika, plan testiranja, plan provođenja reverznih postupaka i praćenje rezultata. Primjena procedura se nadzire u realnom vremenu. Povratne informacije iz prethodnih promjena koriste se za kontinuirano unaprjeđenje procesa.

Reference:

- **ISO/IEC 27001:2022** (A.6.3, A.8.2, A.8.32)
- **ISO/IEC 27002:2022** (8.32)
- **NIST SP 800-53 Rev. 5** (CM-3, CM-4, CM-5, CM-9)
- **CIS v8** (4.1, 4.2)

SKM-008: Blokiranje pristupa iz anonimizacijskih mreža

Kontrola osigurava implementaciju mehanizama za blokiranje pristupa javno dostupnim servisima iz TOR mreža i poznatih anonimizacijskih VPN servisa kako bi se smanjila mogućnost anonimnog napada.

Usklađenost ove kontrole provodi se pregledom konfiguracija mrežnih uređaja i sustava za blokiranje pristupa, analizom ažuriranih popisa TOR čvorova i anonimizacijskih servisa te testiranjem blokiranja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Nema blokiranja pristupa iz anonimizacijskih mreža.
2	Blokiranje je implementirano, ali popisi nisu ažurni.
3	Blokiranje je djelomično provedeno s ažuriranim popisima.
4	Sustavno blokiranje pristupa uz redovito ažuriranje popisa.
5	Napredno blokiranje uz automatiziranu detekciju novih anonimizacijskih servisa.

Reference:

- **ISO/IEC 27001:2022** (A.8.16)
- **ISO/IEC 27002:2022** (8.16)
- **NIST SP 800-53 Rev. 5** (SC-7, AC-17)

SRZ-001: Mehanizmi za identifikaciju i upravljanje ranjivostima u razvoju sustava

Ova kontrola osigurava definiranje, dokumentiranje i primjenu procesa identifikacije i upravljanja ranjivostima u kritičnim mrežnim i informacijskim sustavima koje subjekt samostalno razvija. Sukladno procjeni rizika, subjekt može koristiti neke od sljedećih sigurnosnih provjera tijekom različitih faza razvoja:

- Statička analiza kôda (SAST) – omogućuje rano prepoznavanje ranjivosti kroz analizu izvornog kôda
- Dinamička analiza aplikacija (DAST) – testira sigurnost aplikacija u izvedbenom okruženju.
- Provjera sigurnosti komponenti trećih strana (SCA) – osigurava da korištene biblioteke i vanjske komponente nisu ranjive.
- Penetracijski testovi – identificiraju potencijalne slabosti kroz simulirane napade.
- *Bug bounty* programi ili slični mehanizmi – koriste vanjske istraživače za otkrivanje ranjivosti.

Provjera uključuje pregled dokumentacije o implementiranim sigurnosnim provjerama sukladno procjeni rizika, analizu izvještaja o provedenim testiranjima i njihovim rezultatima, procjenu usklađenosti sa sigurnosnim politikama i praksama subjekta te konzultacije s razvojnim timovima o integraciji sigurnosnih provjera u razvojni ciklus.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt ne provodi nikakve sigurnosne provjere na vlastito razvijenim rješenjima.
2	Sigurnosne provjere se provode povremeno, ali nisu formalizirane niti integrirane u razvojni proces. Koriste se pojedinačni alati bez strategije i sustavne analize ranjivosti. SAST/DAST se ne koristi dosljedno.
3	Subjekt ima dokumentiran osnovni proces upravljanja ranjivostima, uključujući upotrebu jednog ili više alata poput SAST, DAST ili SCA. Provjere se provode na većini projekata, ali još nisu u potpunosti integrirane u razvojni ciklus. Penetracijski testovi se planiraju za kritične sustave, a izvještaji se bilježe i djelomično analiziraju. Komunikacija između sigurnosnog i razvojnog tima postoji, ali suradnja nije stalna.
4	Sigurnosne provjere su standardizirane i sastavni su dio razvojnog ciklusa (SDLC). Koriste se alati za statičku (SAST) i/ili dinamičku analizu (DAST), te provjera komponenti trećih strana (SCA) na svim kritičnim projektima. Penetracijski testovi se redovito planiraju i evaluiraju. Dokumentacija je ažurna i u skladu sa sigurnosnim politikama. Suradnja timova za razvoj i sigurnost je strukturirana Pristup provjerama se temelji na riziku, ali još uvijek nije potpuno automatiziran.

5	Subjekt ima potpuno integriran sustav za upravljanje ranjivostima u okviru CI/CD procesa, s automatiziranim SAST/DAST/SCA alatima i kontinuiranom validacijom. Penetracijski testovi se provode periodično i nakon svake velike promjene, a *bug bounty* programi ili *crowd-sourced* testiranja su aktivni za vanjsku validaciju. Rezultati testiranja se automatski bilježe, prioritiziraju i dodjeljuju odgovornim timovima za ispravke.

Reference:

- **ISO/IEC 27001:2022** (A.8.25, A.8.26, A.8.27, A.8.29)
- **ISO/IEC 27002:2022** (8.25, 8.26, 8.27, 8.29)
- **NIST SP 800-53 Rev. 5** (SA-11, RA-5)
- **NIST CSF v2.0** (ID.RA-01)
- **CIS v8** (16.1, 16.2, 16.3, 16.6, 16.10, 16.12, 16.13)
- **OWASP ASVS 4.0.3** (V1)

SRZ-002: Kriteriji prihvaćanja rješenja i njihova primjena

Ova kontrola osigurava definiranje, dokumentiranje i primjenu kriterija za prihvaćanje rješenja mrežnih i informacijskih sustava prije njihove implementacije. Kriteriji prihvaćanja trebaju biti usklađeni s definiranim sigurnosnim zahtjevima, politikama sigurnosti i identificiranim rizicima te uključivati sigurnosna testiranja i provjere, revizije i procjene kroz testiranje sigurnosnih funkcionalnosti i analizu rizika prije puštanja rješenja u produkcijsku okolinu.

Provjera obuhvaća pregled dokumentacije o definiranim kriterijima prihvaćanja, analizu rezultata sigurnosnih testova i revizija, pregled rezultata provedenih testova usklađenosti te konzultacije s odgovornim osobljem za osiguranje kvalitete i sigurnosti.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoje kriteriji prihvaćanja. Rješenja se puštaju u rad bez testiranja, dokumentacije ili analize rizika.
2	Postoje definirani kriteriji za prihvaćanje rješenja koji nisu usklađeni sa sigurnosnim zahtjevima. Uloga sigurnosti u odlučivanju je ograničena.
3	Postoje dokumentirani kriteriji za prihvaćanje rješenja, usklađeni su sa sigurnosnim zahtjevima, ali nisu dosljedno primijenjeni.
4	Postoje dokumentirani kriteriji za prihvaćanje rješenja, usklađeni su sa sigurnosnim zahtjevima i dosljedno su primjenjivani. Sigurnosno i *QA* osoblje redovito sudjeluju u odlučivanju.
5	Kriteriji su integrirani u automatizirani razvojni proces. Svako rješenje prolazi sigurnosne kontrolne točke, a odluke o izmjenama i dopunama kriterija se temelje na analizi rizika i testovima koji se kontinuirano prate i prilagođavaju.

Reference:

- **ISO/IEC 27001:2022** (6.3, A.8.25, A.8.26, A.8.32)
- **ISO/IEC 27002:2022** (8.25, 8.26, 8.32)
- **NIST SP 800-53 Rev. 5** (SA-11, SA-15)
- **CIS v8** (16.1, 16.10, 16.12)

SRZ-003: Sigurnosni zahtjevi u procesima razvoja i održavanja

Ova kontrola osigurava definiranje, dokumentiranje i primjenu pravila za sigurnost i sigurnosnih zahtjeva tijekom cijelog životnog ciklusa razvoja i održavanja mrežnih i informacijskih sustava. Pravila trebaju obuhvatiti principe sigurnog dizajna („*secure by design*“ i „*secure by default*“), primjenu arhitekture nultog povjerenja *(zero trust*), identifikaciju ranjivosti tijekom svih faza razvoja te osiguranje usklađenosti sa sigurnosnim politikama subjekta. Osim toga, sigurnosni zahtjevi moraju biti definirani već u fazi specifikacije i projektiranja kako bi se osigurala njihova dosljedna primjena u kasnijim fazama razvoja i održavanja. Pravila trebaju biti redovito ažurirana kako bi odražavala nove prijetnje, rizike i tehnološke promjene.

Provjera uključuje pregled dokumentacije o sigurnosnim pravilima u procesima razvoja i održavanja, analizu definiranih sigurnosnih zahtjeva u fazi specifikacije i projektiranja te ocjenu njihove implementacije u svim fazama razvoja. Također se pregledava integracija sigurnih razvojnih praksi učinkovitost njihovih mehanizama primjene te usklađenost sa sigurnosnim politikama subjekta. U sklopu provjere provode se konzultacije s odgovornim osobljem za razvoj i održavanje sustava kako bi se osigurala dosljednost primjene sigurnosnih mjera.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	U procesima razvoja i održavanja sustava nije predviđena nikakva integracija sigurnosnih zahtjeva.
2	Postoje opća pravila ili smjernice za razvoj sustava, ali sigurnost nije formalno integrirana. Sigurnosni zahtjevi se definiraju kasno u razvoju ili samo za kritične komponente. Sigurnosne politike nisu referencirane tijekom razvoja, a razvojni tim nije u stalnom kontaktu sa sigurnosnim timom.
3	Subjekt ima definirana sigurnosna pravila koja pokrivaju razvoj i održavanje, a uključuju osnovne principe osiguravanja sigurnog dizajna i definiranje sigurnosnih zahtjeva u fazi projektiranja. Sigurnosni tim sudjeluje u fazama razvoja, ali nije integriran u svakodnevni proces.
4	Postoji formalni i operativni okvir sigurnosti razvoja, koji uključuje definiranje sigurnosnih zahtjeva već u fazi specifikacije i projektiranja. Primjenjuju se principi osiguranja sigurnog dizajna, a razvoj slijedi definiran model sigurnosne arhitekture. Sustavi se ne puštaju u produkciju bez provjere sigurnosnih kriterija.
5	Sigurnost je potpuno integrirana u sve faze razvoja i održavanja, s automatiziranim alatima za upravljanje sigurnosnim zahtjevima, testiranje ranjivosti i validaciju usklađenosti. Principi osiguranja sigurnog dizajna i arhitektura nultog povjerenja su standard.

Reference:

- **ISO/IEC 27001:2022** (A.8.25, A.8.26, A.8.27, A.8.28, A.8.29)

- **ISO/IEC 27002:2022** (8.25, 8.26, 8.27, 8.28, 8.29)
- **NIST SP 800-53 Rev. 5** (SA-3, SA-8, SA-11, SA-15)
- **CIS v8** (16.1, 16.2, 16.3, 16.7, 16.10, 16.12, 16.13)

KRIP-001: Politike i pravila za primjenu kriptografije

Ova kontrola osigurava razvoj, dokumentiranje, održavanje i implementaciju pravila za primjenu kriptografije u mrežnim i informacijskim sustavima. Pravila trebaju definirati odgovarajuće mehanizme primjene kriptografije na temelju vrste podataka i procjene rizika te osigurati zaštitu autentičnosti, cjelovitosti i povjerljivosti podataka. Pravila također trebaju biti usklađena s internim aktima ali i ažurirana sukladno razvoju prijetnji i tehnologija.

Provjera uključuje pregled dokumentacije o pravilima za primjenu kriptografije, analizu rezultata procjene rizika i analizu primijenjenih kriptografskih metoda te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala dosljedna implementacija pravila.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt nema definirana pravila ni politiku za primjenu kriptografije.
2	Pravila su definirana, ali nisu sveobuhvatna, redovito ažurirana niti usklađena s procjenom rizika.
3	Pravila su definirana i djelomično primijenjena, ali nisu dosljedno ažurirana ili implementirana.
4	Sveobuhvatna pravila su definirana, dokumentirana, revidirana i dosljedno primijenjena u skladu s rizicima.
5	Pravila i politike su potpuno integrirane s procesima upravljanja rizicima.

Reference:

- **ISO/IEC 27001:2022** (A.8.24)
- **ISO/IEC 27002:2022** (8.24)
- **NIST SP 800-53 Rev. 5** (SC-12, SC-13)
- **NIST CSF v2.0** (PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11)

KRIP-002: Kriptiranje podataka u prijenosu

Ova kontrola osigurava primjenu odgovarajućih metoda kriptiranja za zaštitu kritičnih podataka tijekom prijenosa putem mrežnih i informacijskih sustava. Kontrola uključuje odabir odgovarajućih kriptografskih algoritama, metoda nadopune prije kriptiranja (*padding*) i veličinu ključeva koji su usklađeni s najboljim praksama i proporcionalni riziku te važnosti podataka. Također obuhvaća osiguranje primjenjivosti kriptiranja na svim komunikacijskim kanalima koji prenose povjerljive ili kritične podatke. Poseban naglasak stavlja se na primjenu kriptografskih metoda prema osjetljivosti podataka i trenutnim sigurnosnim standardima.

Provjera uključuje pregled dokumentacije o primijenjenim metodama kriptiranja, analizu konfiguracija sustava za prijenos podataka, primijenjenih kriptografskih algoritama i mrežnih protokola, testiranje konfiguracije sustava i kriptiranje tijekom prijenosa podataka, provjeru sukladnosti s internim politikama i regulatornim zahtjevima te konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala dosljedna primjena kriptiranja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Kriptiranje podataka u prijenosu nije implementirano. Podaci se prenose bez zaštite, otvorenim protokolima (npr. HTTP, FTP, telnet).
2	Kriptiranje se koristi samo za pojedine sustave ili vanjsku komunikaciju (npr. web stranice s HTTPS-om), ali nije primijenjeno dosljedno na sve interne ili međusistemske komunikacijske kanale. Algoritmi i metode kriptiranja nisu uvijek u skladu s najboljim praksama – koriste se zastarjeli protokoli i algoritmi (poput TLS 1.0, SHA-1).
3	Većina komunikacijskih kanala koji prenose osjetljive podatke koristi adekvatne kriptografske mehanizme (poput TLS 1.2+, IPsec ili SSH). Subjekt ima dokumentaciju o korištenim algoritmima, ali se ne provodi redovita provjera njihove učinkovitosti i sukladnosti s aktualnim standardima.
4	Kriptiranje u prijenosu je standardna praksa za sve sustave koji obrađuju ili razmjenjuju podatke. Sve konfiguracije se dokumentiraju i redovito testiraju.
5	Subjekt ima potpuno integriran i automatiziran sustav zaštite podataka u prijenosu, s dinamičkim izborom kriptografskih metoda temeljem klasifikacije podataka, rizika i konteksta komunikacije. Svi komunikacijski kanali koriste sigurnosne protokole i algoritme sukladno najboljim praksama. Kontinuirano se prati stanje i zastarjelost algoritama, a sustav se prilagođava u skladu s prijetnjama i standardima.

Reference:

- **ISO/IEC 27001:2022** (A.8.24)

- **ISO/IEC 27002:2022** (8.24)
- **NIST SP 800-53 Rev. 5** (SC-13)
- **NIST CSF v2.0** (PR.DS-02)
- **CIS v8** (3.10)

KRIP-003: Sigurno upravljanje životnim ciklusom kriptografskih ključeva

Ova kontrola osigurava sigurno upravljanje životnim ciklusom kriptografskih ključeva, uključujući generiranje, distribuciju, pohranu, zamjenu, opoziv, oporavak i uništavanje ključeva u skladu s dobrim praksama i sigurnosnim zahtjevima subjekta. Također uključuje definiranje pravila pristupa ključevima, evidenciju aktivnosti i zaštitu od neovlaštenog pristupa.

Provjera uključuje pregled dokumentacije o postupcima za upravljanje ključevima, analizu zapisa o aktivnostima vezanim uz ključeve, analizu mehanizama za sigurno generiranje i pohranu ključeva uz provjere redovitosti zamjene i uništavanja ključeva, testiranje procedura za distribuciju i opoziv ključeva te konzultacije s odgovornim osobljem za sigurnost.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Ne postoji formalno upravljanje ključevima. Ključevi se generiraju i koriste bez dokumentiranih pravila, a često se pohranjuju u nekriptiranom obliku.
2	Postoje osnovna pravila za upravljanje ključevima, ali bez pokrivenosti svih faza životnog ciklusa. Ključevi se ručno distribuiraju, bez kontrole pristupa i nadzora. Zamjena i opoziv ključeva nisu definirani, a postupanje s kompromitiranim ili izgubljenim ključevima nije jasno propisano.
3	Subjekt ima dokumentirana pravila za upravljanje kriptografskim ključevima koja pokrivaju većinu faza životnog ciklusa, uključujući generiranje, pohranu, distribuciju i opoziv. Ključevi se čuvaju u zaštićenim prostorima ili kriptiram datotekama. Postoje osnovne kontrole pristupa i evidencije aktivnosti, ali nisu centralizirane. Zamjena i opoziv se provode, ali bez automatizacije. Nema jasne politike za postupanje s kompromitiranim ili izgubljenim ključevima.
4	Subjekt primjenjuje strukturiran i dokumentiran sustav za upravljanje ključevima, uz jasno definirane politike i procedure za sve faze. Ključevi se pohranjuju sigurno, a pristup je strogo ograničen i kontroliran. Aktivnosti nad ključevima se bilježe, a revizije se provode periodično. Sustav još uvijek zahtijeva ručnu intervenciju za većinu procesa.
5	Subjekt koristi strukturiran i dokumentiran sustav upravljanja ključevima koji pokriva cijeli životni ciklus ključeva. Ključevi su kriptografski zaštićeni, upravljani politikama temeljenim na ulogama, a sve aktivnosti su automatski bilježene. Sustav podržava automatizirane rotacije ključeva, opozive, oporavke i revizijske izvještaje. Kompromitirani ključevi se brzo opozivaju putem automatiziranih mehanizama.

Reference:

- **ISO/IEC 27001:2022** (A.8.24)
- **ISO/IEC 27002:2022** (8.24)
- **NIST SP 800-53 Rev. 5** (SC-12)

KRIP-004: Kriptiranje podataka u mirovanju

Ova kontrola osigurava primjenu kriptografskih metoda za zaštitu kritičnih podataka pohranjenih na različitim medijima (diskovi, baze podataka, prijenosni uređaji). Kriptografski algoritmi, metode nadopune prije kriptiranja (*padding*) i veličine ključeva moraju se usklađivati s najboljim praksama i prilagoditi procijenjenim rizicima subjekta. Kontrola obuhvaća implementaciju mehanizama za automatsko kriptiranje pohranjenih podataka i osiguranje pristupa samo ovlaštenim korisnicima.

Provjera uključuje pregled dokumentacije o metodama kriptiranja podataka u mirovanju, analizu konfiguracija sustava za pohranu podataka, provjere primjene odgovarajućih kriptografskih algoritama i ključeva te konzultacije s osobljem odgovornim za sigurnost kako bi se osigurala dosljedna primjena kriptiranja.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Podaci u mirovanju nisu kriptografski zaštićeni.
2	Kriptiranje se koristi samo za pojedine sustave ili uređaje. Algoritmi i duljine ključeva nisu nužno u skladu s najboljim praksama (primjerice koriste se zastarjeli algoritmi poput DES ili RC4). Ne postoji nadzor nad primjenom, a prijenosni uređaji često nisu pokriveni zaštitom.
3	Postoji politika za zaštitu podataka u mirovanju, a kritični sustavi koriste algoritme sukladno najboljim praksama. Većina baza podataka i diskova s osjetljivim podacima koristi kriptiranje. Kriptografske metode su definirane, ali se ne prate sustavno njihova zastarjelost ili relevantnost prema novim prijetnjama.
4	Kriptiranje podataka u mirovanju je prošireno na sve ključne sustave i uređaje. Politike definiraju preporučene algoritme, metode nadopune prije kriptiranja i minimalnu duljinu ključeva. Pristup kriptiranim podacima je strogo kontroliran putem sustava za autentifikaciju i autorizaciju. Politike se ažuriraju periodično prema razvoju prijetnji i tehnološkim standardima.
5	Subjekt ima automatiziran i centraliziran sustav za kriptiranje podataka u mirovanju, integriran s klasifikacijom podataka i upravljanjem ključevima. Svi mediji, uključujući repozitorije u oblaku, sustave za sigurnosno kopiranje i pohranu, mobilne uređaje i prijenosne medije, automatski se kriptiraju s dinamičkom primjenom algoritama prema riziku.

Reference:

- **ISO/IEC 27001:2022** (A.8.24)
- **ISO/IEC 27002:2022** (8.24)
- **NIST SP 800-53 Rev. 5** (SC-13, SC-28)
- **NIST CSF v2.0** (PR.DS-01)
- **CIS v8** (3.11)

KRIP-005: Primjena kvantno otporne kriptografije

Ova kontrola osigurava implementaciju kvantno otpornih kriptografskih algoritama i metoda za zaštitu podataka sukladno procjeni rizika. Kvantno otporna kriptografija primjenjuje se za zaštitu podataka koji zahtijevaju dugoročnu sigurnost. Kontrola uključuje evaluaciju postojećih kriptografskih sustava, planiranje migracije na kvantno otporne algoritme te ažuriranje kriptografskih politika i procedura.

Provjera uključuje pregled dokumentacije o procjeni rizika za primjenu kvantno otporne kriptografije, analizu implementiranih algoritama, provjeru planova migracije i konzultacije s odgovornim osobljem za sigurnost kako bi se osigurala dosljedna implementacija kvantno otporne kriptografije.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Subjekt nije razmatrao ni evaluirao utjecaj kvantnog računalstva na postojeće kriptografske sustave.
2	Subjekt je identificirao potrebu za kvantno otpornom kriptografijom u teoriji, ali nema provedbeni plan. Postoji osnovna procjena rizika, ali nije povezana s konkretnim sustavima ili vrstama podataka.
3	Subjekt je proveo procjenu rizika i identificirao koje vrste podataka zahtijevaju dugoročnu zaštitu. Postoji plan migracije na kvantno otporne algoritme, ali je još u fazi pripreme. Sigurnosne politike su ažurirane kako bi uključile kvantno otpornu kriptografiju kao nadolazeći zahtjev.
4	Subjekt je implementirao prve faze migracije na kvantno otporne algoritme u ne-kritičnim ili paralelnim okruženjima. U tijeku su validacije interoperabilnosti s postojećim PKI sustavima. Politike i tehnička dokumentacija su ažurirane, sigurnosno osoblje educirano, a partneri i dobavljači uključeni u planiranje. Podaci koji zahtijevaju dugoročnu zaštitu se već pohranjuju ili prenose s kvantno otpornim slojevima.
5	Subjekt ima proaktivnu strategiju za kvantno otpornu sigurnost, s implementiranim kvantno otpornim kriptografskim algoritmima u kritičnim aplikacijama i komunikacijama. Sve komponente koje upravljaju osjetljivim podacima koriste kvantno otporne algoritme.

Reference:

- **ISO/IEC 27001:2022** (A.8.24)
- **ISO/IEC 27002:2022** (8.24)
- **NIST SP 800-53 Rev. 5** (SC-13)

FIZ-001: Implementacija osnovnih fizičkih mjera zaštite

Kontrola zahtijeva implementaciju osnovnih fizičkih mjera zaštite, uključujući odgovarajuće fizičke barijere, brave, sigurnosne kamere i sustave za kontrolu pristupa. Mjere zaštite moraju biti prilagođene procjeni rizika subjekta, uzimajući u obzir kritičnost prostora i imovine koja se u njima nalazi.

Provjerava se dokumentacija o provedenim mjerama zaštite, tehnički specifikacijski podaci o implementiranim sustavima (npr. sigurnosne kamere, kontrole pristupa) te zapisi o provedenim procjenama rizika i njihovoj implementaciji.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Osnovne fizičke mjere zaštite nisu implementirane niti dokumentirane.
2	Djelomična implementacija fizičkih mjera zaštite, bez dokumentacije ili procjene rizika.
3	Implementirane osnovne fizičke mjere zaštite uz djelomičnu dokumentaciju ili procjenu učinkovitosti, ali bez potpunog prilagođavanja procjeni rizika.
4	Sveobuhvatno implementirane osnovne mjere zaštite, uz djelomičnu dokumentaciju ili procjenu učinkovitosti.
5	Osnovne fizičke mjere zaštite su u potpunosti implementirane, dokumentirane i usklađene s procjenom rizika.

Reference:

- **ISO/IEC 27001:2022** (A.7.1, A.7.2, A.7.4)
- **ISO/IEC 27002:2022** (7.1, 7.2, 7.4)
- **NIST SP 800-53 Rev. 5** (PE-2, PE-3, PE-6)

FIZ-002: Revizija i ažuriranje sigurnosnih protokola za fizičke lokacije

Kontrola zahtijeva redovitu reviziju i ažuriranje sigurnosnih protokola za fizičke lokacije, posebno za kritične mrežne i informacijske sustave. Protokoli moraju biti prilagođeni procjeni rizika i razini kritičnosti sustava. Potrebno je osigurati da sigurnosni protokoli ostanu ažurni, učinkoviti i usklađeni s promjenjivim rizicima te poslovnim potrebama.

Pregledava se dokumentacija o revizijama sigurnosnih protokola, rezultati procjena rizika, implementirani protokoli i njihova prilagodba kritičnosti mrežnih i informacijskih sustava.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sigurnosni protokoli nisu uspostavljeni.
2	Sigurnosni protokoli postoje, ali nisu revidirani niti prilagođeni rizicima.
3	Sigurnosni protokoli su uspostavljeni i revidirani, ali bez prilagodbe kritičnim sustavima, dokumentacija nije potpuna
4	Sigurnosni protokoli su revidirani i prilagođeni rizicima, ali dokumentacija nije potpuna.
5	Sigurnosni protokoli su redovito revidirani, dokumentirani i prilagođeni kritičnim sustavima.

Reference:

- **ISO/IEC 27001:2022** (6.1, 7.5, 9.1, 9.2)
- **ISO 22301:2019** (6.1, 7.5, 9.1, 9.2)
- **NIST SP 800-53 Rev. 5** (PE-1, PE-3)

FIZ-003: Evidencija fizičkog pristupa

Kontrola osigurava implementaciju sustava za evidenciju fizičkog pristupa svim kritičnim prostorima. Evidencija mora uključivati jednoznačne zapise koji su sigurno pohranjeni i dostupni za naknadnu analizu ili digitalnu forenziku.

Pregledava se funkcionalnost sustava za evidenciju pristupa, način pohrane podataka i dostupnost za analizu.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za evidenciju fizičkog pristupa nije implementiran.
2	Sustav za evidenciju je implementiran, ali podatci nisu sigurno pohranjeni.
3	Sustav za evidenciju je implementiran i podatci su sigurno pohranjeni.
4	Sustav je potpuno implementiran i integriran sa sustavom za upravljanje zapisima.
5	Sustav je potpuno implementiran, dokumentiran i prilagođen za digitalnu forenziku.

Reference:

- **ISO/IEC 27001:2022** (7.5, A.7.2, A.7.4, A.8.15)
- **ISO/IEC 27002:2022** (7.2, 7.4, 8.15)
- **NIST SP 800-53 Rev. 5** (PE-3, PE-6, PE-8)

FIZ-004: Nadzor prostora u stvarnom vremenu

Potrebno je osigurati implementaciju sustava za nadzor prostora u stvarnom vremenu koji uključuju kritičnu programsku i sklopovsku imovinu sukladno procjeni rizika subjekta. Sustav mora omogućiti kontinuirano praćenje, otkrivanje anomalija i generiranje upozorenja. Cilj je minimizirati rizike neovlaštenog pristupa i omogućiti brzu reakciju na sigurnosne incidente.

Potrebno je ustanoviti funkcionalnost sustava za nadzor, postojanje izvješća o praćenju i detektiranim anomalijama. Provjerava se usklađenost sustava s procjenom rizika i kritičnošću imovine.

Smjernice za ocjenjivanje:

Ocjena	Uvjet
1	Sustav za nadzor prostora nije implementiran bez obzira na utvrđenu potrebu.
2	Sustav je djelomično implementiran, ali nije usklađen s procjenom rizika subjekta.
3	Sustav je implementiran sukladno procjeni rizika subjekta, ali ne omogućuje kontinuirano praćenje ili generiranje upozorenja.
4	Sustav je implementiran sukladno procjeni rizika subjekta, ali nedostaju izvješća o detektiranim anomalijama.
5	Sustav je implementiran, kontinuirano praćen, dokumentiran i prilagođen procjeni rizika.

Reference:

- **ISO/IEC 27001:2022** (A.7.3, A.7.4)
- **ISO/IEC 27002:2022** (7.3, 7.4)
- **NIST SP 800-53 Rev. 5** (PE-3, PE-6)
- **NIST CSF v2.0** (DE.CM-02)