ISO/IEC 27001 - norma za informacijsku sigurnost

Marodi, Bartol

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:580287

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-10-17**

Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2023./2024.

Bartol Marodi

ISO/IEC 27001 – norma za informacijsku sigurnost

Završni rad

Mentor: dr. sc. Hrvoje Stančić, red. prof.

Zagreb, lipanj 2024.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod 1
2. Općenito o normi 1
   2.1. Informacijska sigurnost 1
   2.2. O ISO/IEC-u 2
   2.3. Sustav upravljanja informacijskom sigurnošću (ISMS) 4
   2.4. Što je ISO/IEC 27001 4
3. Povijest i sadržaj norme 7
   3.1. Povijest norme 7
   3.2. Sadržaj norme 8
   3.3. Ostale norme serije 27000 13
   3.4. Relacija između norme ISO/IEC 27001 i GDPR-a 14
4. Implementacija norme 17
   4.1. Certifikacija 18
   4.2. Dobrobiti primjene norme ISO/IEC 27001 19
5. Studija slučaja – uvođenje norme ISO/IEC 27001 u organizaciju 22
   5.1. Osnovne informacije o organizaciji 22
   5.2. Aktivnosti za uvođenje norme 22
      5.2.1. GAP analiza 23
      5.2.2. Dokumentacija 24
      5.2.3. Unaprjeđenje sigurnosti podataka unutar programskih rješenja 25
      5.2.4. Evidencija ciljeva i repetitivnih aktivnosti 26
      5.2.5. Evidencija imovine i zaduženja djelatnika 28
      5.2.6. Promjene u mrežnoj i računalnoj infrastrukturi 30
      5.2.7. Fizička sigurnost 30
   5.3. Certifikacija 30
   5.4. Osvrt uprave na uvođenje norme 31
6. Zaključak 34
7. Popis literature 35
8. Popis slika 38

Sažetak 39

Summary 40

1. Uvod

Informacija je, u mnogim slučajevima, najvrjednija imovina koju organizacija posjeduje. U ovoj eri digitalne tehnologije i njezine rastuće kompleksnosti, upravljanje sigurnošću informacija je prilično izazovan zadatak za razne tvrtke, institucije i ostale organizacije. Tu je organizacijama od velike pomoći norma za informacijsku sigurnost ISO/IEC 27001, koja pruža smjernice kako na sustavan i dugoročno isplativ način implementirati sustav za upravljanje informacijskom sigurnošću.

2. Općenito o normi

2.1. Informacijska sigurnost

Sve organizacije posjeduju informacije ili podatke koji su kritični ili osjetljivi. Organizacije su visoko ovisne o elektroničkim informacijama i sustavima koji ih obrađuju. Nezamislivo je poslovanje bez interneta, web stranica, email poruka i dokumenata u elektroničkom obliku. Prijetnje sigurnosti ovim sustavima i informacijama su velike i kontinuirano se povećavaju. Zbog toga je u svakoj organizaciji neophodan sustav upravljanja sigurnošću informacija. (Calder, 2008)

Vijeće za nacionalnu sigurnost Republike Hrvatske definira informacijsku sigurnost na sljedeći način: informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. (Ured vijeća za nacionalnu sigurnost, 2014)

Informacijska sigurnost temelj je današnjeg poslovanja i vrlo je bitna za sve gospodarske subjekte. Informacijska sigurnost u različitim okolnostima znači

različite stvari. Za prodavače sigurnosnih proizvoda obično je ograničeno na proizvode koje prodaju. Mnogim direktorima i menadžerima to znači nešto što oni ne razumiju i s čime se mora nositi IT menadžer. Korisnicima IT opreme to obično znači neželjena ograničenja onoga što mogu raditi na svojim korporativnim računalima. No, sve su to uski pogledi na informacijsku sigurnost. (Calder, 2008)

Informacijska sigurnost usredotočena je na cijelu organizaciju i odnosi se na sigurnost informacijske tehnologije. Naime, sigurnost informacija usmjerena je na podatke koje obrađuju elektronički sustavi, no i na sigurnost informacija na analognim nosačima podataka kao što je papir.

Sigurnost informacijske tehnologije i informacijska sigurnost usko su povezane. S obzirom na digitalizaciju procesa obrade podataka, informacije se obično obrađuju, pohranjuju ili prenose uz pomoć informacijskih tehnologija. (DQS Zagreb, 2022)

Elektronički napadi i ugrožavanja informacijske sigurnosti sve su složeniji te je u odgovoru na njih potrebno stalno učenje, praćenje trendova i inovativnost u rješenjima. Zbog propuštanja provedbe i održavanja odgovarajuće kontrole rizika i sigurnosti informacije, organizacije postaju kazneno odgovorne, a u nekim slučajevima su i direktori osobno odgovorni.

Za učinkovitu zaštitu informacijskih sustava i informacija unutar organizacije, potreban je sustavni pristup. Takav pristup uključuje uvođenje normi i standarda zaštite informacija.

2.2. O ISO/IEC-u

Međunarodna organizacija za normizaciju ISO (punim nazivom International Organization for Standardization) je međunarodno tijelo za donošenje normi koje je sastavljeno od predstavnika raznih nacionalnih normizacijskih tijela. Trenutno na donošenju norma zajednički rade stručnjaci iz normizacijskih tijela iz 170 zemalja. Organizacija je osnovana 23. veljače 1947, a izdaje industrijske i komercijalne norme.

Iako se ISO definira kao nevladina organizacija, donosi norme koje često postanu zakoni, bilo kroz međunarodne ugovore ili kroz nacionalne norme, što ju čini moćnijom od većine nevladinih organizacija. U praksi, ISO se ponaša kao konzorcij usko povezan s vladama. (Wikipedija, n.d.)

Slika 1. Logo organizacije ISO (Wikipedija, n.d.)

IEC (punim nazivom International Electrotechnical Commision) je svjetska neprofitna organizacija čiji rad podupire kvalitetnu infrastrukturu i međunarodnu trgovinu električnim i elektroničkim putem. Njezin rad olakšava tehničke inovacije, razvoj dostupnih infrastruktura, učinkovit i održiv pristup energiji, pametnu urbanizaciju i sustave transporta, ublažavanje klimatskih promjena i povećanje sigurnosti ljudi i okoliša. (International Electrotechnical Commision, 2024)

Slika 2. Logo organizacije IEC (IEC, n.d.)

ISO i IEC imaju zajednički tehnički odbor: ISO/IEC JTC 1. Taj odbor ima nekoliko pod-odbora. Jedan od njih je i SC 27, čija je djelatnost tehnike sigurnosti u informacijskoj tehnologiji. Upravo taj odbor je zadužen za stvaranje norme ISO/IEC 27001, koja je tema ovog rada. (Calder, 2009)

2.3. Sustav upravljanja informacijskom sigurnošću (ISMS)

Sustav upravljanja informacijskom sigurnošću (engl. Information security management system, skraćeno ISMS) je dio upravljačkog sustava organizacije koji se bavi poslovnim rizikom da bi uspostavio, implementirao, rukovao, nadgledao, analizirao, održavao i konstantno poboljšavao informacijsku sigurnost. (Calder, 2009)

Jednostavnije sročeno, ISMS je sustav koji obuhvaća cjelokupno upravljanje informacijskom sigurnošću u organizaciji. Djelatnosti tog sustava uključuju definiranje politika, identifikaciju i procjenu rizika, uspostavu kontrola i mjera zaštite, te redovito praćenje i reviziju sigurnosnih aktivnosti. Glavni cilj ISMS-a je zaštititi informacije od prijetnji, održavati povjerljivost, integritet i dostupnost podataka, te osigurati usklađenost s relevantnim propisima i zahtjevima.

ISMS služi organizacijama kao pomoć u održavanju sigurnog i nerizičnog poslovanja. (Junaid, 2023) Njegova implementacija u organizaciju ovisi o ciljevima i potrebama organizacije, sigurnosnim zahtjevima, organizacijskim procesima koji su korišteni, te o veličini i strukturi organizacije.

2.4. Što je ISO/IEC 27001

Da bi ISMS ispravno funkcionirao, važno je da se pridržava zahtjeva međunarodne norme za informacijsku sigurnost, koja nosi naziv ISO/IEC 27001. To je najpoznatiji svjetski standard za sustave upravljanja sigurnošću informacija, koji definira zahtjeve za uspostavljanje, uvođenje, održavanje i trajno poboljšavanje sustava upravljanja informacijskom sigurnošću unutar konteksta organizacije. Norma

ISO/IEC 27001 se jednako odnosi na sve tvrtke, bez obzira na njihovu veličinu ili djelatnost kojom se bave.

Sukladnost s ISO/IEC 27001 znači da je organizacija uspostavila sustav za upravljanje rizicima povezanim sa sigurnošću podataka kojima posjeduje ili njima rukuje te da taj sustav poštuje sve najbolje prakse i načela ugrađena u ovu međunarodnu normu. (ISO, n.d.)

ISO 27001 je standard koji obuhvaća politike, procedure smjernice potrebne za uspostavljanje cjelovite informacijske sigurnosti. Cjelovita informacijska sigurnost odnosi se na rizike temeljene na tehnologiji, ljudima i procesima, šte uključuje i rizike vezane uz slabo informirane zaposlenike ili neučinkovite postupke.

Norma propisuje načine na koje organizirati informacijsku sigurnost u bilo kojoj vrsti organizacije (profitnoj ili neprofitnoj, privatnoj ili državnoj, maloj ili velikoj). ISO/IEC 27001 je temeljna norma za upravljanje informacijskom sigurnošću i pomaže organizacijama da zaštite svoje važne informacije od zloupotrebe, oštećenja ili gubitka.

S obzirom na veliki značaj norme ISO/IEC 27001, mnoga su zakonodavstva uzela tu normu kao temelj za pisanje regulative iz područja zaštite osobnih podataka, zaštite tajnosti podataka, zaštite informacijskih sustava, upravljanja operativnim rizicima u financijskim ustanovama i sl.

ISO 27001 daje specifikaciju za informacijsku sigurnost sustava upravljanja, a oslanja se na znanje skupine iskusnih praktičara informacijske sigurnosti u širokom krugu značajnih organizacija u više od 40 zemalja kako bi postavili najbolju praksu u informacijskoj sigurnosti. ISO 27001-usklađen sustav omogućit će sustavan pristup identificiranju i borbi protiv cijelog niza potencijalnih rizika informacijskih sredstava organizacije. (Calder, 2008)

Standard obuhvaća upravljanje svim aspektima informacijske sigurnosti, uključujući fizičku sigurnost, sigurnost osoblja, upravljanje rizicima, kontinuitet poslovanja, nadzor i reviziju, kao i usklađenost s regulatornim zahtjevima.

Sigurnost informacija promatra se kroz aspekt dostupnosti, integritet i povjerljivost informacija. (Calder, 2008) Dostupnost označava svojstvo informacije da je pristupačna i upotrebljiva članovima organizacije i njenim klijentima kad god je to potrebno. Integritet (ili cjelovitost) se odnosi na čuvanje točnosti i kompletnosti informacija, a povjerljivost označava da informacija nije dostupna ili razotkrivena neovlaštenim individuama, entitetima ili procesima. (Calder, 2009)

Uz rastući kibernetički kriminal i stalno pojavljivanje novih prijetnji, može se činiti da je teško ili čak nemoguće upravljati kibernetičkim rizicima. ISO/IEC 27001 pomaže organizacijama da postanu svjesne rizika i proaktivno prepoznaju i riješe slabosti. ISO/IEC 27001 promiče holistički pristup informacijskoj sigurnosti, koji uključuje provjeru ljudi, politika i tehnologije. Sustav upravljanja informacijskom sigurnošću implementiran prema ovoj normi je alat za upravljanje rizicima, kibernetičku otpornost i operativnu izvrsnost. (ISO, n.d.)

3. Povijest i sadržaj norme

3.1. Povijest norme

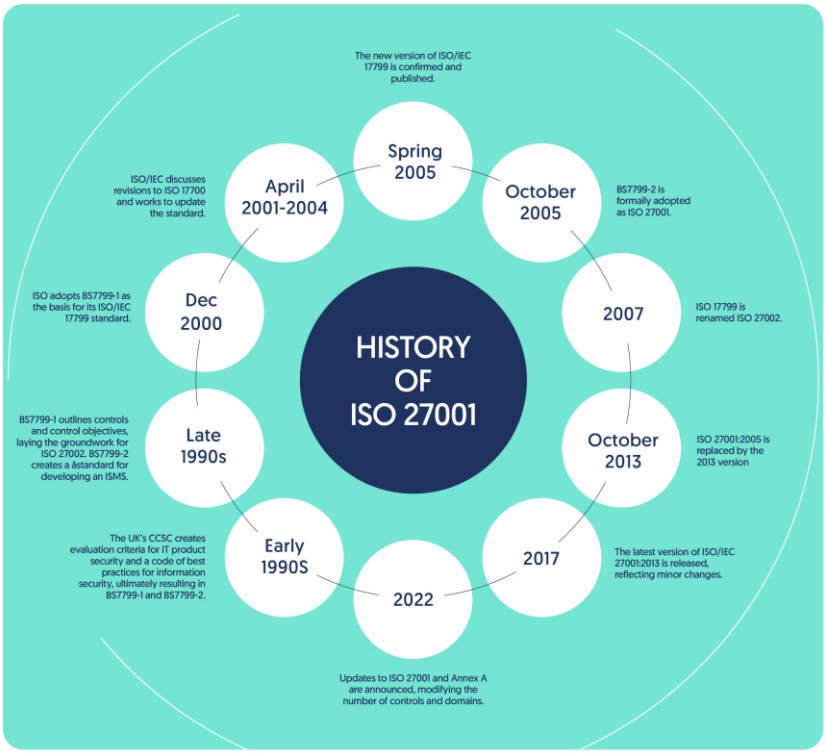
Korijeni norme ISO/IEC 27001 sežu još u početak zadnjeg desetljeća prošlog stoljeća. Tada je Odjel za trgovinu i industriju (DTI) vlade Ujedinjenog Kraljevstva zatražio od Centra za komercijalnu računalnu sigurnost (CCSC) da izradi skup kriterija procjene za određivanje sigurnosti IT proizvoda. Od CCSC-a je također zatraženo da izradi kodeks najboljih praksi za informacijsku sigurnost. Rezultat je bio dokument poznat kao DISC PD003. Rad na DISC PD003 se nastavio i bio je podijeljen u dva glavna fronta: BS 7799-1 i BS 7799-2. (Secureframe, n.d.)

BS 7799 je bio britanski standard za sigurnost informacija koji je, dakle, bio podijeljen na 2 dijela. Prvi dio (BS 7799-1) je nosio naziv Code of Practice for Information Security Management, koji je davao smjernice za praktična pitanja uspostave informacijske sigurnosti u organizaciji. Drugi dio (BS 7799-2), Specification for Information Security Management Systems, je, kako samo ime kaže, specifikacija na temelju koje organizacije mogu biti procijenjene i certificirane. Dok se prvi dio norme BS 7799 bavi praktičnim pitanjima, drugi dio je zapravo teorijski i normativni okvir za praktična rješenja koja se preporučuju u prvom dijelu norme. (Calder, 2009)

Sa željom da internacionaliziraju normu BS 7799, kompanije ISO i IEC su 2000. godine donijele svoju normu o informacijskoj sigurnosti: ISO/IEC 17799:2000. 2002. godine je nastala druga verzija norme BS 7799. Neke od promjena su dodatak PDCA (plan-do-check-act) modela implementacije norme te dodatak zahtjeva da se konstantno poboljšava ISMS organizacije. BS 7799-2:2002 je i dalje bio britanski standard, iako je preveden na nekoliko jezika, a neke države su ga čak uvele kao svoj nacionalni standard. (Calder, 2009)

ISO i IEC su ponovno željeli internacionalizirati britansku normu, što se i dogodilo u lipnju 2005. Tada je nastala prva verzija norme ISO/IEC 27001. Trenutno je na snazi treća verzija norme, koja je izdana 2022. godine. Uz manje promjene u tekstu norme, glavna promjena u normi od prve verzije do trenutne je modifikacija tablice s

preporučenim kontrolama informacijske sigurnosti: u trenutnoj verziji kontrole su organizirane u 4 umjesto u 14 grupa sa sveukupno 93 kontrola umjesto prijašnjih 114.



Slika 3. Povijest norme ISO/IEC 27001 (Secureframe, n.d.)

3.2. Sadržaj norme

Norma ISO/IEC 27001 je organizirana u deset poglavlja, od kojih prva tri daju općenite informacije i smjernice za ostatak dokumenta. Svako poglavlje od četvrtog do desetog se bavi jednom kategorijom zahtjeva za ostvarivanje ispravnog ISMS-a.

Četvrto poglavlje se bavi organizacijom koja želi implementirati svoj ISMS. Naglašava kako je potrebno razumjeti organizaciju i njen kontekst, te kako je potrebno razumjeti potrebe i očekivanja zainteresiranih strana (klijenata) organizacije. U tom poglavlju se također kaže da je u organizaciji potrebno odrediti

opseg, odnosno granice i primjenjivost ISMS-a kojeg želi implementirati. Tu informaciju organizacija je dužna dokumentirati.

Peto poglavlje govori o vođenju uspostave i održavanja ISMS-a u organizaciji. Također zahtjeva da organizacija uspostavi politiku informacijske sigurnosti koja je primjerena svrsi organizacije i njezinim ciljevima informacijske sigurnosti, ali i koja ispunjava zahtjeve ove norme. Politika informacijske sigurnosti također mora biti poznata svim članovima organizacije i zainteresiranim stranama, te mora biti dostupna kao dokumentirana informacija. U tom poglavlju se zahtjeva i da se unutar organizacije podijele odgovornost i ovlasti za osiguravanje da je sustav upravljanja informacijskom sigurnošću sukladan zahtjevima norme i za izvještavanje poslovodstva o performansama sustava upravljanja informacijskom sigurnošću.

Šesto poglavlje govori o planiranju ISMS-a. Prilikom planiranja, organizacija mora utvrditi rizike i prilike koji se moraju otkloniti zbog uspješne implementacije ISMS-a. Potrebno je procijeniti rizik informacijske sigurnosti. U tom procesu se mora uspostaviti i održavati kriterij za prihvaćanje rizika i kriterij za provođenje procjene rizika informacijske sigurnosti. Također je potrebno identificirati, analizirati i vrednovati rizike informacijske sigurnosti, te sve to dokumentirati i tu dokumentaciju sačuvati. Što se tiče otklanjanja rizika, tu norma nalaže da je potrebno odabrati prikladne opcije i kontrole za otklanjanje rizika. Preporučene kontrole su nabrojane na kraju norme, u dodatku (Annex A). Budući da je to lista preporučenih kontrola, organizacija može uvesti neke svoje kontrole i izbaciti neke kontrole s te liste, no za to mora imati obrazloženje koje je potrebno navesti u dokumentaciji. Poglavlje o planiranju zahtjeva i uspostavu ciljeva informacijske sigurnosti i planiranje njihova postizanja (što je potrebno dokumentirati) te nalaže da se promjene, kad se utvrde, moraju planirano provesti.

Sedmo poglavlje norme govori o podršci. Tu se najprije zahtjeva od organizacije da odredi i osigura resurse potrebne za uspostavljanje, uvođenje, održavanje i trajno poboljšavanje sustava upravljanja informacijskom sigurnošću. Nadalje, zahtjeva se od organizacije da odredi nužne kompetencije za osobu koja izvodi poslove koji su utjecajni na performanse informacijske sigurnosti. Osoba mora steći kompetencije

edukacijom, osposobljavanjem ili iskustvom, a gdje je primjenjivo, organizacija mora poduzeti radnje radi stjecanja nužnih kompetencija i ocijeniti djelotvornost poduzetih radnji. Potrebno je sačuvati primjerene dokumentirane informacije kao dokaze kompetencije. Nadalje, u ovom poglavlju stoji da osobe koje izvode poslove pod nadzorom organizacije moraju biti svjesni politike informacijske sigurnosti koju organizacija provodi, svojega doprinosa djelotvornosti sustava upravljanja informacijskom sigurnošću, te implikacija neusklađenosti sa zahtjevima ove norme. Organizacija također mora odrediti potrebu za internom i eksternom komunikacijom relevantnom za sustav upravljanja informacijskom sigurnošću. I na kraju tog poglavlja dane su smjernice za upravljanje vođenje i upravljanje dokumentacijom.

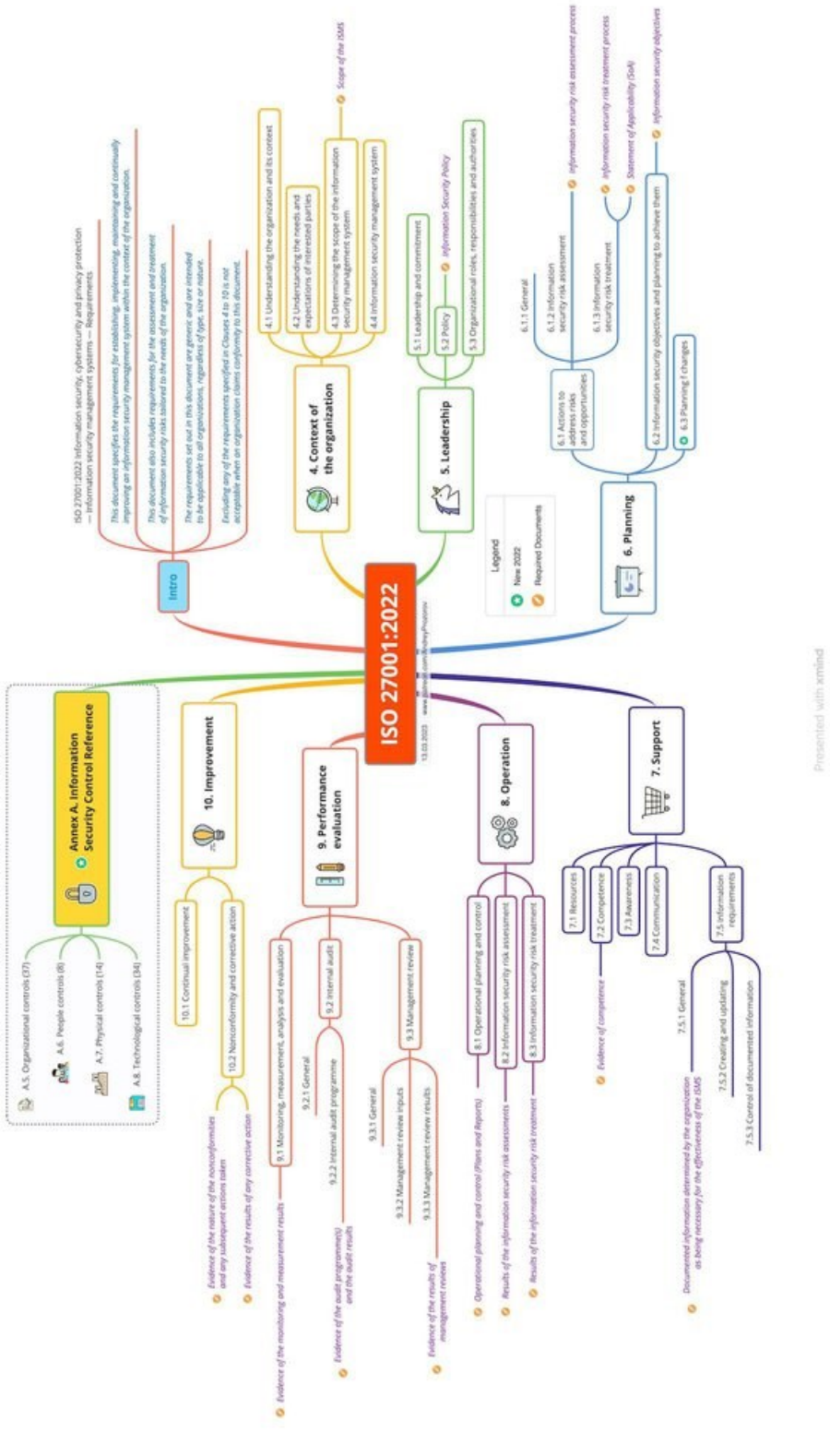
Osmo poglavlje se tiče provedbe norme. Navodi se da organizacija mora planirati, implementirati i nadzirati procese potrebne kako bi se ispunili zahtjevi i kako bi se implementirale radnje vezane uz otklanjanje rizika. Zahtjeva se od organizacija da provode procjenu rizika informacijske sigurnosti u planiranim intervalima ili kad se dogode ili predlože značajne promjene, pritom uzimajući u obzir kriterije rizika (iz šestog poglavlja). Organizacija mora implementirati plan otklanjanja rizika i sačuvati dokumentaciju o tome.

Deveto poglavlje govori o vrednovanju performansi. Navedeno je da organizacija mora odrediti postupak nadzora i mjerenja, odgovorom na pitanja što, kojim metodom, kada i tko mora provesti nadzor i mjerenje. Organizacija također mora odrediti tko i kada treba analizirati i vrednovati rezultate nadzora i mjerenja. Zahtjeva se od organizacije da provodi interne procjene (eng. audit) u planiranim intervalima kako bi se utvrdilo je li njihov ISMS u skladu s njihovim zahtjevima i potrebama, te sa zahtjevima ove norme. Ukazuje se na potrebu izrade programa interne procjene O internim procjenama organizacija je dužna voditi i čuvati dokumentaciju. U tom poglavlju su također navedene smjernice za ocjenjivanje ISMS-a organizacije od strane uprave.

Konačno, deseto poglavlje govori o kontinuiranom poboljšavanju. Navodi se da organizacija mora trajno poboljšavati prikladnost, primjerenost i djelotvornost

sustava upravljanja informacijskom sigurnošću. Dane su smjernice za postupke koje organizacija treba poduzeti ako se u ISMS-u organizacije pojavi nesukladnost.

Na samom kraju norme, u dodatku je tablica s referentnim kontrolama informacijske sigurnosti koje se mogu koristiti pri otklanjanju rizika. Kontrole su usklađene sa sadržajem navedenim u normi ISO/IEC 27002. Podijeljene su u 4 grupe: organizacijske kontrole, kontrole zaposlenika, fizičke kontrole i tehnološke kontrole.



Slika 4. Sadržaj norme (Aikido, n.d.)

3.3. Ostale norme serije 27000

ISO/IEC 27001 je član serije normi ISO 27000 (često se može vidjeti naziv ISO 27K). koja ima oko 63 objavljenih normi, ali samo norma ISO/IEC 27001 može organizaciji donijeti certifikat. Sve te norme pružaju smjernice za implementaciju kontrola za upravljanje informacijskom sigurnošću. No, ono što pruža samo ISO/IEC 27001 je implementacija okvira u koji se zatim smještaju te kontrole. (Junaid, 2023) Dakle, može se zaključiti da je ISO/IEC 27001 glavna norma u seriji ISO 27K, a sve ostale norme se nadopunjuju na tu, glavnu normu.

Najznačajnija „podnorma“ je zasigurno ISO/IEC 27002. Ona je zapravo neraskidivo povezana s glavnom normom još od samog početka postojanja tih dviju normi. Pa čak i prije ISO/IEC normi, sadržaj norme BS7799 je bio podijeljen na dva dijela: jedan dio je bio praktičan, a drugi je bio teoretski. Tako je i kod ISO/IEC normi: ISO/EC 27002 se nadovezuje na ISO/IEC 27001 tako što pruža praktične smjernice za uspostavljanje referentnih kontrola koje su navedene u dodatku norme ISO/IEC 27001.

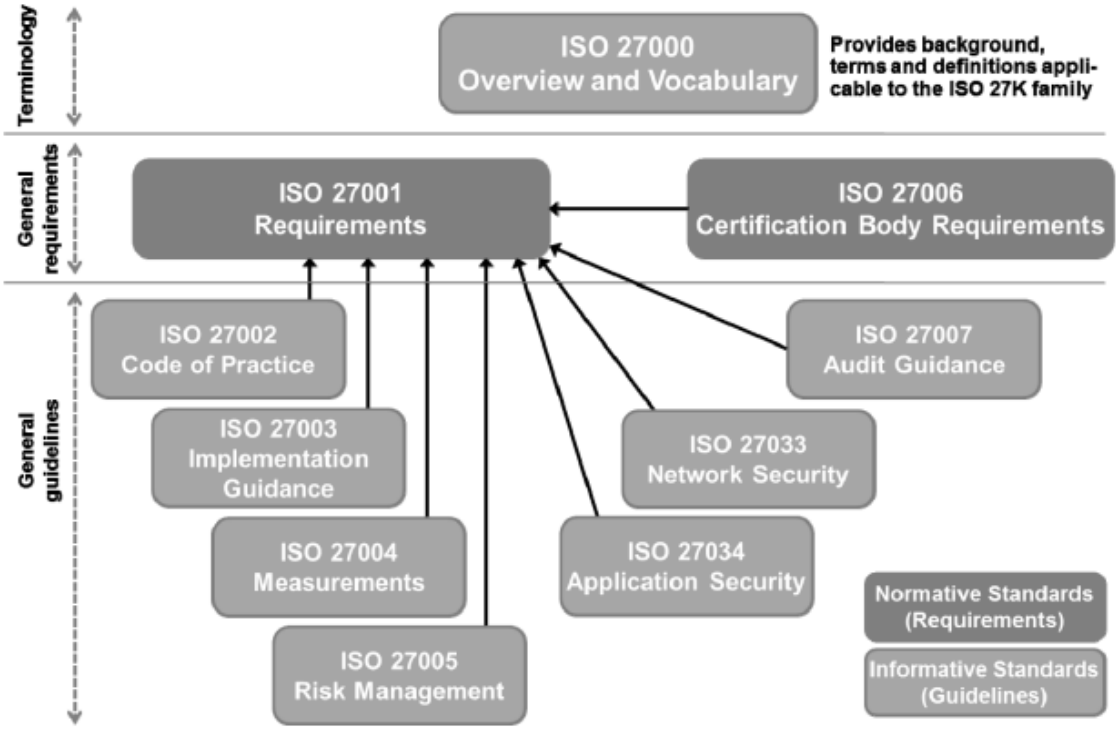
Norma ISO/IEC 27003 pruža objašnjenje i smjernice za ISO/IEC 27001. (ISO, n.d.)

Norma ISO/IEC 27004 pruža smjernice za pomoć organizacijama u evaluaciji performanse vlastite informacijske sigurnosti i učinkovitosti ISMS-a, sa željom da se ispune zahtjevi norme ISO/IEC 27001. Osim toga, ta norma služi još i za praćenje i mjerenje performanse informacijske sigurnosti, praćenje i mjerenje učinkovitosti ISMS-a (uključujući procese i kontrole ISMS-a) te za analizu i evaluaciju rezultata praćenja i mjerenja. (ISO, n.d.)

Norma ISO/IEC 27005 pruža smjernice za pomoć organizacijama pri ispunjenju zahtjeva 27001 norme (i to onih dijelova koji se tiču adresiranja rizika informacijske sigurnosti) i pri upravljanju rizicima informacijske sigurnosti, posebice pri procjeni i obradi rizika. (ISO, n.d.)

Od ostalih normi, vrijedilo bi spomenuti još nekoliko njih. Norma ISO/IEC 27006 daje zahtjeve za certifikacijska tijela. Norma ISO/IEC 27007 pruža smjernice za revizore. (Disterer, 2013) Norme ISO/IEC 27017 i ISO/IEC 27018 organizacijama daju

smjernice i kontrole za zaštitu podataka koji se pohranjuju u računalni oblak (eng. cloud). (Secureframe, 2023) Norma ISO/IEC 27032 pruža smjernice za kibernetičku sigurnost. Norma ISO/IEC 27033 se sastoji od šest dijelova te pruža smjernice za mrežnu sigurnost, a norma ISO/IEC 27034 se sastoji od pet dijelova te pruža smjernice za sigurnost aplikacija. (Disterer, 2013) Norma ISO/IEC 27035 pokriva upravljanje incidentima, odnosno pruža smjernice kako treba reagirati da se nastavi kontinuitet poslovanja u slučaju da se dogodi bilo kakvi incident. (Secureframe, 2023)



Slika 5. Najbitnije norme iz 27000 grupe (Disterer, 2013)

3.4. Relacija između norme ISO/IEC 27001 i GDPR-a

Budući da norma ISO/IEC 27001 sama po sebi nema nikakve zahtjeve za zaštitu osobnih podataka, 2019. godine je donesena (pod)norma ISO/IEC 27701 koja

propisuje zahtjeve za uspostavu, implementaciju, održavanje i kontinuirano unaprjeđivanje sustava za upravljanje privatnim informacijama (eng. PIMS - Privacy Information Management System). (ISO, n.d.) Prema organizaciji ISO, PIMS je zapravo vrsta ISMS-a koji fokus stavlja na zaštitu privatnosti. (Anwar i Gill, 2020.) Tako je ta norma ustvari ekstenzija norme koja je tema ovog rada.

Glavna zadaća PIMS-a je zaštita i kontrola osobnih podataka (eng. PII – Personally Identifiable Information), a njih se definira kao informacije koje su vezane za specifičnog pojedinca i koje mogu otkriti njegov identitet. Primjeri takvih podataka su ime, prezime, broj telefona i e-mail adresa. (IBM, n.d.) Norma ISO 27701 sadrži popis sigurnosnih kontrola vezanih uz PII, koje su podijeljene u dvije grupe: jedna grupa se odnosi na organizacije koje se bave kontrolom podataka, dok se druga grupa odnosi na organizacije koje se bave obradom podataka. (Advisera, 2019)

Kod implementacije norme ISO/IEC 27001 u organizaciju je dosta pažnje posvećeno poštovanju regulative GDPR (punim nazivom General Data Protection Regulation). To je naziv za uredbu Vijeća Europskog parlamenta o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. Cilj te uredbe je, dakle, zaštita pojedinaca i njegovih osobnih podataka te pružanje sigurnosti tvrtkama koje obrađuju osobne podatke. (Tomić Rotim, n.d.)

Kao sponu između te dvije norme možemo shvatiti upravo normu ISO/IEC 27701, iako se ona i GDPR razlikuju u nekoliko točaka. Prije svega, osnovna razlika je u njihovoj namjeni. Tako je ISO/IEC 27701 norma koja organizacijama daje smjernice kako poboljšati vlastitu poslovnu praksu i stoga je usmjerena na zaštitu privatnosti unutar organizacije i poslovnih operacija koje ona obavlja. Ta norma se bavi zaštitom privatnih podataka od raznih rizika, tako što nalaže organizacijama da određenim dokumentima, koji sadrže osobne i privatne podatke, osiguraju potrebnu razinu povjerljivosti i integriteta te da ograniče dostupnost takvim podacima. (Anwar i Gill, 2020.) S druge strane, GDPR je usmjeren na zaštitu pojedinca u svim područjima njegovog djelovanja pa je prema tome fokus stavljen na prava i slobodu pojedinca u vezi s upravljanjem njegovim osobnim podacima. (Anwar i Gill, 2020.) I dok je ISO/IEC 27701 usmjerena na svaku organizaciju pojedinačno i na specifične uvjete

koji su prisutni u toj organizaciji, GDPR osigurava jednaku razinu zaštite svakom pojedincu iz Europske unije. (Tomić Rotim, n.d.) Prema tome, GDPR se odnosi na sve pravne osobe koje posluju u Europskoj uniji ili obrađuju osobne podatke građana u Europskoj uniji, što uključuje voditelje i izvršitelje obrade osobnih podataka. U konačnici, GDPR obuhvaća sve javne institucije, urede i agencije, te sve tvrtke (i privatne obrte) koje obrađuju osobne podatke u bilo kojem opsegu i količini, bez obzira na lokaciju sjedišta. (Tomić Rotim, n.d.)

Iako se razlikuju u osnovnoj namijeni te vrsti i opsegu svojih (u slučaju norme ISO/IEC 27701, potencijalnih) obveznika razlikuju, ISO/IEC 27701 i GDPR imaju i neke dodirne točke. Tako obje norme zahtijevaju od organizacija da definiraju svoje uloge kao nekoga tko posjeduje nečije privatne informacije. Pritom trebaju razmotriti utjecaj unutarnjih i vanjskih faktora, kao što su neke posebne regulacije privatnosti ili pak zahtjevi ugovora o radu. Osim toga, obje norme daju smjernice, odnosno zahtjeve koji pobliže definiraju i objašnjavaju pojedinačne uloge i načine na koje provesti određene procese. Te smjernice (kod ISO/IEC 27701) i zahtjevi (kod GDPR) se dosta podudaraju. (Anwar i Gill, 2020.)

Zaključno za normu ISO/IEC 27701, odnosno za vezu norme ISO/IEC 27001 i GDPR-a može se reći da ISO/EC norma ne zadovoljava zahtjeve GDPR-a u potpunosti, no njezinom implementacijom organizacija stječe dobre temelje za poštovanje regulative GDPR koja je u biti zakonski okvir i zbog toga ga organizacije imaju obvezu poštovati, tj. biti usklađene s njegovim odredbama. (Secureframe, 2023)

4. Implementacija norme

Proces implementacije obuhvaća niz koraka koji sežu od inicijalne procjene rizika do postavljanja i održavanja kontrola kako bi se zaštitili povjerljivost, integritet i dostupnost informacija. Ti koraci se mogu podijeliti u četiri faze. Tako dobivamo PDCA (plan-do-check-act) model.

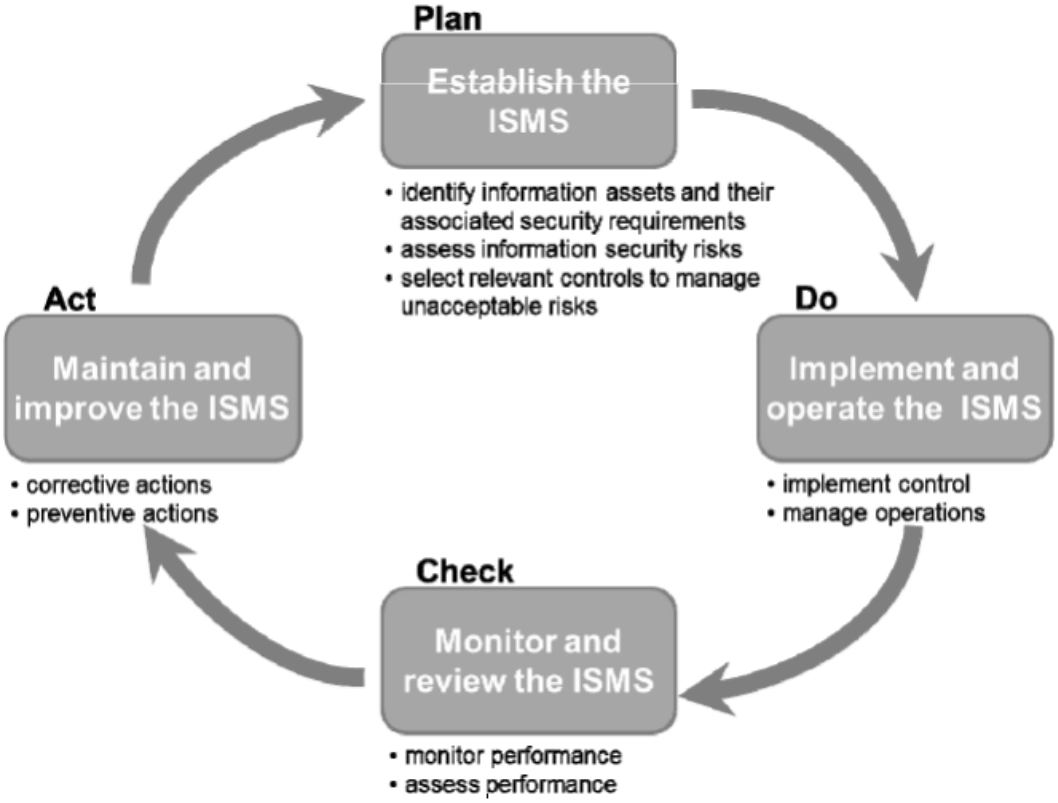
ISO/IEC 27001 zahtjeva strukturiran pristup uspostavljanju ISMS-a. To čini prvu fazu implementacije – planiranje. To je ustvari pripremna faza koja se provodi u šest koraka. Najprije se definira opseg ISMS-a kojeg organizacija želi implementirati. Zatim se definira politika informacijske sigurnosti. Slijedeći korak je provođenje procjene rizika da bi identificirali, unutar konteksta politike i opsega ISMS-a, važna informacijska sredstva organizacije i rizike koji im prijete. Nakon toga slijedi identificiranje i procjena opcija za otklanjanje ovih rizika odabirom, gdje je to potrebno, ciljeva i kontrola koje treba provesti. Naposlijetku, zadnji korak je priprema izjava o primjenjivosti. (Calder, 2008)

Kada su ti koraci izvršeni, onda tek možemo započeti s implementacijom, odnosno s „do“ fazom. Ta faza se sastoji od pet koraka. Prvi korak je izrada plana obrade rizika i dokumentacije, uključujući planirane procese i svu potrebnu popratnu dokumentaciju. Slijedeći korak je provedba plana obrade rizika i planiranih kontrola. Nakon toga slijedi odgovarajuća obuka zaposlenika te programi za podizanje svijesti među zaposlenima. Četvrti korak je upravljanje poslovima i resursima u skladu sa ISMS-om. I konačno, peti i posljednji korak je provođenje postupaka koji omogućuju promptno otkrivanje i odgovor na sigurnosne incidente. (Calder, 2008)

Nakon implementacije se radi provjera (check) i to je samo jedan korak koji uključuje praćenje, pregled, testiranje i reviziju. Međutim, to je kontinuirani proces koji mora obuhvatiti cijeli sustav. Prilikom dodjele certifikata, certifikacijsko tijelo će tražiti dokaze o barem jednom skupu testova i revizija na ISMS-u koji su izvršeni prije posjete certifikatora. (Calder, 2008)

Posljednja faza je faza djelovanja (act). U toj fazi je potrebno pregledati rezultate testiranja i revizije, kao i to treba li ISMS poboljšati u svjetlu promjenjivog okruženja

rizika, tehnologije ili drugih okolnosti. Slijede stalni pregledi, daljnje testiranje i kontinuirano poboljšanje. (Calder, 2008)



Slika 6. PDCA model (Disterer, 2013)

4.1. Certifikacija

ISMS organizacije je uspješno implementiran tek kad certifikacijsko tijelo utvrdi da je sve u redu, odnosno da je sve u skladu s normom ISO/IEC 27001. Kao potvrdu toga, organizaciji je uručen certifikat. Proces certifikacije je podijeljen na dva koraka, odnosno na dvije revizije. (Disterer, 2013)

Prva revizija uključuje pregled svih dokumenata koji se tiču implementacije ISMS-a. Primjerice, oni mogu biti o politici informacijske sigurnosti koju organizacija provodi ili o dokumentiranim procesima koji su se dogodili prilikom implementacije norme. Te dokumente dolazi pregledati revizor koji ih zatim šalje certifikacijskoj organizaciji

koja još jednom pregledava i provjerava te dokumente. Ta prva revizija je ustvari priprema za glavnu reviziju, koja može trajati i po nekoliko dana. (Disterer, 2013)

Drugi dio certifikacije, odnosno druga i glavna revizija se sastoji od intervjua sa svim odgovornim osobama u organizaciji. U tim intervjuima revizori provjeravaju njihovo razumijevanje sigurnosne politike organizacije. Navodi ih se da opisuju procese i prisutne detalje s kojima su se susreli prilikom implementacije norme, te raspravljaju s njim o manjkavostima njihovog sustava te o mogućem poboljšanju. (Disterer, 2013)

Nakon što se analiziraju rezultati intervjua, donosi se konačna odluka. Pozitivna odluka rezultira tima da organizacija dobi certifikat kao dokaz da je njihov ISMS usklađen sa zahtjevima ISO/IEC 27001 norme. Negativna odluka znači da organizacija ponovno mora proći proces implementacije ISMS-a. (Disterer, 2013)

Certifikat vrijedi tri godine. Nakon isteka valjanosti certifikata može se provesti recertifikacija koja iziskuje manji napor nego početna certifikacija. Osim toga, certifikacijsko tijelo provodi praćenje napretka na godišnjoj razini. Prva takva provjera mora biti barem 12 mjeseci poslije izdavanja certifikata. Ako se u takvim provjerama primijete ozbiljne devijacije i kršenja norme, certifikacijsko tijelo može suspendirati ili čak poništiti certifikat, koji se može dobiti natrag tek dok se uočene devijacije poprave. (Disterer, 2013)

4.2. Dobrobiti primjene norme ISO/IEC 27001

Postoji niz izravnih, praktičnih razloga za provedbu politike informacijske sigurnosti i implementaciju ISMS-a. Certifikat govori postojećim i potencijalnim klijentima da je organizacija definirala i postavila učinkovite procese informacijske sigurnosti, čime se pomaže stvoriti odnos povjerenja. Proces certifikacije također pomaže organizacijama usredotočiti se na kontinuirano poboljšanje procesa svoje informacijske sigurnosti. Naravno, prije svega certifikacija, te redoviti vanjski pregled o čemu ovisi stalna certifikacija, osigurava da organizacija zadrži svoj sustav informacijske sigurnosti od kad je postavljen. Većina informacijskih sustava nije od samog početka dizajnirana da bude sigurna. Tehničke sigurnosne mjere ograničene

su u svojoj sposobnosti zaštite informacijskih sustava. Sustavi upravljanja i proceduralne kontrole su bitne komponente svakog zaista sigurnog informacijskog sustava i, da bi bili učinkoviti, potrebno je pažljivo planiranje i posvećenost detaljima. (Calder, 2008)

Implementacija ISO 27001 standarda predstavlja sveobuhvatan pristup osiguravanju sigurnosti informacijskih sustava unutar organizacije, smanjenje rizika od sigurnosnih incidenata, usklađenost s regulativama te jačanje povjerenja klijenata. To su sve ključne prednosti koje doprinose dugoročnom uspjehu i održivosti poslovanja.

Pridržavanje ISO 27001 standarda postaje sve važnije u doba sveprisutne informacijske tehnologije i povezanosti, gdje organizacije suočavaju s rizicima sve sofisticiranijih kibernetičkih napada i prijetnji informacijskoj sigurnosti.

Različiti izvori navode različite dobrobiti uvođenja ISO/IEC 27001 norme. ISO na svojoj službenoj internetskoj stranici (ISO, n.d.) navodi slijedeće dobrobiti i razloge implementacije norme:

- smanjenje ranjivosti na rastuću prijetnju kibernetičkih napada,
- odgovor na sve veće sigurnosne rizike,
- osiguranje da sredstva kao što su financijska izvješća, intelektualno vlasništvo, podaci o zaposlenicima i informacije povjerene trećim stranama ostanu neoštećene, povjerljive i dostupne prema potrebi,
- omogućavanje centralno upravljanog okvira koji osigurava sve informacije na jednom mjestu,
- priprema ljudi, procesa i tehnologije u cijeloj organizaciji za suočavanje s tehnološkim rizicima i drugim prijetnjama,
- zaštita informacija u svim oblicima, uključujući papirnate podatke, podatke u oblaku i digitalne podatke,
- ušteda novca povećanjem učinkovitosti i smanjenjem troškova za neučinkovitu obrambenu tehnologiju.

Gledano s marketinške strane, implementacija ISO/IEC 27001 norme može (osim uštede novca povećanjem učinkovitosti i smanjenjem troškova za neučinkovitu obrambenu tehnologiju) pridonijeti boljem pozicioniranju u odnosu na konkurenciju, smanjenju troškova poslovanja zbog prevencije reklamacija i ostalih incidentnih situacija, smanjenju financijskih gubitaka te jačem povjerenju klijenata i poslovnih partnera.

5. Studija slučaja – uvođenje norme ISO/IEC 27001 u organizaciju

5.1. Osnovne informacije o organizaciji

Uniplus d.o.o. iz Čakovca bavi se razvojem, implementacijom i održavanjem programskih rješenja za različite oblike poslovanja, namijenjenih malim, srednjim i velikim tvrtkama. Osnovan je 1993. godine. Trenutno zapošljava 11 djelatnika.

U posljednjih nekoliko godina pretežito se bave programskim rješenjima za upravljanje ljudskim potencijalima. Budući da programska rješenja sadrže i obrađuju kritične i osjetljive podatke o djelatnicima njihovih klijenata, posebnu pažnju posvećuju zakonskim odredbama i zaštiti podataka. Temeljem poslovnih potreba za unaprjeđenje sigurnosti, odlučili su uskladiti svoje poslovanje sa zahtjevima norme ISO/IEC 27001.

U daljnjem tekstu opisat će se postupci koje je organizacija provela kako bi se uskladila s normom i dobila pripadajući certifikat.

5.2. Aktivnosti za uvođenje norme

Temeljem poslovnih potreba uprava organizacije je sredinom 2023. donijela odluku o uvođenju norme. Slijedeći korak bio je angažiranje konzultanta koji će ih voditi u tom procesu. Proces je otpočeo u studenom 2023., a predviđeni rok za dobivanje certifikata bio je šest do devet mjeseci.

Konzultant je na početku napravio snimku trenutnog stanja i analizu razine usklađenosti sa zahtjevima norme. Rezultat toga procesa je GAP analiza koja je po svim područjima norme ukazala što Uniplus treba napraviti i koje procese prilagoditi kako bi se uskladio sa zahtjevima norme, te na taj način unaprijedio poslovne procese u cilju povećanja sigurnosti podataka i računalnih sustava.

Uslijedilo je nekoliko mjeseci u kojima je Uniplus radio na prilagodbi i dokumentiranju ključnih poslovnih procesa, edukaciji djelatnika, doradama programskih rješenja i uvođenju novih praksi u svakodnevni rad. U tom procesu bili su u stalnom kontaktu s konzultantom, te zajedno s njime putem radionica i sastanaka online i uživo, preispitivali pojedine teme, raspravljali o mogućim rješenjima, prezentirali mu odrađeno i dogovarali daljnje aktivnosti. Konzultant je u nekoliko navrata odradio procjenu s ciljem presjeka trenutnog stanja projekta.

Taj proces rezultirao je dokumentima kojima se definiraju poslovni procesi, poslovnim praksama koje se svakodnevno primjenjuju i ciljevima za unaprjeđenja u budućem razdoblju.

U trenutku kad su Uniplus i konzultant utvrdili da su poslovne prakse u dovoljnoj mjeri usklađene sa zahtjevima norme, zatražena je formalna procjena odnosno pregled ovlaštene certifikacijske kuće.

5.2.1. GAP analiza

Spomenuto jeda je konzultant pri svom prvom posjetu Uniplusu napravio takozvanu GAP analizu. To je metoda procjene performansi (odnosno rada i njegovog rezultata) neke organizacije ili organizacijske jedinice čiji je cilj odrediti jesu li neki zahtjevi (u ovom slučaju regulatorni zahtjevi) zadovoljeni i na čemu treba poraditi ako nisu. (TechTarget, n.d.) Konzultant je, dakle, u Uniplusu analizirao trenutno stanje i na temelju te analize je napravio procjenu usklađenosti sa zahtjevima norme. Sama analiza je koncipirana u četiri grupe: fizičke kontrole, kontrole zaposlenika, organizacijske kontrole i tehnološke kontrole. Te kontrole su ustvari sadržane u popisu na samom kraju norme, u dijelu Annex A.

Konzultant je konačni rezultat GAP analize pripremio u obliku Excel tablice, u kojoj je pobrojao sve te kontrole, te je za svaku kontrolu naveo njezin naziv, njezin zahtjev u normi, nalaz toga što je u Uniplusu već pokriveno i prijedloge za poboljšanje. Za kontrole za koje je konzultant utvrdio da su usklađene s normom, u rezultatima analize je to navedeno pa tako za te točke nisu dani daljnji prijedlozi za poboljšanje.

Uzmimo za primjer kontrolu A8.28. To je tehnološka kontrola koja nosi naziv „Sigurno programiranje“ i njezin zahtjev je da načela sigurnog programiranja moraju biti primijenjena na razvoj softvera. Nalaz konzultanta je da Uniplus nije imao formalizirana interna pravila za sigurnosno kodiranje, a prijedlog za poboljšanje je standardiziranje izrade programskog koda uz korištenje OWASP i NIST standarda za kodiranje.

Kao primjer zadovoljene kontrole može se uzeti kontrola A6.7, iz grupe kontrole zaposlenika. Ta kontrola nosi naziv „Rad na daljinu“ i ona zahtjeva da kada osoblje radi na daljinu, sigurnosne mjere se moraju primijeniti kako bi se zaštitile informacije kojima se pristupa, koje se obrađuju ili koje se pohranjuju izvan prostorija organizacije. Ta kontrola je zadovoljena na način da je zaposlenicima tvrtke koji rade na daljinu omogućen i dozvoljen rad na opremi koja je u vlasništvu organizacije. Stoga nije bilo potrebe za daljnjim unaprjeđenjima.

5.2.2. Dokumentacija

Kako su rezultati GAP analize pokazali nedostatke na putu do dobivanja željenog ISO certifikata, odnosno neusklađenosti s normom, Uniplus je morao poduzeti određene radnje kako bi uskladio vlastite poslovne prakse sa zahtjevima norme. Cilj ovog djela rada je pokušati pobliže opisati taj proces i koje je sve poteze potrebno povući da bi se on ispravno izvršio. Najprije će se prikazati sve promjene koje je bilo potrebno napraviti u području dokumentacije i dokumentiranja raznih aktivnosti.

Uniplus je tako dobio obavezu izraditi temeljne dokumente koje norma sama po sebi zahtjeva, a koji prije u tvrtki nisu postojali. Prije svega to je dokument „Odluka o imenovanju Voditelja informacijske sigurnosti/CISO“ (eng. chief information security officer) u kojem su se ujedno i definirale ovlasti i odgovornosti te osobe. Zatim je bilo potrebno kreirati dokument „Politika sustava upravljanja informacijskom sigurnošću“, a nakon toga i dokumente „Upravljanje sigurnosnim slabostima i incidentima“, te „Upravljanje rizicima“.

Nakon toga, bilo je potrebno kreirati i specifične dokumente koji su vezani za poslovanje tvrtke. Prema tome, morali su izraditi skicu, tj. model svoje mrežne infrastrukture, te u istom dokumentu prikazati prostorni raspored računala i ostalih uređaja, uključujući i antivirusnu zaštitu radi prikaza trenutnog stanja u tvrtki. Taj dokument je potrebno ažurirati ukoliko se dogode kakve promjene. S obzirom da je glavna djelatnost Uniplusa projektiranje i razvoj programskih rješenja, bilo je potrebno izraditi dokument vezan uz siguran razvoj programskih rješenja. U njemu je trebalo navesti postupke i pravila kojih se programski inženjeri moraju pridržavati u postupku programiranja.

Osim toga, postojali su i određeni dokumenti koje je Uniplus već imao izrađene, no oni nisu zadovoljavali zahtjeve norme. U takve dokumente su spadali ugovori o radu. Njih je trebalo uskladiti s trenutno važećim Zakonom o radu, bilo je potrebno uskladiti ih s GDPR-om (trebalo je dodati uredbe GDPR-a vezane uz tajnost i povjerljivost osobnih podataka), te je bilo potrebno dodati uredbe vezane uz autorska prava i intelektualno vlasništvo.

Osim ugovora o radu, na sličan način je trebalo promijeniti dokumente vezane uz sklapanje poslova s poslovnim partnerima, u što spadaju kupoprodajni ugovori, ugovori o najmu i održavanju programskih rješenja te razne ponude. Tako je i u tim dokumentima bilo potrebno dodati GDPR odredbe, te je trebalo ugraditi odredbe vezane uz siguran razvoj i razdvajanje razvojne, testne i produkcijske okoline.

5.2.3. Unaprjeđenje sigurnosti podataka unutar programskih rješenja

Slijedeća kategorija su programska rješenja. U nastavku se navode elementi koje je Uniplus trebao promijeniti ili poboljšati u izradi svojih proizvoda da se uskladi s normom za sigurnost informacija.

U svoju testnu i razvojnu okolinu su trebali ugraditi maskiranje podataka (eng. data masking). To je proces skrivanja podataka na način da se modificiraju znakovi (slova i brojke) koji čine podatak. Tako se zapravo stvara lažna verzija podataka. No, ta lažna verzija mora biti jednako realistična kao i originalna verzija (samo iskrivljenog

sadržaja), kako bi se dobio dojam da su ti podaci stvarni. Jednom kad su podaci maskirani, originalni zapis je jedino vidljiv u originalnoj bazi podataka kojoj može pristupiti isključivo stvaratelj tih podataka. (Amazon Web Services, n.d.)

Dio kritičnih podataka koji se evidentiraju putem programskih rješenja bilo je potrebno dodatno zaštititi kriptiranjem. Kriptiranje je metoda zaštite podataka koja pretvara podatke u šifru ili kod. Taj kod može se pročitati samo posredstvom tajnog ključa ili lozinke. (Cloudian, n.d.)

Uniplus kriptira kritične podatke unutar vlastite baze podataka. Pri tome slijedi slijedeće principe: šifriranje svih povjerljivih podataka koristeći snažne kriptografske tehnike, upotreba snažnih kriptografskih algoritama s dovoljno dugim ključem (npr. FIPS algoritmi), te šifriranje korisničkih lozinki pomoću ireverzibilnih algoritama (npr. bcrypt).

Također, u Uniplusu su trebali unaprijediti logiranje korisničkih aktivnosti. To je postupak kojim program tijekom rada aktivnosti korisnika i evidentira ključne akcije korisnika (na primjer: prijava, odjava, unos podataka, izmjena i brisanje podataka).

5.2.4. Evidencija ciljeva i repetitivnih aktivnosti

Na temelju nalaza GAP analize Uniplus je definirao ciljeve za poboljšanja sigurnosti. Ti ciljevi su evidentirani unutar Uniplusovog programskog rješenja, te se definiraju osobe koje će na tom cilju raditi, prioritet izvršavanja ciljeva i rokovi do kada bi se ciljevi trebali izvršiti. Tijekom unaprjeđenja uključene osobe evidentiraju aktivnosti koje su poduzele za postizanje cilja. Cilj se može pratiti kroz određene statuse: od stvaranja novog cilja preko realizacije pa sve do završetka. Odgovorna osoba na kraju provjerava je li cilj postignut te daje konačan zaključak. Neki ciljevi su realizirani u tijeku prilagodbe normi, a neki su evidentirani i planiraju se riješiti u narednom razdoblju.

Novi | Preuzet | Realiziran | Završen bez obračuna

Broj naloga	Prioritet	Datum prijave	Rok izvršenja	Partner	Stranka	Nositelj	Suradnici	Zahtjev	Opis	Dokumenti	Ukupno sati	
RN2401440		15.03.2024.		Uniplus d.o.o.				Unaprjeđenje sigurnosti podataka vezanih uz konekcije prema poslovnim partnerima i ostalim vanjskim servisima: kriptiranje podataka, omogućavanje prikaza određenim korisnicima kojima su dodijeljene ovlasti, omogućavanje prikaza podataka na zahtjev i uz potvrdu autentifikacije. Priprema programskog rješenja, uređenje podataka.			27:00	▸ …
RN2401409		09.02.2024.	09.02.2024.	Uniplus d.o.o.				Otklanjanje problema sa DNS resolvingom produkcija.uniplus.local dok je VPN konekcija aktivna.	Analiza problema, apliciranje rješenja po računalima.		1:00	▸ …
RN2401396		26.01.2024.	15.02.2024.	Uniplus d.o.o.				Prebacivanje produkcijskog Uniplus programskog rješenja osobnaStranica s interneta na intranet.			2:10	▸ …
RN2401389		17.01.2024.	31.01.2024.	Uniplus d.o.o.				Isključenje mobilnih telefona iz UWInt mreže i prebacivanje na guest WiFi mrežu. Pomoć i provjera postavki na telefonima djelatnika.	Provjera mobilnih uređaja od zaposlenika i pomoć oko spajanja na novu Uniplus "guest" mrežu.		1:00	▸ …
RN2401403	5 - Srednji prioritet	15.01.2024.	14.02.2024.	Uniplus d.o.o.				Povećanje sigurnosti Uniplus web aplikacija.	Zaprimljeni rezultati penetracijskih testova. Analiza dobivenog dokumenta, rješavanje ranjivosti aplikacija, unaprjeđenje aplikacija sa sigurnosnim zakrpama. Nakon unaprijeđenja sustava prema točkama, provođenje internih penetracijskih testova aplikacija pomoću alata OWASP ZAP. Implementacija zakrpa na javljena upozorenja prema rezultatima penetracijskog testa.		91:11	▸ …
RN2401381		11.01.2024.	15.01.2024.	Uniplus d.o.o.				Postavljanje lozinki na sva računala zaposlenika (operativne sustave).	Postavljanje lozinki na sva računala zaposlenika (operativne sustave), napomena za kompleksnost lozinka. Provjera da li su lozinke postavljene na sva računala djelatnika.		2:00	▸ …
RN2401382		11.01.2024.	31.01.2024.	Uniplus d.o.o.				Evidencija osposobljavanja djelatnika.	Evidencija osposobljavanja djelatnika. Prilaganje popratnih dokumenata (uvjerenja, potvrde...).		5:05	▸ …

Slika 7. Evidencija ciljeva za poboljšanje sigurnosti

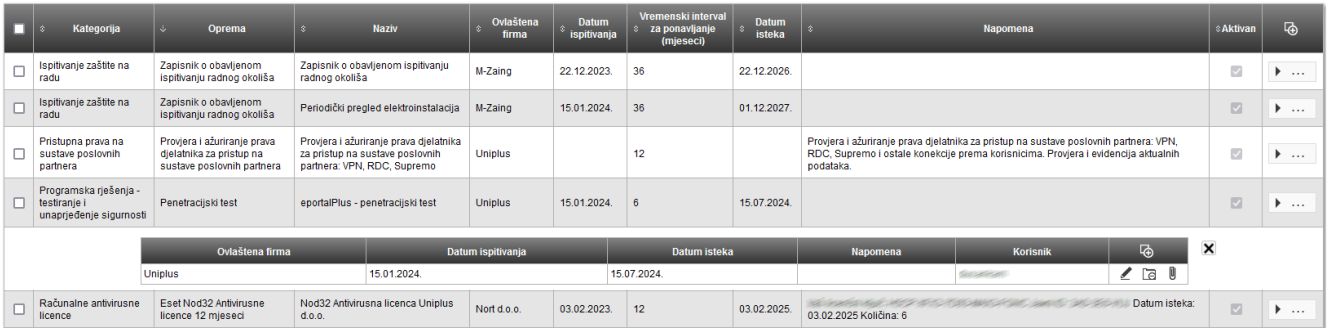
Kao primjer cilja može se uzeti unaprjeđenje sigurnosti podataka vezanih uz veze prema poslovnim partnerima, koji uključuje kriptiranje podataka i kontrolirani prikaz podataka određenim korisnicima (prvi redak u tablici prikazanoj na slici 7).

Na slici 8 prikazane su pojedine aktivnosti vezane uz realizaciju toga cilja.

Stavka	Opis / Naziv	Vrijeme početka	Vrijeme završetka	Broj suradnika	Ukupno sati	Lokacija	Suradnik	Korisnik	Unos	Izmjena	
1	Kriptiranje podataka za korisnika (poslovni partner) i podataka za vezu. Za kriptiranje se koristi AES algoritam.	05.04.2024. 08:00	05.04.2024. 16:00	1	08:00				11.04.2024.	11.04.2024.	▸ …
2	Dodavanje dodatne autentifikacije na dohvat osjetljivih podataka unutar modula Korisnici, Veze i Intervencije	08.04.2024. 10:00	08.04.2024. 16:00	1	06:00				11.04.2024.	11.04.2024.	▸ …
3	Dodavanje dodatne autentifikacije na dohvat osjetljivih podataka unutar modula Korisnici, Veze i Intervencije.	09.04.2024. 10:00	09.04.2024. 16:00	1	06:00				11.04.2024.	11.04.2024.	▸ …
4	Izmjena meni-a. Vrste dokumenata, poslovni partnerni i veze preseljeni u meni Opći podaci. Intervencije i radni nalozi grupirani unutar meni-a Intervencije i radni nalozi. Pregled Korisnici preimenovan u Poslovni partneri, termin Korisnik preimenovan u Poslovni partner na svim pregledima koji su ga koristili.	10.04.2024. 10:00	10.04.2024. 12:00	1	02:00				11.04.2024.	11.04.2024.	▸ …
5	Uređenje veza za	12.04.2024. 13:00	12.04.2024. 13:30	1	00:30				12.04.2024.		▸ …
6	Uvedene arhivske tabele za poslovne partner i veze koje se pune kod novog unosa i kod izmjene. Kod veza uvedeno novo polje za korisnika koji je prvotno unio tu vezu. Taj korisnik se smatra vlasnikom veze i samo taj korisnik može dodjeljivati tu vezu drugim korisnicima za prikaz. Kad je veza dodjeljena korisniku, taj korisnik može dohvatiti i izmjeniti vezu. Ne može je izbrisati.	19.04.2024. 10:00	19.04.2024. 12:00	1	02:00				22.04.2024.		▸ …
7	Kod enkriptiranja / dekriptiranja osjetljivih podataka, dodano eksplicitno čitanje / pisanje podataka u UTF-8 encodingu. S eksplicitnim postavljanjem encoding-a se osigurava da su podaci uvijek u istom encoding-u i da encoding podataka ne ovisi o encoding-u postavljenome na serveru.	16.05.2024. 13:00	16.05.2024. 15:00	1	02:00				20.05.2024.		▸ …
8	Svi dogovoreni mehanizmi zaštite podataka su implementirani.	20.05.2024. 13:30	20.05.2024. 14:00	1	00:30				20.05.2024.		▸ …
	Ukupno:				**27:00**						

Slika 8. Aktivnosti vezane uz ostvarenje jednog cilja

Neke aktivnosti na unaprjeđenjima poslovnih procesa se trebaju provoditi repetitivno, u zadanim razdobljima (slika 9). Takve aktivnosti također se evidentiraju unutar Uniplusovog programskog rješenja te približavanjem predviđenog roka za obavljanje aktivnosti odgovorne osobe dobivaju automatski podsjetnik. Na temelju podsjetnika se kreira novi cilj (postupak opisan iznad) i prate se aktivnosti na realizaciji.



Slika 9. Repetitivne aktivnosti

Kao primjer repetitivne aktivnosti može se uzeti provođenje penetracijskih testova svakih šest mjeseci, obnavljanje antivirusne licence svakih dvanaest mjeseci i sl.

5.2.5. Evidencija imovine i zaduženja djelatnika

U postupku pripreme za certifikaciju bilo je potrebno evidentirati svu imovinu, posebice onu koja sadrži memoriju, odnosno onu koja sadrži neke podatke. Djelatnike je trebalo zadužiti za imovinu koja im je dana na korištenje u svrhu obavljanja djelatnosti, a trebalo je zadužiti i odgovorne osobe za imovinu koju koristi više djelatnika ili na kojoj se odvijaju bitni procesi (npr. pisači, poslužitelji, i sl.) (slika 10). Djelatnike je također trebalo zadužiti i za nematerijalna prava, kao što su pristupi određenim resursima tvrtke (npr. poslužiteljima ili ključevima i pinovima za pristup poslovnom prostoru) (slika 11).

Aktivan	Podkategorija	Marka	Model	Datum garancije	Status	
☑	Sustav protuprovalne zaštite	Ajax	HUB 2		Zadužen	▸ …
☑	Poslužitelj	Debian 6.0.9	Debian			▸ …
☑	Računala	Dell	Inspiron		Zadužen	▸ …
☑	Računala	Dell	Inspiron		Zadužen	▸ …
☑	Računala	Dell	Optiplex 3080		Zadužen	▸ …
☑	Računala	Dell	Vostro 3510		Zadužen	▸ …
☑	Računala	Dell	Vostro 5620		Zadužen	▸ …
☑	Računala	Dell	Vostro 5620		Zadužen	▸ …
☑	Računala	HP	470 G10	21.03.2027.	Zadužen	▸ …
☑	Mrežna oprema	HP	HP 1920s			▸ …
☑	Mrežna oprema	HP	JH296A			▸ …
☑	Računala	HP	Probook 430 G5		Zadužen	▸ …
☑	Računala	HP	Probook 470 G8		Zadužen	▸ …
☑	Poslužitelj	Intel	Uniplus			▸ …

Slika 10. Evidencija imovine

Oznaka	Naziv	Dodatni opis	Količina	Datum	Datum isteka	Korisnik	Napomena	…
Osposobljavanja								
	Liječnički pregledi							
40082	Pregled za rad sa računalom		1.0	05.09.2022.	05.09.2025.	[redacted]		✎ 🗀 📄 🖶 📄
	Zaštita na radu							
40049	Osposobljavanje za rad na siguran način (ZOS obrazac)		1.0	04.05.2005.		[redacted]		✎ 🗀 📄 🖶 📄
	Zaštita od požara							
40087	Osposobljavanje iz zaštite od požara		1.0	04.05.2005.		[redacted]		✎ 🗀 📄 🖶 📄
Pristup								
	OpenVPN pristup mreži Uniplusa							
50003	OpenVPN pristup	OpenVPN pristup	1.0	31.05.2024.	30.11.2024.	[redacted]	Lozinka se mora mijenjati svakih 6 mjeseci	✎ 🗀 📄 🖶 📄
	Uniplus Ajax ulazni PIN							
50000	AJAX pin	PIN za isključenje/uključenje alarma	1.0	01.07.2023.		[redacted]	PIN za isključenje/uključenje alarma	✎ 🗀 📄 🖶 📄
50001	Ključ ulaznih vrata Uniplus		1.0	01.05.2023.		[redacted]		✎ 🗀 📄 🖶 📄
Sim kartice								
	SIM kartice mobilnih uređaja							
70000	T-Mobile +385981715981		1.0	02.09.2004.		[redacted]		✎ 🗀 📄 🖶 📄
Uređaji								
	Mobilni uređaji							
20067	Samsung S22		1.0	15.02.2024.		[redacted]		✎ 🗀 📄 🖶 📄
	Prijenosna memorija							
20084	Sandisk 128GB		1.0	23.02.2024.		[redacted]		✎ 🗀 📄 🖶 📄
	Računala							
20022	Lenovo Thinkbook		1.0	25.10.2021.		[redacted]		✎ 🗀 📄 🖶 📄

Slika 11. Evidencija zaduženja djelatnika

5.2.6. Promjene u mrežnoj i računalnoj infrastrukturi

GAP analiza je pokazala da je potrebno napraviti određene prilagodbe na mrežnoj i računalnoj infrastrukturi. Konkretno, bilo je potrebno dodatno urediti izradu sigurnosnih kopija (eng. backup) sistemskih logova servera, kriptiranje sigurnosnih kopija, uređenje procesa provjere izrađenih sigurnosnih kopija, uspostava nadzora web prometa kako bi se prevenirali pokušaji malicioznih pristupa, odvajanje WiFi-a za goste i sl.

5.2.7. Fizička sigurnost

S ciljem približavanja zahtjevima norme, javila se potreba za dodatnom fizičkom zaštitom prostora i opreme Uniplusa. Uz postojeće mjere zaštite poslovnog prostora koja je uključivala video nadzor i alarmni sustav bilo je potrebno dodatno urediti kontrolu pristupa na ulazu u poslovni prostor. Takva kontrola bila je potrebna zbog fizičke zaštite poslužitelja i računala koji se nalaze u poslovnom prostoru.

Jedan od ciljeva na kojem Uniplus trenutno radi je izmještanje poslužitelja u podatkovni centar (eng. dana center), tj. u računalni oblak (eng. cloud), čime bi se ublažila potreba za fizičkom sigurnošću poslovnog prostora.

5.3. Certifikacija

Nakon prilagodbe poslovnih praksi zahtjevima norme, organizacije prolaze kroz proces certifikacije. Uniplus je odabrao certifikacijsku kuću koja je ponudila svoj plan aktivnosti, koji je podijeljen u četiri koraka.

Prvi korak je planiranje i priprema. On uključuje jednodnevni sastanak u kojemu se dogovara cilj procjene, opseg i kriteriji kao i logistička pitanja koji će biti obrađeni tijekom same procjene.

Drugi korak obuhvaća pregled dokumentacije, preliminarnu provjeru i certifikaciju. Ova faza aktivnosti certifikacijske kuće ima za cilj procjenu praktične primjene sustava u organizaciji u odnosu na zahtjeve norme. Uniplus je u toj fazi dužan demonstrirati praktičnu i djelotvornu primjenu postupaka. U slučaju pozitivnog nalaza ove procjene, certifikacijska kuća izdaje certifikat o sukladnosti s normom.

Treći i četvrti korak se odnose na naknadne preglede, recertifikacije i izdavanje izvještaja na temelju tih pregleda. Ti koraci se odvijaju nakon što organizacija već jednom stekne ISO certifikat.

5.4. Osvrt uprave na uvođenje norme

U sklopu istraživanja je proveden kratki intervju s predsjednikom uprave Uniplusa s ciljem utvrđivanja motivacije, stupnja zadovoljstva i općenitog dojma vezanog uz uvođenje norme ISO/IEC 27001. U nastavku slijedi transkript intervjua.

P: *Zašto ste se odlučili na uvođenje ISO norme? Koji su bili problemi koje ste željeli riješiti?*

O: Na uvođenje norme odlučili smo se iz razloga što smo stjecanjem certifikata sebi željeli potvrditi, a našim poslovnim partnerima dodatno zajamčiti, da su naše poslovne operacije i svakodnevni rad u skladu s najboljom utvrđenom praksom.

P: *Prije prvog sastanka s konzultantom, jeste li znali nešto o normi ili ste postepeno učili?*

O: Znali smo općenito o normi i zahtjevima norme, no nismo znali kako će se zahtjevi norme praktično odraziti na naše uobičajene poslove i što ćemo sve trebati učiniti da bismo svoje poslovne operacije uskladiti sa zahtjevima norme. Nakon prvih sastanaka s konzultantom naše je uvjerenje da smo na dobrom putu samo

učvršćeno i ako je prije toga postojala bilo kakva skepsa oko smisla uvođenja norme, nakon prvih sastanaka ona je otklonjena.

P: *Jeste li u nekom trenutku shvatili da norma previše očekuje od vas? Jeste li pomislili na odustajanje od uvođenja norme zbog toga ili ste spremni na sve njezine izazove?*

O: Vjerujemo da je izbor konzultanta jako bitan za proces uvođenja norme, kao i za odnos prema normi. Konzultant koji je radio s nama je, prema našem mišljenju, odradio izvrstan posao u uvođenju norme i zajedno s nama generirao dodanu vrijednost koja je općenito unaprijedila naše poslovne operacije. Slijedom toga, kada smo počeli raditi na normi nismo razmišljali o odustajanju, već naprotiv, to je za nas postalo izazov.

P: *Je li proces uvođenja težak? Mora li se puno toga mora mijenjati?*

O: U našem se slučaju pokazalo da je naš svakodnevno posao jako dobro organiziran i u velikoj mjeri je sam po sebi usklađen s normom. Ono što je bilo potrebno dodati je standardizirano dokumentiranje poslovnih procesa, dok su sami procesi zahtijevali vrlo malo sadržajnih promjena.

P: *Koliko vremena posvećujete tom problemu? Oduzima li Vam puno energije?*

O: Posao je zahtjevan, posebno zbog toga što se odvija usporedno s uobičajenim poslovnim aktivnostima koje se ne smiju zanemariti ili zapostaviti.

P: *Što ste sve morali promijeniti? Na što najviše obraćate pažnju kod promjena (kibernetička sigurnost, fizička sigurnost, GDPR, nešto treće)?*

O: Gotovo svi segmenti poslovnih operacija moraju se sagledati kroz zahtjeve norme. Počevši od sigurnosti radnih prostora i opreme nadalje. Najviše je pažnje,

naravno, potrebno pokloniti onim aktivnostima na kojima se intenzivno radi. U našem slučaju je to siguran razvoj programskih rješenja i sigurnost podataka. To su nam bili i najveći izazovi.

P: *Što mislite, što ćete dobiti s dobivanjem certifikata? Koje dobrobiti očekujete?*

O: Prije svega želimo dobiti potvrdu da su naše poslovne operacije dobro organizirane zbog nas samih. A nakon toga želimo to pokazati i našim korisnicima. Želimo im pružiti dodatnu sigurnost i povjerenje u naša programska rješenja i poslovnu suradnju.

6. Zaključak

Norma ISO/IEC 27001 ima veliku važnost u današnjem poslovanju. Ona pomaže raznim organizacijama, bez obzira na njihovu veličinu i djelatnost kojom se bave, da na siguran i sustavan način uspostave, implementiraju, održavaju i konstantno poboljšavaju svoj sustav za upravljanje informacijskom sigurnošću. Prednosti uvođenja tog sustava pomoću norme su mnoge. Variraju od administrativnih, poput imanja odgovora na sve veće sigurnosne rizike, do onih marketinških, kao što je smanjenje financijskih gubitaka. Rezultati studije slučaja koja je provedena u sklopu rada detaljnije prikazuju proces uvođenja norme u organizaciju. Uprava organizacije koja je bila jedinica istraživanja je navela kako je osnovni motiv za uvođenje norme poboljšanje njihovih poslovnih praksi, prvo zbog njih samih, a onda i zbog povjerenja od strane njihovih klijenata. Najviše pažnje u tom procesu posvećeno je sigurnoj izradi programskih rješenja, budući da je to primarna djelatnost organizacije, a ono što je bila najveća novost u njihovoj dotadašnjoj poslovnoj praksi je standardizirano dokumentiranje poslovnih procesa.

7. Popis literature

Advisera (2019). *Relationship between ISO 27701, ISO 27001, and ISO 27002*. Preuzeto 1. lipnja 2024. https://advisera.com/27001academy/blog/2019/12/10/relationship-between-iso-27701-iso-27001-and-iso-27002/

Aikido (n.d.). *How to prepare yourself for ISO 27001:2022.* Preuzeto 31. svibnja 2024. https://www.aikido.dev/blog/iso-270012022-preparation

Amazon Web Services (n.d.). *What is Data Masking?* Preuzeto: 2. lipnja 2024. https://aws.amazon.com/what-is/data-masking/#:~:text=Data%20masking%20creates%20fake%20versions,access%20to%20the%20original%20dataset.

Anwar, M. J., & Gill, A. (2021). Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. In Australasian Conference on Information Systems 2020.

Calder, A. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Publishers.

Calder, A. (2009). *Information Security based on ISO 27001/ISO 27002*. Van Haren.

Cloudian (n.d.). *Data Encryption: The Ultimate Guide.* Preuzeto: 2. lipnja 2024. https://cloudian.com/guides/data-protection/data-encryption-the-ultimate-guide/#:~:text=Data%20encryption%20is%20a%20security,information%20is%20known%20as%20cryptography.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

DQS Zagreb (2022). Sigurnost informacijske tehnologije (IT) vs. Informacijska sigurnost - u čemu je razlika? Preuzeto 22. siječnja 2024.

https://www.dqsglobal.com/hr-hr/edukacija/blog/sigurnost-informacijske-tehnologije-it-vs.-informacijska-sigurnost-u-cemu-je-razlika

IBM (n.d.). *What is personally identifiable information (PII)?* Preuzeto 1. lipnja 2024. https://www.ibm.com/topics/pii#:~:text=What%20is%20PII%3F,email%20address%20or%20phone%20number.

International Electrotechical Commission (2024). *What we do.* Preuzeto: 24. siječnja 2024. https://www.iec.ch/what-we-do

ISO (n.d.). *ISO/IEC 27001:2022.* Preuzeto: 22. siječnja 2024. https://www.iso.org/standard/27001

ISO (n.d.) *ISO/IEC 27701:2019*. Preuzeto: 1. lipnja 2024. https://www.iso.org/standard/71670.html

Junaid, T. S. (2023). *ISO 27001: information security management systems*. Frankfurt University of Applied Sciences, Frankfurt am Main.Secureframe (2023). *ISO 27000 Series: What the Standards Are + Their Purpose.* Preuzeto 31. svibnja 2024. https://secureframe.com/blog/iso-27000

Secureframe (2023). *ISO 27001 vs ISO 27701: Key Differences and Similarities Explained*. Preuzeto: 1. lipnja 2024. https://secureframe.com/blog/iso-27001-vs-iso-27701

Secureframe (n.d.). *The History of ISO 27001*. Preuzeto: 22. siječnja 2024. https://secureframe.com/hub/iso-27001/history

TechTarget (n.d.) *gap analysis.* Preuzeto: 2. lipnja 2024. https://www.techtarget.com/searchcio/definition/gap-analysis#:~:text=A%20gap%20analysis%20is%20a,assessment%20or%20need%2Dgap%20analysis.

Tomić Rotim S. (n.d.). *Primjena Uredbe o zaštiti osobnih podataka*. Preuzeto: 1. lipnja 2024. https://www.archery.hr/wp-content/uploads/2018/11/GDPR-Prezentacija.pdf

Ured vijeća za nacionalnu sigurnost (2014) *Što je to informacijska sigurnost?* Preuzeto 22. siječnja 2024. https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost

Wikipedija (n.d.). *Međunarodna organizacija za standardizaciju*. Preuzeto 20. siječnja 2024. https://hr.wikipedia.org/wiki/Me%C4%91unarodna_organizacija_za_standardizaciju

8. Popis slika

Slika 1. Logo organizacije ISO 3

Slika 2. Logo organizacije IEC 3

Slika 3. Povijest norme ISO/IEC 27001 8

Slika 4. Sadržaj norme 12

Slika 5. Najbitnije norme iz 27000 grupe 14

Slika 6. PDCA model 18

Slika 7. Evidencija ciljeva za poboljšanje sigurnosti 27

Slika 8. Aktivnosti vezane uz ostvarenje jednog cilja 28

Slika 9. Repetitivne aktivnosti 28

Slika 10. Evidencija imovine 29

Slika 11. Evidencija zaduženja djelatnika 30

ISO/IEC 27001 – Norma za informacijsku sigurnost

Sažetak

Suvremeno društvo se često opisuje kao informacijsko društvo – društvo u kojem se informacija vrednuje kao najvrjedniji resurs, bilo kod pojedinca ili kod organizacije. U svrhu sigurnosti i zaštite informacija u poslovnom svijetu postoji međunarodna norma ISO/IEC 27001. Ta norma zahtjeva da svaka organizacija uspostavi vlastiti sustav upravljanja informacijskom sigurnošću koji se mora pridržavati norme da bi bio funkcionalan. Ovaj rad je jednim dijelom teorijski. U tom dijelu se definira informacijska sigurnost i norma ISO/IEC 27001, daje se kratak pregled povijesti nastanka norme te se navode njezine podnorme i slične norme koje mogu pomoći organizacijama u uspostavljanju sustava za upravljanje informacijskom sigurnošću. Drugi dio rada se bavi praktičnim pitanjima, odnosno načinom na koji je potrebno implementirati normu u organizaciju, procesom certifikacije te, naposlijetku, prednostima i praktičnim razlozima zbog kojih se organizacijama iz raznih područja djelovanja preporuča da implementiraju normu ISO/IEC 27001. Rad također donosi studiju slučaja koja za cilj ima istražiti kako je tekao proces uvođenja norme u konkretnu organizaciju.

Ključne riječi: sigurnost, informacije, organizacija, poslovanje, studija slučaja, ISO/IEC 27001

ISO/IEC 27001 – Information security standard

Summary

The modern society is often described as information society – society in which information is appraised as most valuable resource, either at some organization or individual. For security and protection of information asset in business world there is an international security standard ISO/IEC 27001. That standard demands of every organization to establish its own information security management system which must conform to standard in order to be functional. This thesis is theoretical in one part. In that part information security and ISO/IEC 27001 standard are defined, it gives short historical overview of the origin of the standard and the most important and the most useful sub-standards explained. Second part of the paper is more practical - it is concerned with implementation of standard in organization, with process of certification and with benefits and practical reasons recommending organizations from different fields to implement ISO/IEC 27001 standard. This thesis also discusses a case study examining the process of implementation of standard in an organization.

Key words: security, information, organization, business, case study, ISO/IEC 27001