Unaprjeđenje sigurnosti poslovnog okruženja implementacijom norme ISO 27001

Maleković, Zoran

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:151434

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-20**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Zoran Maleković

UNAPRJEĐENJE SIGURNOSTI POSLOVNOG OKRUŽENJA IMPLEMENTACIJOM NORME ISO/IEC 27001:2013

DIPLOMSKI RAD

ZAGREB, 2020.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 27. ožujka 2020.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 5919

Pristupnik: **Zoran Maleković (0246037056)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Unaprjeđenje sigurnosti poslovnog okruženja implementacijom norme ISO 27001**

Opis zadatka:

Uzimajući u obzir da je broj tvrtki u Republici Hrvatskoj sa implementiranim sustavima ISO 27001 još uvijek relativno mali, ovaj rad ima za zadatak na objektivan način i na temelju činjenica analizirati, opisati i implikacijama obrazložiti prednosti koje implementacija norme ISO 27001 može imati u pogledu osiguranja informacijske sigurnosti tvrtkama u Republici Hrvatskoj koje se odluče na njenu implementaciju u svoje poslovanje, kao i identificirati ključne kritične točke u postupku implementacije, a o kojima će u konačnici ovisiti maksimiziranje koristi od tako uspostavljenog sustava.
Ispunjavanjem tako postavljenog cilja, ovaj rad će sa stručne točke gledišta tvrtkama u Republici Hrvatskoj koje bi se na takvu implentaciju u budućnosti mogle odlučiti, služiti kao vodič i model za uspješnu implementaciju norme ISO 27001 u njihovo poslovanje.

Mentor:

prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

UNAPRJEĐENJE SIGURNOSTI POSLOVNOG OKRUŽENJA IMPLEMENTACIJOM NORME ISO/IEC 27001:2013

IMPROVING THE SECURITY OF THE BUSINESS ENVIRONMENT BY IMPLEMENTATION STANDARD ISO/IEC 27001:2013

Mentor: prof. dr. sc. Dragan Peraković

Student: Zoran Maleković

JMBAG: 0246037056

Zagreb, rujan 2020.

SAŽETAK

Norme niza ISO/IEC 27000, s naglaskom na normi ISO/IEC 27001:2013, daju smjernice i definiraju dobru praksu za dizajniranje, implementaciju i auditiranje Sustava upravljanja informacijskom sigurnosti (engl. Information Security Management Systems), s ciljem zaštite povjerljivosti, integriteta i dostupnosti informacija kojima raspolaže svaka organizacija.

Sustav upravljanja informacijskom sigurnosti pomaže u zaštiti podataka, a temelji se na procjeni rizika i upravljanju rizikom pri čemu on nije samo skup tehničkih rješenja, već uključuje nadzor upravljanja i definiranje postupanja organizacije na svim razinama upravljanja informacijama.

U radu se daje pregled zahtjeva norme ISO/IEC 27001:2013, objašnjavaju se ključni zahtjevi norme te se na primjeru organizacije koja se bavi razvojem poslovnih aplikacija koje plasira na strano tržište objašnjava proces uvođenja norme u poslovanje organizacije.

Kroz ukazivanje na kritične faktore implementacije zahtjeva norme, ovaj rad ima za zadaću istaknuti ključne elemente čiji bi izostanak rezultirao neadekvatno i neučinkovito uspostavljenim sustavom upravljanja informacijskom sigurnosti.

KLJUČNE RIJEČI: ISO/IEC 27001:2013, Sustav upravljanja informacijskom sigurnosti, zaštita informacija, zahtjevi norme, implementacija zahtjeva

SUMMARY

ISO / IEC 27000 series of standards, with mainly ISO/IEC 27001: 2013, provide guidance and define good practice for the design, implementation and auditing of Information Security Management Systems, with the aim to protect confidentiality, integrity and availability of organization's information.

The information security management system helps in data protection, and it is based on risk assessment and risk management, where it is not only a set of technical solutions, but also includes monitoring management and definition of the actions in the organization at all levels of information management.

This paper provides an overview of the requirements of the ISO/IEC 27001:2013 standard, explains the key requirements of the standard and explains the process of implementation the standard in the organization 's business where the services example of roll model organization is develeopment of buisness applications. Through the outline of the critical factors of standard

requirements implementations in business organization, this paper aims to to highlight the key elements whose absence would result in inadequately and inefficiently established information security management system.

KEYWORDS: ISO/IEC 27001:2013, information security management system, information protection, standard requirements, implementation of requirements

SADRŽAJ

1. Uvod ... 1

2. Općenito ... 3

2.1. Norme i normizacija ... 3

2.2. Norme niza ISO/IEC 27000 ... 4

3. Norma ISO/IEC 27001:2013 ... 6

3.1. Općenito o normi ... 6

3.1.1. Svrha norme ... 6

3.1.2. Razvoj norme ... 7

3.1.3. Statistički podaci u svijetu, Europi i Republici Hrvatskoj ... 9

3.2. Pregled zahtjeva norme ... 12

3.3. Sadržaj ključnih zahtjeva norme ... 13

4. Implementacija norme u poslovno okruženje ... 31

4.1. Prikaz poslovnog okruženja ... 31

4.2. Proces implementacije ključnih zahtjeva norme u poslovno okruženje ... 34

4.2.1. Odluka najviše uprave o uvođenju sustava informacijske sigurnosti ... 35

4.2.2. Osnivanje radne skupine za uvođenje sustava informacijskom sigurnosti ... 35

4.2.3. Edukacija članova radne skupine o zahtjevima norme ISO/IEC 27001:2013 ... 36

4.2.4. Izrada dokumentacije sustava upravljanja informacijskom sigurnosti ... 36

4.2.5. Aktivnosti na osiguranju fizičke sigurnosti ... 40

4.2.6. Aktivnosti na osiguranju računalne sigurnosti ... 43

4.2.7. Interni audit ... 46

4.2.8. Upravina ocjena ... 47

4.2.9. Certifikacija sustava ... 47

4.3. Kritični faktori implementacije norme ... 48

4.3.1. Opredijeljenost najviše uprave 48
4.3.2. Uključenost zaposlenih 49
4.3.3. Kontinuirano poboljšanje 49
4.4. Koristi od implementacije norme u poslovanje 51
4.4.1. Unutarnje koristi od implementacije norme u poslovanje 51
4.4.2. Vanjske koristi od implementacije norme u poslovanje 51
5. Zaključak 53
6. Literatura 55
POPIS SLIKA 57
POPIS TABLICA 58

1. Uvod

Utjecajem globalizacije i razvojem informacijsko komunikacijskih tehnologija, gotovo pa je i nemoguće pronaći područje poslovanja koje nije pod utjecajem informacijskih tehnologija. Informacije postaju najvrjednija imovina organizacija te se nameće važnost očuvanja njihovog integriteta, povjerljivosti i cjelovitosti, kako bi se osigurao kontinuitet poslovanja organizacije. Iako se pojam informacijske sigurnosti najčešće povezuje s računalnim mrežama i internetom, informacijska sigurnost obuhvaća daleko širi kontekst. U današnje vrijeme, informacije unutar organizacija se nalaze u digitalnom obliku, no dio informacija još uvijek postoji i u papirnatom obliku. Neželjeno „curenje“ informacija, bez obzira u kojem obliku se nalaze, za organizaciju može imati dalekosežne negativne posljedice.

Norma ISO/IEC 27001:2013 predstavlja temelj informacijske sigurnosti. Ona definira zahtjeve za uspostavu sustava upravljanja informacijskom sigurnosti, koji za cilj ima spriječiti pojavu sigurnosnih incidenata te minimizirati štetu nastalu pojavom sigurnosnog incidenta. Norma ISO/IEC 27001:2013 je generička, što znači da je primjenjiva na sve vrste organizacija neovisno o njihovoj veličini i djelatnosti.

Rad je podijeljen u šest cjelina:

1. Uvod
2. Općenito
3. Norma ISO/IEC 27001:2013
4. Implementacija norme u poslovno okruženje
5. Koristi od implementacije norme u poslovanje
6. Zaključak

Druga cjelina opisuje same početke normizacije od pojave prvih pramjera do nastanka međunarodnih organizacija koje se bave normama i normizacijom. Dan je pregled normi niza ISO/IEC 27000 te njihov značaj i utjecaj za normu ISO/IEC 27001:2013.

Treća cjelina ukratko opisuje povijesni razvoj norme te prikazuje kako je rastao broj izdanih certifikata od 2006. do 2018. godine. Opisuje sadržaj poglavlja same norme, a detaljno opisuje obavezna poglavlja norme (poglavlja 4-10).

Četvrta cjelina opisuje postupak uvođenja Sustava za upravljanje informacijskom sigurnosti. Definira i objašnjava ključne zahtjeve koje organizacija mora ispuniti kako bi bila u skladu s normom.

Peta cjelina navodi koristi koje će organizacija ostvariti uvođenjem sustava za upravljanje informacijskom sigurnosti.

2. Općenito

2.1. Norme i normizacija

Normizacija ili standardizacija je djelovanje na sastavljanje odredaba (standarda, normi) za opću i višekratnu upotrebu u stvarnim ili mogućim problemima, radi postizanja optimalne uređenosti u određenom području [1]. To djelovanje se prvenstveno sastoji od izrade, prihvaćanja i primjene norme. Norma ili standard je dokument donesen konsenzusom i odobren od priznatoga tijela, koji za opću i višekratnu uporabu daje pravila, upute ili značajke za djelatnosti ili njihove rezultate s ciljem postizanja najboljeg stupnja uređenosti u danome kontekstu [2].

Počeci normizacije se mogu pronaći u prapovijesti gdje su vidljivi „standardi“ u oblicima posuda u lončarstvu ili izradi primitivnih alata. Prva poznata pramjera pronađena je uklesana u kip sumerskog vladara Gudea (2144 – 2124 pr. Kr.) te je služila kao mjera za dužinu. Različiti oblici normizacije vidljivi su u starom Egiptu gdje su postojale norme za dimenzije opeke, ili u starom Rimu gdje su postojale norme za promjer vodovodnih cijevi, na temelju kojih je naplaćivana potrošnja vode. Danas su norme prisutne u skoro svakom segmentu modernog života. Od normizacije u informacijsko komunikacijskim tehnologijama, što omogućava interoperabilnost različitih komponenti do standardizacije u proizvodnim procesima što omogućava kontinuitet kvalitete proizvoda [3]. Postoji više kriterija za podjelu normi. Jedna od podjela je na tehničke i „ne tehničke“ norme [4]. Tehničke norme (norme za kompatibilnost ili norme za sučelje) definiraju se kao „kodificirane specifikacije komponenata i njihovih relacijskih atributa [5]“. Takve norme za cilj imaju osigurati kompatibilnost i interoperabilnost komponenata različitih tehnoloških sustava. Postojanje više tehničkih standarda je kontraproduktivno, dok postojanje jednog, općeprihvaćenog standarda utječe na tehnološki razvoj u vidu smanjenja raznolikosti proizvoda. „Netehničke“ norme susreću se u različitim domenama normizacije kao što su kontrola kvalitete, zaštita okoliša, financijsko poslovanje i sl. Druga česta podjela normi je podjela na norme procesa i norme proizvoda [4]. Norme procesa reguliraju procese unutar i između organizacija bez unaprijed određenih rezultata. Naprimjer ISO 9001 ne mjeri izravno kvalitetu proizvoda ili usluge već određuje procese koji bi trebali osigurati kvalitetu proizvoda ili usluge. Norme proizvoda definiraju zahtjevan mjerljive veličine koje izlazni proizvod mora zadovoljiti.

Najpoznatije organizacije koje se bave izdavanjem normi je Međunarodna organizacija za standardizaciju (ISO- International Organization for Standardization) i Međunarodni odbor za elektrotehniku (IEC - International Electrotechnical Commission). ISO organizacija djeluje kao mreža nacionalnih normizacijskih tijela sa glavnom zadaćom pripreme, prihvaćanja i izdavanja međunarodnih normi, a trenutno broji 164 zemlje članice [6]. IEC je međunarodna organizacija za standardizaciju koja priprema i objavljuje norme električne, elektroničke i srodne tehnologije.

2.2. Norme niza ISO/IEC 27000

Norme niza ISO/IEC 27000 daju smjernice i dobre prakse za dizajniranje, implementaciju i auditiranje Sustava za upravljanje informacijskom sigurnosti (engl. Information Security Management Systems) s ciljem zaštite povjerljivosti, integriteta i dostupnosti informacija.

ISO/IEC 2700 kreće od pretpostavke da sve organizacije bez obzira na tip organizacije ili veličinu, posjeduju određene informacije. Organizacije bi trebale zaštititi podatke od gubitka, neovlaštenog pristupa ili narušavanja dostupnosti. Također je potrebno zaštititi i druga svojstva, poput autentičnosti, odgovornosti, nerevidiranja i pouzdanosti. Primjenom Sustava za upravljanje informacijskom sigurnosti organizacije održavaju i poboljšavaju svoju informacijsku sigurnost. Norme niza 27000 predstavljaju PDCA model (engl. Plan-Do-Check-Act) koji je temelj ovog niza normi.

PDCA model funkcionira na sljedeći način: *Plan* - Proces u kojem organizacija navodi sve svoje podatke, sigurnosne zahtjeve i razloge zbog kojih je potrebna implementacija Sustava za upravljanje informacijskom sigurnosti. *Do* – Faza provedbe, implementacije i izvršenja kontrola za upravljanje rizicima informacijske sigurnosti. *Check* - Faza nadziranja i mjerenja efikasnosti implementiranih mjera s obzirom na postavljenu politiku, ciljeve i zahtjeve. Act - Poduzimanje radnji za daljnje poboljšavanje procesa. Rezultat svake faze PDCA modela započinje novu fazu (Slika 1.) te se cijeli ciklus kontinuirano i neprestano ponavlja.

Slika 1. PDCA model

Sustav upravljanja informacijskom sigurnosti pomaže u zaštiti podataka, a temelji se na procjeni rizika i upravljanju rizikom. Sustav upravljanja informacijskom sigurnosti nije samo skup tehničkih rješenja, već uključuje nadzor upravljanja i postupke za organizaciju.

Međunarodna organizacija za standardizacija objavila je veći broj normi u području zaštite i sigurnosti informacija kao što su:

- ISO/IEC 27000:2020 – Pregled normi iz ISO/IEC 27000 niza normi
- ISO/IEC 27001:2013 – Sustav upravljanja informacijskom sigurnosti
- ISO/IEC 27002:2017 – Kodeks postupaka za upravljanje sustava informacijske sigurnosti
- ISO/IEC 27003:2017 – Vodič za uvođenje sustava informacijske sigurnosti;
- ISO/IEC 27004:2016 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti;
- ISO/IEC 27005:2018 – Upravljanje rizicima informacijske sigurnosti;
- ISO/IEC 27006:2015 – Zahtjevi za postupkom analize i certificiranja standarda;
- ISO/IEC 27011:2016 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru.

Od navedenih normi najznačajnije su ISO/IEC 27001:2013 i ISO/IEC 27002:2017. Implementacijom ovih normi u procese unutar organizacije osigurava se usklađenost s važećom zakonskom regulativom, ostvaruje se povećanje pouzdanosti sustava u slučaju sigurnosnih incidenata te se podiže svijest o važnosti obuke zaposlenika organizacije. Trenutno je 49 objavljenih normi u nizu normi ISO/IEC 27000, a u pripremi su nove norme koje bi pratile razvoj tehnologija i organizacijskih procesa [7].

3. Norma ISO/IEC 27001:2013

3.1. Općenito o normi

U doba digitalnih informacija, zaštita informacija o kupcima, zaposlenima, proizvodima i poduzećima je od velike važnosti. Gubitak tih informacija za posljedicu može imati izravne financijske gubitke ili gubitke u vidu narušavanja ugleda organizacije. Informacijski sustavi koji često komuniciraju putem interneta ne samo da moraju pouzdano funkcionirati u svakodnevnom poslovanju, već moraju biti zaštićeni i od vanjskih smetnji i rizika. Da bi se osigurala kontinuirana operativna spremnost i netaknuta organizacija procesa u svakom trenutku, potrebno je profesionalno upravljanje informacijskom sigurnosti u tvrtki, kako na konceptualnoj tako i na razini procesa.

ISO/IEC 27001:2013 međunarodna je norma koja ima za cilj osigurati sigurnost informacija u organizacijama poput tvrtki, neprofitnih organizacija ili javnih ustanova. Osnova norme je opis zahtjeva za implementaciju i rad sustava upravljanja informacijskom sigurnosti (ISMS). Sustav je prilagođen okolnostima odgovarajuće organizacije i uzima u obzir pojedinačne posebnosti.

Pored sustava upravljanja informacijskom sigurnošću, ISO/IEC 27001:2013 bavi se analizom i postupkom s rizicima informacijske sigurnosti. U okviru opisanih zahtjeva, vrijednosti i lanci vrijednosti zaštićeni su odabirom odgovarajućih sigurnosnih mehanizama. Za organizacije, ISO 27001 nudi sustavno strukturiran pristup zaštiti integriteta podataka organizacije i njegove povjerljivosti. Istovremeno osigurava dostupnost IT sustava koji su uključeni u poslovne procese [8].

Norma ISO/IEC 27001:2013 je dio niza normi ISO / IEC 2700x, a objavila ga je Međunarodna organizacija za standardizaciju. Do danas napravljeno je nekoliko revizija norme ISO/IEC 27001. Prva revizija izvršena je 2005. godine, a najnovije izdanje datira iz 2015. godine. Organizacije se mogu certificirati u skladu s ISO 27001 i na taj način dokumentirati provedbu i usklađenost s važećim standardima za informacijsku sigurnost. ISO 27001 nametnuo se u cijelom svijetu kao norma i jedna je od najpoznatijih normi za informacijsku sigurnost.

3.1.1. Svrha norme

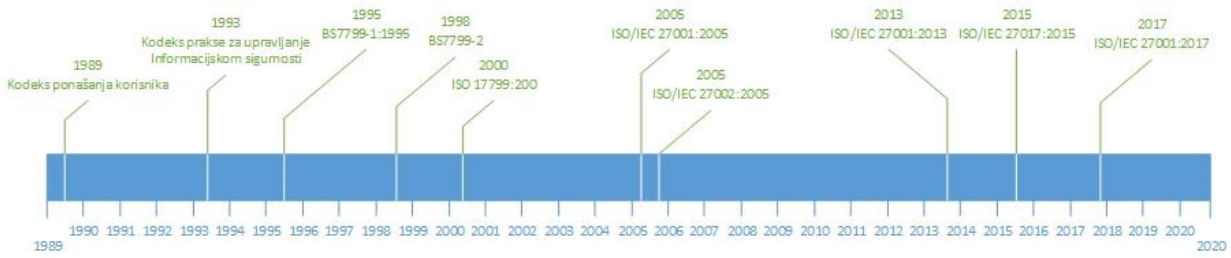
Norma ISO/IEC 27001:2013 razvijena je kako bi se pružio model za uspostavljanje, primjenu, djelovanje, nadzor, pregled, održavanje i poboljšanje sustava upravljanja informacijskom sigurnosti. Zajednički su je razvili, implementirali i nadzirali Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC), u okviru zajedničkog pododbora. Cilj navedenih organizacija bio je razviti široko primjenjivu normu koja će služiti:

- kao pomoć organizacijama u formuliranju zahtjeva i ciljeva informacijske sigurnosti;
- za pružanje pomoći organizacijama u osiguravanju učinkovitog upravljanja troškovima sigurnosti;
- kao pomoć organizacijama u pridržavanju zakona i propisa;
- kao procesni okvir organizacijama za provedbu i upravljanje kontrolama radi postizanja sigurnosnih ciljeva;
- kao pomoć u definiranju novih procesa upravljanja informacijskom sigurnošću;
- kao pomoć u identificiranju i pojašnjenju postojećih procesa upravljanja informacijskom sigurnošću;
- kao pomoć organizacijama za utvrđivanje statusa aktivnosti upravljanja informacijskom sigurnosti;
- za uporabu unutarnjih i vanjskih audita organizacije, radi određivanja stupnja usklađenosti s politikama, direktivama i normama informacijske sigurnosti koje je usvojila organizacija;
- kao pomoć organizacijama u pružanju relevantnih informacija o politikama informacijske sigurnosti, direktivama, standardima i postupcima trgovinskim partnerima i drugim organizacijama s kojima komuniciraju iz operativnih ili komercijalnih razloga;

Unatoč tome što je ISO/IEC 27001:2013 usmjerena na informacijsku sigurnost, ona predstavlja platformu odnosno tehnološki neutralan okvir primjenjiv u svim vrstama organizacija (profitnoj ili neprofitnoj, privatnoj ili državnoj, maloj ili velikoj). Postoji sedam područja kojima tvrtke trebaju upravljati kako bi postigle sukladnost sa ISO/IEC 27001:2013: kontekst organizacije, rukovođenje, planiranje, podrška, djelovanje, ocjena učinka i poboljšanje. Svako navedeno područje objašnjeno je detaljnije u narednim cjelinama ovog rada.

3.1.2. Razvoj norme

U svibnju 1987. godine u Velikoj Britaniji osnovan je Komercijalni centar za računalnu sigurnost (engl. *Commercial Computer Security Centre –CCSC*) [9]. CCSC je imao dva glavna zadatka Prvi je bio pomoći dobavljačima proizvoda u području IT (engl. Information technology) sigurnosti uspostavljanjem skupa međunarodno priznatih kriterija za procjenu, evaluaciju i certificiranja sigurnosti. Drugi zadatak bio je pomoći korisnicima stvaranjem kolekcije pravila u području IT sigurnosti, koja su se u praksi pokazala učinkovita. Ta kolekcija pravila, objavljena je 1989. kao Kodeks ponašanja korisnika (*engl. User Code of Practice*) [9]. Daljnji razvoj kodeksa je nastavio Nacionalni računalni centar (*engl. National Computing Centre*), a kasnije i konzorcij korisnika, prvenstveno britanske industrije. Konačni rezultat prvi je put objavljen 1993. godine kao vodeći dokument britanskog Standarda PD 0003 kao Kodeks prakse za upravljanje informacijskom sigurnosti (*engl. A code of practice for information security management*), a nakon javnog savjetovanja i dopuna preoblikovan je u normu pod nazivom BS7799-1:1995, te je objavljen od strane British Standards Institution. 1998. godine objavljen je BS7799-2 koji specificira sustav za upravljanje informacijskom sigurnosti (*engl. Information Security Management System – ISMS*). Norma BS7799-2 uvodi PDCA ciklus (*engl. Plan – Do – Check-Act*) usklađujući ga sa standardima kvalitete poput ISO 9000. 2000. godine BS7799-1 prihvaćen je kao međunarodna norma ISO 17799:2000. Organizacije se ne nisu mogle certificirati prema normi ISO 17799 pošto isti predstavlja samo dobru praksu, dok je specifikacija sustava za upravljanje informacijskom sigurnosti definirana u normi BS7799-2. 2005. ISO organizacija preuzima i poboljšava normu BS7799-2 te ju izdaje ju pod nazivom ISO 27001 kao normu prema kojoj bi se organizacije mogle certificirati. 2005. godine norma ISO 17799:2000 doživljava svoju reviziju kako bi bila u skladu s normama serije ISO 27000 i iste godine je objavljena kao norma ISO27002. Iz norme ISO27002, 2015. godine nastaje norma ISO27017 koja definira dodatne sigurnosne kontrole za „računarstvo u oblaku“ (*engl. Cloud computing*). 25. rujna 2013. godine norma ISO 27001 doživljava svoju reviziju u kojoj slijedi novu strukturu za sve sustave upravljanja. Također, mnogi pojmovi su generalizirani s poboljšanjima u načinu specificiranja zahtjeva. Naprimjer revizija norme ISO27001 općenitijim zahtjevima odobrava dokumentiranje informacija spremanjem u računalne baze podataka dok je norma iz 2005. prihvaćala isključivo dokumentiranje u obliku fizičkog dokumenta. Grafički prikaz razvoja norme ISO/IEC 27001 dan je na Slici 2.



Slika 2. Grafički prikaz razvoja norme ISO/IEC 27001:2013

3.1.3. Statistički podaci u svijetu, Europi i Republici Hrvatskoj

Prema podacima Međunarodne organizacije za normizaciju, broj certificiranih pravnih subjekata u svijetu po normi ISO/IEC 27001 u 2008. godini iznosio je 9246, 2012. godine taj broj je narastao na skoro 20 000, a 2017. godine se približio brojci od 40 000 izdanih certifikata (Tablica 1.). Očekivano, najveći broj certifikata je izdan u gospodarski najrazvijenijim dijelovima svijeta (Istočna Azija i Europa). Iz navedenih podataka je vidljiv porast značaja i potrebe za učinkovito upravljanje informacijskom sigurnosti u svim vrstama organizacija. 2018. godine dolazi do pada broja izdanih certifikata. Kao razlog Međunarodna organizacija za normizaciju navodi da su pojedine certifikacijske kuće u dotadašnjim izvješćima, situacije u kojima organizacije djeluju na više lokacija, evidentirale kao zasebne certifikate. Također, u 2018. godini neke od certifikacijskih kuća nisu sudjelovale u kreiranju izvješća [10].

Tablica 1. Broj izdanih certifikata u svijetu od 2008. do 2018. godine

Godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.	2016.	2017.	2018.

Europa	2172	3563	4800	5289	6379	7952	8663	10446	12532	14605	11945
Afrika	16	47	46	40	64	99	79	129	224	301	209
Istočna Azija	5807	7394	8340	9110	9722	10116	10414	11994	14704	17562	13657
Središnja i južna Azija	839	1303	1328	1497	1668	2002	2251	2569	2987	3382	3142
Sjeverna Amerika	212	322	329	435	552	712	814	1445	1469	2108	1054
Južna Amerika	72	100	117	150	203	272	273	347	564	620	650
Bliski Istok	128	206	218	279	332	451	511	606	810	923	882
Ukupno	9246	12935	15178	16800	18920	21604	23005	27536	33290	39501	31539

Izvor: [11]

U Tablici 2. navedena je usporedba izdanih certifikata u Hrvatskoj i nekim europskim zemljama, u razdoblju od 2006. do 2018. godine[1]. Također je vidljivo da je broj izdanih certifikata veći u gospodarski razvijenijim zemljama.

Tablica 2. Usporedba izdanih certifikata u Hrvatskoj i nekim europskim zemljama

Godina	**2008.**	**2009.**	**2010.**	**2011.**	**2012.**	**2013.**	**2014.**	**2015.**	**2016.**	**2017.**	**2018.**

[1] U trenutku pisanja ovog rada, zadnje dostupni podaci su podaci za 2018. godinu. Podaci za 2019. godinu biti će objavljeni krajem 2020. godine.

Hrvatska	10	22	24	32	58	69	96	55	110	123	138
Njemačka	239	253	357	424	488	581	634	994	1338	1339	1057
Mađarska	135	146	151	178	199	280	295	323	421	472	484
Bosna i Hercegovina	0	4	4	2	7	9	9	13	17	27	24
Češka	88	264	529	301	264	399	276	381	507	463	543
Grčka	20	28	44	45	49	77	62	136	150	727	240
Ujedinjeno Kraljevstvo	738	946	1157	1464	1701	1923	2253	2790	3367	4503	2444

Izvor: [11]

U Tablici 3. naveden je broj izdanih certifikata po djelatnostima, u Hrvatskoj u 2018. godini. Očekivano, najveći broj certifikata izdan je u informacijsko komunikacijskom sektoru.

Tablica 3. Broj izdanih certifikata u Hrvatskoj u 2018. godini, po djelatnostima

Djelatnost	Broj izdanih certifikata
Izdavačke djelatnosti	1
Tiskarske djelatnosti	1
Naftna industrija	2
Proizvodnja strojeva i opreme	2
Proizvodnja električne i optičke opreme	2
Recikliranje	1
Opskrba električnom energijom	1
Građevina	1
Trgovina	1
Transport i skladištenje	2
Financijsko posredovanje	3
Informacijske tehnologije	46
Inženjerske usluge	3
Edukacija	2
Ostale djelatnosti	25

Izvor: [11]

3.2. Pregled zahtjeva norme

Poglavlja norme ISO/IEC 27001:2013, 0 do 3 nisu obavezna za primjenu dok su poglavlja 4 do 10 obavezna, tj. svi zahtjevi unutar njih moraju biti ispunjeni. U nastavku ove cjeline rada, dan je popis svih poglavlja norme ISO/IEC 27001:2013 (Tablica 4.), a u narednoj cjelini ovog rada, detaljnije su opisana obavezna poglavlja norme ISO/IEC 27001:2013 (poglavlja 4-10) [12].

Tablica 4. Pregled zahtjeva norme

Poglavlje	Zahtjev norme
0	Uvod
1	Područje primjene
2	Upućivanje na druge norme
3	Nazivi i definicije
4	Kontekst organizacije
5	Vodstvo
6	Planiranje
7	Podrška
8	Izvedba
9	Vrednovanje
10	Poboljšavanje

3.3. Sadržaj ključnih zahtjeva norme

U ovoj cjelini rada, detaljno su opisani zahtjevi obaveznih poglavlja norme ISO/IEC 27001:2013, koje organizacija mora zadovoljiti kako bi bila u skladu s normom. Norma ISO/IEC 27001:2013 nema službeni prijevod na hrvatski jezik pa je za potrebe ovog rada korištna izvorna inačica norme na engleskom jeziku [12][2]. Odbrojčavanja u ovoj podcjelini rada slijede odbrojčavanja poglavlja norme ISO/IEC 27001:2013.

Poglavlje 4: Kontekst organizacije

- Zahtjev 4.1: Kontekst organizacije

  Zahtjev 4.1 norme traži od organizacije da analizira i prepozna sva svoja relevantna unutarnja i vanjska pitanja koja su bitna za funkcioniranje same organizacije i sustava. U sklopu analize, organizacija u praktičkom smislu treba identificirati sve svoje jake i slabe strane, odnosno prepoznati dijelove u svom poslovanju iz kojeg su moguće prijetnje koje bi se mogle negativno odraziti na sigurnost informacija. Pod ovim zahtjevom organizacija će tako analizirati npr. strukturu radne snage, dostupnost resursa u ljudskom ili tehničkom smislu,

[2] Opisi poglavlja i zahtjeva norme predstavljaju autorov slobodan prijevod i interpretaciju

specifičnosti vezane za svoj fizički smještaj, ograničenja u pogledu upravljanja i korištenja energenata, konkurenciju, specifičnosti industrije u kojoj djeluje i sl.
Izlaz analize organizacijinog konteksta, provedbeno će dalje biti tretiran i vrednovan kroz analizu rizika te druge zahtjeve norme na strateškom i provedbenom nivou.

- Zahtjev 4.2: Očekivanja zainteresiranih strana

Zahtjev 4.2 norme od organizacije traži da prepozna koje su zainteresirane strane od važnosti za funkcioniranje sustava upravljanja informacijskom sigurnosti, kao i koje eventualno specifične potrebe i očekivanja te zainteresirane strane imaju za sami sustav upravljanja. Zahtjevi zainteresiranih strana uključuju regulatorne i pravne zahtjeve i ugovorne obveze, a kao najčešće zainteresirane strane svakog sustava ističu se vlasnik organizacije, korisnici usluga organizacije (kupci), zaposlenici, zakonodavac te mikro zajednica koja okružuje samu organizaciju.

- Zahtjev 4.3: Opseg primjene sustava upravljanja informacijskom sigurnosti

Zahtjev 4.3 norme traži da organizacija odredi granice i opseg primjene sustava za upravljanja informacijskom sigurnosti, a pri čemu mora uzeti u obzir unutarnja i vanjska pitanja definirana zahtjevom 4.1, kriterije zainteresiranih strana iz zahtjeva 4.2 te vezu i zahtjeva interakcije između aktivnosti koje obavlja sama organizacija i aktivnosti vanjskih pružatelja usluga, a koje potencijalno imaju utjecaj na sigurnost informacija same organizacije. Način ispunjenja zahtjeva norme mora biti dokumentiran kao zapis/dokumentirana informacija, a u kojemu se navodi opseg primjene (djelatnost tvrtke) te granice primjenjivosti (informacija o fizičkim lokacijama/smještaju same organizacije).

- Zahtjev 4.4: Sustav upravljanja informacijskom sigurnosti

Zahtjev 4.4 norme traži da organizacija uspostavi, implementira, održava i kontinuirano poboljšava sustav upravljanja informacijskom sigurnosti u skladu sa zahtjevima predmetne međunarodne norme.

Poglavlje 5: Rukovodstvo

- Zahtjev 5.1: Opredjeljenje najviše uprave

Zahtjev 5.1 norme usmjeren je na vidljivu i materijalnu podršku vrhovne uprave. Svoju predanost prema sustavu za upravljanje informacijskom sigurnosti, uprava demonstrira kroz:

a) definiranje politike sigurnosti informacija te ciljeva informacijske sigurnosti koji moraju biti uspostavljeni i definirani u skladu sa strateškim smjerom organizacije
b) omogućavanjem implementacije svih zahtjeva koji se odnose na sustav upravljanja informacijskom sigurnosti u procese organizacije
c) omogućavanje raspoloživosti resursa potrebnih za efikasno funkcioniranje sustava upravljanja informacijskom sigurnosti
d) promoviranje značaja učinkovitog upravljanja sustavom informacijske sigurnosti te usklađivanja sa zahtjevima sustava za upravljanje informacijskom sigurnosti
e) ostvarivanje da sustav upravljanja informacijskom sigurnosti ispunjava zadane ciljeve
f) motiviranje i poticanje zaposlenika da doprinose kvaliteti sustava za upravljanje informacijskom sigurnosti
g) nastojanjem konstantnog poboljšanja
h) poticanje svih zaposlenika uključenih u proces upravljanja da pokažu inicijativu u dijelu koji se odnosi na njihovo područje odgovornosti.

Opredijeljenost najviše uprave, podrška i poticanje funkcioniranja sustava od strane najviše uprave jedan je od kritičnih faktora za učinkovito funkcioniranje sustava upravljanja informacijskom sigurnosti.

- Zahtjev 5.2: Politika sustava upravljanja informacijskom sigurnosti

Zahtjev 5.2 norme traži od organizacije formuliranje politike kao dokumentirane informacije koja mora biti dostupna zainteresiranim stranama te priopćena i prihvaćena kroz organizaciju od strane svih zaposlenika, te koja mora:

a) biti primjerena svrsi organizacije,
b) uključivati ciljeve informacijske sigurnosti, tj. osigurati radni okvir za izradu ciljeva,
c) uključivati obvezu uprave da ispuni zahtjeve koji su primjenjivi na organizaciju, a odnose se na informacijsku sigurnost
d) uključivati obvezu uprave za neprekidno unaprjeđenje sustava za upravljanje informacijskom sigurnosti

Politika sustava upravljanja informacijskom sigurnosti temeljni je dokument sustava upravljanja te iz nje proizlazi uspostava, dokumentiranje te primjena svih drugih dokumenata nižih hijerarhijskih razina.

- Zahtjev 5.3: Organizacijske uloge, odgovornosti i ovlasti

Zahtjev 5.3 norme od organizacije zahtijeva da su jasno definirane odgovornosti i ovlasti funkcija koje su ključne za funkcioniranje sustava.

Jasna definiranost tko je od zaposlenika odgovoran za što te kako je dužan provoditi aktivnosti unutar organizacije, jedna je od ključnih pretpostavki funkcioniranja sustava upravljanja informacijskom sigurnosti.

Osim navedenog, najviša uprava mora imenovati osobu odgovornu za uspostavu i održavanje sustava informacijske sigurnosti, odnosno osobu koja je odgovorna za postizanje da sustav upravljanja informacijskom sigurnosti bude u skladu sa zahtjevima norme ISO/IEC 27001:2013 te za izvješćivanje uprave o izvedbi sustava upravljanja sigurnosti informacija.

Poglavlje 6: Planiranje

- Zahtjev 6.1: Aktivnosti na identifikaciji rizika i prilika

Norma u zahtjevu 6.1 od organizacije zahtijeva provedbu sveobuhvatne analize rizika koji mogu nepovoljno djelovati na sami sustav i potencijalno ugroziti sigurnost informacija s kojima organizacija raspolaže, odnosno prilika koje mogu povoljno djelovati na sami sustav upravljanja.

Sama norma ne propisuje način niti metodologiju kako organizacija mora pristupiti provedbi analize rizika i prilika, tako da je svaki pristup koji rezultira kompletno sagledanim rizicima i prilikama organizacije zadovoljavajući.

Preporučljivo je međutim da se analiza rizika provodi numeričkim vrednovanjem svakog zasebnog rizika, nakon čega rezultat daje ponderski izražen podatak koliko je koji od rizika zaista rizičan za samu organizaciju.

Organizacija mora nadalje planirati mjere za rješavanje prepoznatih rizika i prilika kako bi se iste integrirale i implementirale u procese sustava upravljanja informacijskom sigurnosti, odnosno procijeniti učinkovitost svih provedenih aktivnosti.

Organizacija treba utvrditi i koristiti proces procjene rizika informacijske sigurnosti na način da:

a) formira i definira kriterije rizika informacijske sigurnosti koji uključuju parametre prihvatljivosti rizika te parametre za provođenje procjene rizika informacijske sigurnosti,
b) osigura da ponovljeni postupak procjene rizike informacijske sigurnosti rezultira vjerodostojnim, relevantnim i mjerljivim rezultatima,
c) definira rizike informacijske sigurnosti, koristi postupak procjene rizika informacijske sigurnosti te određuje vlasnike rizika.
d) sagledava rizike informacijske sigurnosti na način da identificira neželjene posljedice ukoliko bi se identificirani rizici dogodili, odnosno da odredi ukupnu razinu rizika
e) vrednuje razinu rizika na način da uspoređuje rezultate analize rizika s kriterijima rizika te na osnovu njih odredi prioritete za obradu rizika.

Organizacija treba definirati i implementirati proces obrade rizika informacijske sigurnosti na način da izabere adekvatnu metodu obrade rizika informacijske sigurnosti, uvažavajući rezultate procesa procjene rizika, definira sve kontrole neophodne za primjenu odabrane metode obrade rizika informacijske sigurnosti, usporedi kontrole koje su utvrđene s onima u Dodatku A Norme i utvrdi da nijedna propisana kontrola nije izostavljena. Dodatak A norme sadržava detaljan popis ciljeva i kontrola.

Norma nadalje zahtijeva da organizacija producira tzv. Izjavu o primjenjivosti koja sadrži potrebne kontrole iz Dodatka 1, kao i opravdanje za uključenje i isključenje pojedine kontrole. Organizacija mora formulirati plan za obradu rizika informacijske sigurnosti, kao i prihvaćanje razine rizika koji će preostati nakon primjene odgovarajuće kontrola koja će navedeni rizik svesti na prihvatljivu mjeru, tj. minimizirati ga

Norma zaključno u ovom zahtjevu norme zahtijeva da organizacija čuva dokumentiranu informaciju kao dokaz provedbe aktivnosti rješavanja prepoznatih rizika.

- Zahtjev 6.2: Ciljevi sustava upravljanja informacijskom sigurnosti i planiranje njihovog postizanja

Organizacija treba definirati ciljeve informacijske sigurnosti na ključnim pozicijama i razinama u organizaciji, pri čemu ciljevi informacijske sigurnosti moraju biti usuglašeni s politikom informacijske sigurnosti te moraju biti ostvarivi i mjerljivi. Uzimajući u obzir sve

primjenjive zahtjeve informacijske sigurnosti i rezultate postupka procjene i obrade rizika, ciljevi informacijske sigurnosti moraju biti priopćeni i nadopunjavani u slučaju potrebe.
Organizacija ima obvezu čuvanja svih dokumentiranih informacija o ciljevima informacijske sigurnosti. Prilikom planiranja načina postizanja ciljeva informacijske sigurnosti, potrebno je da organizacija utvrdi: što će se učiniti, potrebne resurse, odgovorne osobe, rokove za realizaciju te način na koji će rezultati biti procijenjeni.

Poglavlje 7: Podrška

- Zahtjev 7.1: Resursi

  Organizacija treba definirati i omogućiti resurse neophodne za izgradnju, realizaciju, održavanje i neprekidno unapr jeđenje sustava za upravljanje informacijskom sigurnosti.

- Zahtjev 7.2: Kompetentnost

  Organizacija treba procijeniti i ustanoviti potrebnu osposobljenost svih zaposlenika koji rade u organizaciji, a koji imaju utjecaj na performanse i funkcionalnost sustava informacijske sigurnosti. Potrebna osposobljenost definira se putem kompetencijskih kriterija koji uključuju zahtjeve u pogledu potrebnog radnog iskustva, školske spreme, potrebnih dodatnih unutarnjih i vanjskih izobrazbi, certifikata i sl.
  Organizacija nadalje mora osigurati da osobe uključene u sustav, budu educirane i stručne na temelju adekvatne izobrazbe, treninga ili iskustva. Kada je to moguće, organizacija mora poduzeti sve radnje kako bi zaposlenici putem edukacija, treninga i izobrazbi stekli potrebna znanja i kompetenciju, te procijeniti učinkovitost poduzetih aktivnosti.
  Na kraju, organizacija mora čuvati odgovarajuće dokumentirane informacije kao dokaz o osposobljenosti – CV, diplome, certifikati s pohađanih izobrazbi, zapisnici sa sastanaka i internih edukacija i sl.

- Zahtjev 7.3: Svijest

  Svi zaposlenici organizacije, moraju biti svjesni postojanja politike informacijske sigurnosti, vlastitog utjecaja i doprinosa efikasnosti sustava upravljanja informacijskom sigurnosti, uključujući benefite unaprijeđenih značajki informacijske sigurnosti, kao i

implikacija i posljedica u slučaju da njihov rad ne bude sukladan zahtjevima sustava upravljanja informacijskom sigurnosti.

- Zahtjev 7.4: Komunikacija

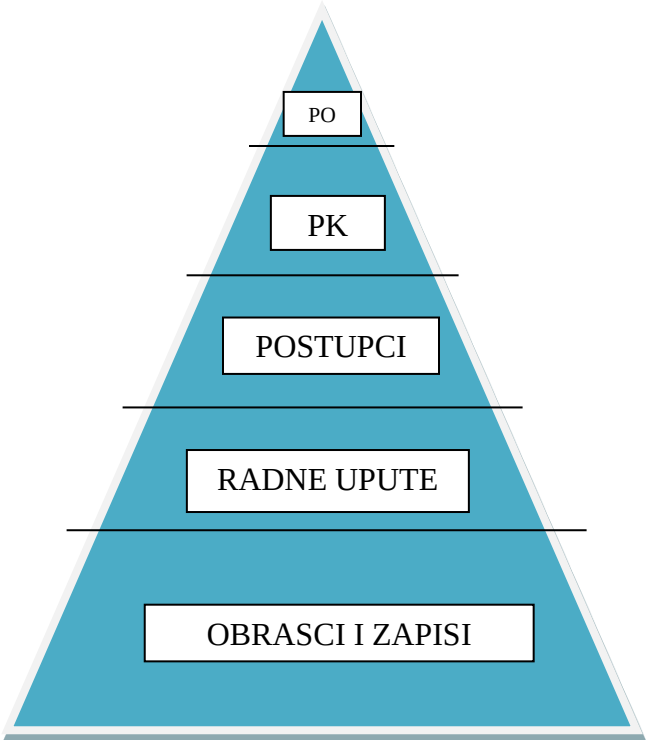
Organizacija mora definirati potrebnu unutarnju i vanjsku komunikaciju važnu za sustav upravljanja informacijskom sigurnosti, a što uključuje o čemu će se komunicirati, kada će se komunicirati, s kime će se komunicirati, tko će komunicirati te kako bi se komunikacija trebala provoditi.

Prilikom određivanja unutarnje i vanjske komunikacije, organizacija mora uzeti u obzir specifičnosti svoje djelatnosti kao i pripadajućih zahtjeva za komunikacijom koji proizlaze iz primjenjivih zakonskih odredbi.

- Zahtjev 7.5: Dokumentirane informacije

Zahtjev 7.5 norme sadrži zahtjeve koji se odnose na sustav upravljanja dokumentiranim informacijama u samoj organizaciji.

Sustav upravljanja dokumentiranim informacijama odnosi se na sve tipove dokumenata u sustavu upravljanja od čega se na vrhu, hijerarhijski nalazi Politika informacijske sigurnosti, dok se na nižim hijerarhijskim razinama nalaze Priručnik upravljanja informacijskom sigurnosti, postupci sustava, radne upute, obrasci te zapisi. Hijerarhijski prikaz dokumenata dan je na Slici 3.



Slika 3. Struktura dokumentacije sustava upravljanja informacijskom sigurnosti

Dokumentacija sustava je srž samog funkcioniranja odredbi sustava, a zadatak joj je osigurati jasnu definiranost poslovnih procesa organizacije s jasnom definiranosti odgovornosti i ovlaštenja unutar sustava kako bi se jednoznačno odredilo kako se pojedini poslovni procesi odvijaju i pod kojim uvjetima, odnosno pravilima.

Općenito gledano, sustav upravljanja informacijskom sigurnosti organizacije mora sadržavati:

a) dokumentirane informacije koju zahtjeva sama norma

b) dokumentirane informacije za koje je sama organizacija odredila da su joj potrebne unutar sustava.

Pregled dokumentiranih informacija zahtijevanih normom, dan je u Tablici 5.

Tablica 5. Pregled obaveznih dokumentiranih informacija u sustavu upravljanja informacijskom sigurnosti

Dokumentirana informacija	Opis	Zahtjev norme ISO/IEC 27001:2013
Opseg ISMS-a	Samostalan dokument, no može biti sadržan i kao dio sigurnosne politike. Definira okvir za izgradnju ISMS-a, tj. da li će se ISMS odnositi na cijelu organizaciju ili samo na dio organizacije.	4.3
Politika informacijske sigurnosti i ciljevi	Politika informacijske sigurnosti predstavlja temeljni dokument ISMS-a, te opisuje njegovu svrhu i namjenu.. Politike postavljaju načela kojih se moraju pridržavati svi članovi organizacije ali i treće strane koje sudjeluju u procesima organizacije.	5.2, 6.2
Metodologija za procjenu i obradu rizika	Dokument kojim se utvrđuju pravila koja se koriste za upravljanje rizicima	6.1.2
Izjava o primjenjivosti	Radi se nakon postupka obrade rizika. Definira koje kontrole iz Aneksa A norme su primjenjive za organizaciju, a koje ne.	6.1.3d
Plan za obradu rizika	Definira način implementacije kontrola koje su sadržane u izjavi o primjenjivosti. Ovaj dokument je potrebno ažurirati tijekom cijele implementacije ISMS-a.	6.1.3e, 6.2

Izvješće o procjeni rizika i obradi rizika	Dokumentiranje procijenjenih rizika te načina na koji će se ti rizici riješiti.	8.2, 8.3
Definicija sigurnosnih uloga i odgovornosti	Precizno opisuje sigurnosne uloge u svim politikama i procedurama organizacije. Ugovorima se definiraju odgovornosti i sigurnosne uloge trećih strana.	A.7.1.2, A.13.2.4
Popis resursa	Evidencija resursa unutar ISMS sustava.	A.8.1.1
Prihvatljivo korištenje informacijskih resursa	Dokument u kojem se definiraju pravila za korištenje resursa organizacije.	A.8.1.3
Politika kontrole pristupa	Dokument koji se izrađuje nakon procjene i obrade rizika. Sadrži poslovnu stranu odobravanja pristupa određenim informacijama ili tehničku stranu kontrole pristupa.	A.9.1.1
Operativne procedure za upravljanje IT-om	Dokument koji se izrađuje nakon procjene i obrade rizika. Može biti izrađen kao jedan dokument ili kao niz politika i procedura. Obuhvaća sva područja iz sekcije A.12 i A.13 (usluge vanjskih strana, sigurnosne kopije, upravljanje promjenama, sigurnost mreže, maliciozni kod, prijenos informacija itd.)	A.12.1.1
Načela sigurnog sistemskog inženjeringa	Jedna od kontrola unutar ISO/IEC 27001:2013 koja zahtjeva dokumentiranje svih načela sigurnog sistemskog inženjeringa u obliku procedure ili standarda. Dokument definira na koji način implementirati sigurnosne tehnike u sve slojeve arhitekture, poslovne podatke i aplikacije.	A.14.2.5
Sigurnosna politika za dobavljače	Jedna od kontrola unutar ISO/IEC 27001:2013 koja zahtjeva definiranje postupka odabira dobavljača. Potrebno je provesti postupak procjene rizika za dobavljače, odrediti koje sigurnosne	A.15.1.1

	klauzule treba uvrstiti u ugovor, kako onemogućiti pristup informacijama nakon raskida ugovora itd.	
Procedura za upravljanje incidentima	Procedura koja definira postupak prijave sigurnosnih slabosti i sigurnosnih incidenata te način njihova klasificiranja i obrade.	A.16.1.5
Procedure kontinuiteta poslovanja	Obuhvaća planove reakcije u slučaju sigurnosnih incidenata te planove oporavka nakon havarije.	A.17.1.2
Pravni, regulatorni i ugovorni zahtjevi	Dokument kojim se definiraju odgovornosti i rokovi za ispunjenje pojedinih zahtjeva.	A.18.1.1
Zapisi o obučavanju, vještinama, iskustvu i kvalifikacijama	Dokumentiranje informacija o obučavanju, vještinama, iskustvu i kvalifikacijama svih zaposlenika. Najčešće u nadležnosti odjela ljudskih potencijala.	7.2
Rezultati monitoringa i mjerenja	Opisuje način mjerenja kontrola ili grupa kontrola. Pišu se ne kraju svakog dokumenta i definiraju ključne pokazatelje učinka. Nakon uspostave metoda mjerenja, potrebno je provoditi mjerenja u skladu s njom.	9.1
Program internog audita	Jednogodišnji plan za provedbu internog audita. Definira odgovorne osobe, metode i kriterije za provedbu audita	9.2

Rezultati internih audita	Izrađuje se na temelju provedenog internog audita. Sadrži rezultate audita i korektivne mjere koje je potrebno provesti. Potrebno ga je izraditi u roku dva dana, nakon provedenog internog audita.	9.2
Rezultati pregleda od strane menadžmenta	Dokument sastavljen u obliku zapisnika sa sastanka. Sadrži sve važne činjenice i odluke donesene na sastanku.	9.3
Rezultati popravnih radnji	Dokument kojim se definiraju odgovornosti i rokovi za pojedine zadatke.	10.1
Dnevnici o aktivnostima korisnika, iznimkama i sigurnosnim događajima	Najčešće se čuva u digitalnom i papirnatom obliku.	A.12.4.1, A.12.4.3

Izvor: [13]

Prilikom kreiranja i ažuriranja dokumentiranih informacija, organizacija je dužna osigurati adekvatnu identifikaciju i opis (naziv, nadnevak, autor ili poziv na broj), oblik (jezik, inačica softvera, grafika) i medij (papirnati ili digitalni oblik) za dokumentiranu informaciju, kao i evidenciju pregleda i odobrenja prikladnosti i primjerenosti i primjerenosti za upotrebu određene dokumentirane informacije od strane za to ovlaštene funkcije.

Dokumentirane informacije koje zahtjeva sustav upravljanja informacijskom sigurnosti te norma ISO/IEC 27001:2013, potrebno je kontinuirano provjeravati kako bi se omogućilo da budu dostupne i prikladne za upotrebu gdje i kada je to potrebno te da je primjereno zaštićena (od gubitka povjerljivosti, cjelovitosti ili neodgovarajućeg korištenja)

Kako bi se na adekvatan način kontrolirale dokumentirane informacije, organizacija mora definirati sljedeće aktivnosti:

a) distribucija, pristup, dohvat i korištenje
b) pohrana i očuvanje uključujući očuvanje čitljivosti
c) kontrola promjena
d) osiguranje i čuvanje.

Dokumentirane informacije vanjskog podrijetla, kao što su zakoni, pravilnici, uredbe i sl., a koje su određene od organizacije kao potrebne za funkcioniranje sustava upravljanja informacijskom sigurnosti, moraju biti identificirane kao prikladne te pod kontrolom u smislu da organizacija ima osigurano praćenje ažurnosti navedenih dokumenata.

Poglavlje 8: Operacije

- Zahtjev 8.1: Operativno planiranje i upravljanje

Kako bi se osigurala implementacija svih mjera utvrđenih zahtjevom 6.1 norme, potrebno je da organizacija planira, primjenjuje i nadzire procese neophodne za ispunjenje zahtjeva informacijske sigurnosti. Organizacija mora primijeniti planove kako bi ispunila ciljeve informacijske sigurnosti određene u zahtjevu 6.2 norme, dokumentirati informacije te voditi dokumentiranu informaciju u mjeri u koju je potrebno imati povjerenja da su procesi provedeni kao što je planirano.

Organizacija treba omogućiti da su procesi koje je proveo vanjski pružatelj usluge, ako je to i kada primjenjivo, obrađeni i kontrolirani.

- Zahtjev 8.2: Procjena rizika

Procjena rizika informacijske sigurnosti provodi se u planiranim intervalima ili kada nastupe značajnije promjene u sustavu. Rezultati procjene rizika dokumentiraju se kao dokaz da je procjena rizika provedena te kako bi se ispunili kriteriji iz zahtjeva 6.1.2 norme.

- Zahtjev 8.3: Obrada rizika informacijske sigurnosti

Organizacija treba primijeniti plan obrade rizika informacijske sigurnosti, te dokumentirati i čuvati rezultate obrade rizika informacijske sigurnosti.

Poglavlje 9: Procjena učinka

- Zahtjev 9.1: Praćenje, mjerenje, analiza i procjena

Cilj praćenja i mjerenja je pomoć pri procjenjivanju da li su ciljevi informacijske sigurnosti, uključujući i procjenu i tretiranje rizika, ispunjeni kako je planirano. Funkcioniranje i učinkovitost sustava se vrednije na način da se utvrdi:

a) što će se u sustavu nadgledati i mjeriti,
b) tko su odgovorne osobe koje će provesti postupak nadzora i mjerenja,
c) metode koje će se koristiti pri praćenju, mjerenju, analizi i vrednovanju
d) kada će se provesti nadzor i mjerenje,
e) tko i kada analizira i ocjenjuje rezultate praćenja i mjerenja.

- Zahtjev 9.2: Interni audit sustava upravljanja informacijskom sigurnosti

Interni auditi se provode u planiranim intervalima s ciljem ishođenja informacije o tome da li sustav upravljanja sigurnosti informacija zadovoljava organizacijine vlastite zahtjeve za sustav upravljanja informacijskom sigurnosti, kao i zahtjeve definirane samom normom.

Osoba koja u ime organizacije provodi interni audit, ne može biti osoba koja je direktno odgovorna za auditirano područje.

Osim navedenog, organizacija mora:

a) planirati, formirati, provoditi i održavati program audita, koji definira koliko često će se audit provoditi, koje metode će se koristiti te zahtjeve za planiranje i izvještavanje uprave
b) odabrati auditore i obavljati audit na način koji osigurava objektivnost i nepristranost u postupku audita,
c) definirati kriterije i opseg za svaki audit,

d) osigurati da rezultat audita bude priopćen odgovarajućoj upravnoj razini,
e) čuvati dokumentirane informacije kao dokaz provedenog internog audita.

- Zahtjev 9.3: Upravina ocjena

Najviša uprava mora u planiranim vremenskim intervalima (najčešće jednom godišnje), preispitati i ocijeniti sustav upravljanja informacijskom sigurnosti, kako bi se osigurala njegova trajna prikladnost, adekvatnost i učinkovitost.

Upravina ocjena mora uzeti u obzir:

a) status radnji iz prethodne upravine ocjene
b) promijene u vanjskim i unutarnjim pitanjima relevantnima za sustav upravljanja informacijskom sigurnosti
c) povratne informacije o izvedbi sustava upravljanja informacijskom sigurnosti, uključujući trendove s nesukladnostima i popravnim radnjama, rezultatima praćenja i mjerenja, rezultatima audita i ispunjenju ciljeva sustava upravljanja informacijskom sigurnosti.
d) povratne informacije zainteresiranih strana
e) rezultate procjene rizika i status plana obrade rizika
f) mogućnosti za trajno poboljšanje sustava.

Poglavlje 10: Poboljšavanje

- Zahtjev 10.1: Nesukladnosti i popravne radnje

Kada se u sustavu upravljanja pojavi nesukladnost, organizacija mora:

a) Odgovoriti na istu i prema potrebi poduzeti mjere za kontrolu i ispravljanje posljedice
b) procijeniti potrebu za djelovanjem kako bi se uklonili uzroci nesukladnosti, kako se iste ne bi vratile ili pojavile na drugom mjestu u sustavu i to kroz pregled nesukladnosti, utvrđivanje uzroka nesukladnosti te utvrđivanje da li postoje slične nesukladnosti, ili bi se mogle pojaviti,
c) primijeniti sve potrebne radnje,
d) provjeriti efikasnost svih ranije poduzetih radnji
e) napraviti promjenu u sustavu upravljanja informacijskom sigurnosti, ako je to potrebno.

Organizacija mora čuvati dokumentiranu informaciju o prirodi utvrđenih nesukladnosti te rezultata obrade istih.

- Zahtjev 10.2: Neprekidno poboljšavanje

Organizacija mora kontinuirano poboljšavati prikladnost, adekvatnost i učinkovitost sustava upravljanja informacijskom sigurnosti.

Osim osnovnog dijela norme u kojem su navedeni zahtjevi, norma ima i normativni dodatak u kojem se nalaze kontrole koje organizacijama stoje na raspolaganju u osiguranju informacijske sigurnosti.

Kontrola ima ukupno 114 i podijeljene su u 14 kategorija, a broj kontrola koje će neka organizacija primijeniti ovisi o specifičnosti same organizacije.

S obzirom da organizacije primjenjuju one kontrole koje mogu primijeniti s obzirom na svoju djelatnost, jasno je da broj kontrola u konačnici varira od organizacije do organizacije.

Kontrole iz Dodatka A norme navedene su u Tablici 6.:

Tablica 6. Kontrole iz Dodatka A norme ISO/IEC 27001:2013

1.	A.5 Politika informacijske sigurnosti
2.	A.6 Organizacija informacijske sigurnosti
	a) interna organizacija informacijske sigurnosti
	b) mobilni uređaji i rad na daljinu
3.	A.7 Sigurnost ljudskih resursa
	a) prije zapošljavanja
	b) za vrijeme zapošljavanja u organizaciji
	c) nakon prestanka zapošljavanja u organizaciji
4.	A.8 Upravljanje imovinom
	a) odgovornost za imovinu
	b) klasifikacija informacija
	c) upravljanje medijima na kojima se nalaze informacije
5.	A.9 Kontrola pristupa
	a) poslovni zahtjevi u pogledu kontrole pristupa

	b) upravljanje računima zaposlenika
	c) odgovornost zaposlenika
	d) upravljanje kontrolama u sustavu i aplikacijama
6.	A.10 Kriptografija
7.	A.11 Fizička sigurnost i sigurnost okruženja
	a) sigurnosne zone
	b) sigurnosna oprema
8.	A.12 Sigurnost operacija
	a) operativne procedure i odgovornosti
	b) zaštita od malware-a
	c) back-up
	d) logiranje i monitoring
	e) kontrola software-a
	f) upravljanje tehničkim ranjivostima
	g) aspekti sigurnosti internog audita
9.	A.13 Sigurnost komunikacija
	a) sigurnost na mreži
	b) transfer informacija
10.	A.14 Nabava, razvoj i održavanje informacijskih sustava
	a) zahtjevi sigurnosti za sustav informacija
	b) sigurnost informacija u postupku dizajna i razvoja
	c) sigurnost podataka koji se koriste za testiranje
11.	A.15 Odnosi s dobavljačima
	a) sigurnost informacija u odnosima s dobavljačima
	b) sigurnost informacija prilikom pružanja usluga dobavljačima
12.	A.16 Upravljanje incidentima informacijske sigurnosti
13.	A.17 Aspekti informacijske sigurnosti u upravljanju kontinuitetom poslovanja
14.	A.18 Sukladnost
	a) sukladnost sa zakonskom regulativom
	b) preispitivanje sustava upravljanja informacijskom sigurnosti

4. Implementacija norme u poslovno okruženje

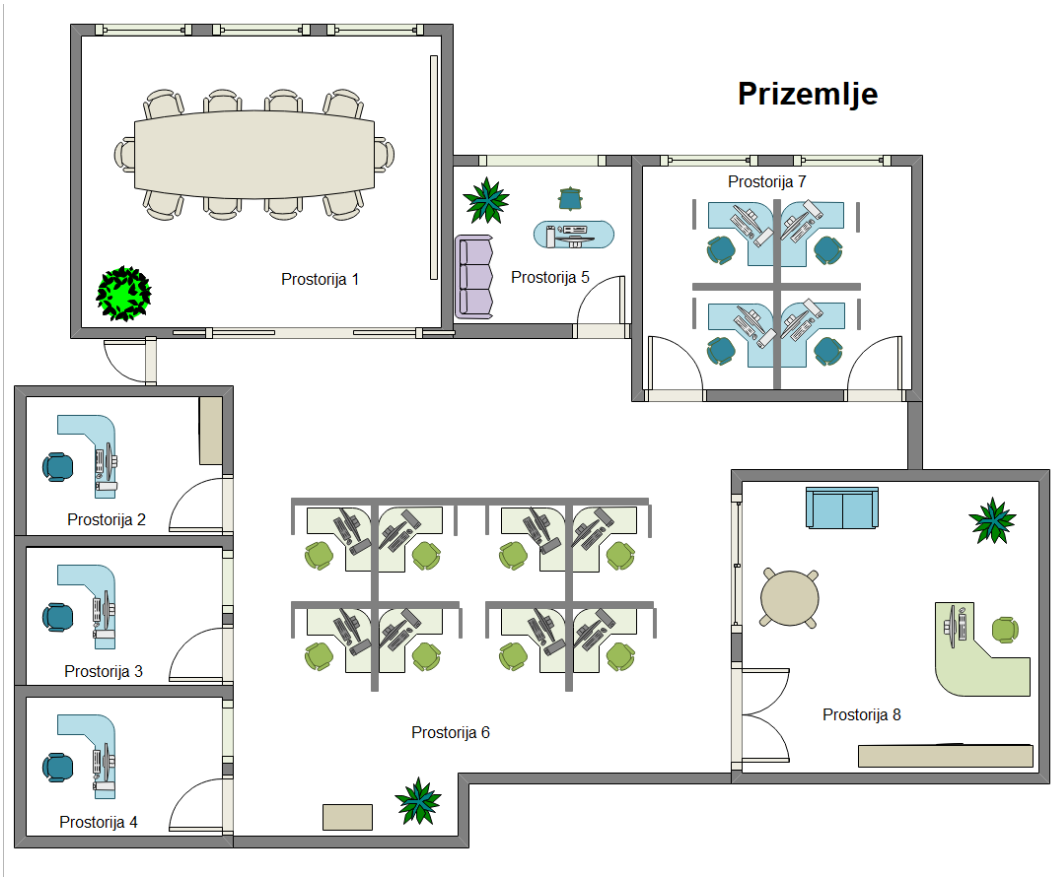
4.1. Prikaz poslovnog okruženja

Za potrebe ovog rada, bit će opisana imaginarna tvrtka koja se bavi razvojem poslovnih aplikacija koje plasira na strano tržište. Tvrtka razvija i održava sustav elektroničkog poslovanja za nekoliko inozemnih osiguravateljskih kuća. Sustav se sastoji od dijela namijenjenog za kupce i dijela namijenjenog za zaposlenike osiguravateljske kuće. Kupci preko web aplikacije mogu ugovoriti više vrsta osiguranja (životno osiguranje, zdravstveno osiguranje, auto osiguranje, osiguranje nekretnine, putno osiguranje i sl.). Dio aplikacije namijenjen za zaposlenike osiguravajuće kuće služi za upravljanje odnosima s klijentima, proizvodima i financijama te statističku obradu podataka.

Tvrtka je osnovana 2000. godine sa sjedištem u Zagrebu te trenutno nema urede na drugim lokacijama. Sjedište tvrtke se nalazi u poslovnoj zgradi, u prizemlju i prvom katu. Tlocrt prizemlja prikazan je na Slika 4.

U prizemlju se nalazi 8 prostorija:

1. Sala za sastanke
2. Računovodstvo
3. Ured voditelja marketinga
4. Ured system administratora
5. Ured voditelja ljudskih resursa
6. Ured za programere
7. Ured voditelja projekata
8. Ured glavnog direktora



Slika 4. Tlocrt prizemlja

Tlocrt prvog kata prikazan je na Slika 5. Na prvom katu nalazi se 7 prostorija:

9. Arhiva
10. Ured za programere
11. Čajna kuhinja
12. Spremište
13. Toalet
14. Toalet
15. Server sala

Slika 5. Tlocrt 1. kata

Trenutno ima 33 stalnozaposlenih, a prema potrebi angažiraju se vanjski suradnici. Struktura zaposlenih je:

- Generalni direktor – 1
- Project manageri – 4
- Programeri – 24 (Front end -5, back end – 18)
- Ljudski resursi – 1
- Računovodstvo – 1
- Marketing – 1
- System administrator - 2

4.2. Proces implementacije ključnih zahtjeva norme u poslovno okruženje

U ovoj cjelini rada detaljnije su opisani ključni koraci pri implementaciji norme ISO/IEC 27001:2013, a na Slici 6. su prikazani grafički.

Slika 6. Koraci implementacije norme ISO/IEC 27001:2013

4.2.1. Odluka najviše uprave o uvođenju sustava informacijske sigurnosti

Najviša uprava tvrtke koju predstavlja direktor, donijela je odluku o uvođenju sustava upravljanja informacijskom sigurnosti. Navedenom odlukom, definirana je glavna odgovorna osoba koja će ujedno obnašati i funkciju predstavnika uprave za informacijsku sigurnost te ciljani rok od 8 mjeseci kao rok za završetak postupka certifikacije.

Direktor je također rezervirao namjenska sredstva u iznosu od 95.000,00 kn koja će biti utrošena u uvođenje i certifikaciju sustava.

Objektivni dokaz:

Dokument: Odluka o uvođenju sustava upravljanja informacijskom sigurnosti.

4.2.2. Osnivanje radne skupine za uvođenje sustava informacijskom sigurnosti

Direktor tvrtke odlukom je imenovao radnu skupinu koju čine predstavnik uprave za informacijsku sigurnost te još 4 zaposlenika kao tim odgovoran za uvođenje te održavanje sustava upravljanja informacijskom sigurnosti.

Imenovani djelatnici su voditelji organizacijskih jedinica tvrtke te su uključeni u radnu skupinu kako bi se osigurala učinkovita razmjena informacija kroz tvrtku na način da su voditelji ujedno odgovorni i za komunikaciju odluka, planova i ukupnih aktivnosti te osigurala informiranost svih zaposlenih o samom sustavu upravljanja informacijskom sigurnosti.

Voditelj skupine – predstavnik uprave za sustav upravljanja informacijskom sigurnosti zadužen je da u roku 2 tjedna odabere i osigura provedbu edukacije/treninga članova radne skupine o primjenjivim zahtjevima i načelima sustava upravljanja informacijskom sigurnosti.

Javnim pozivom za prikupljanje ponuda, zaprimljene su 4 ponude za usluge edukacije članova radne skupine o zahtjevima norme ISO/IEC 27001:2013 od čega je odabrana jedna koja je po ocjeni direktora bila najpovoljnija te je određen termin provedbe edukacije.

Objektivni dokaz: Odluka o osnivanju radne skupine te sklopljen ugovor za provedbu edukacije djelatnika.

4.2.3. Edukacija članova radne skupine o zahtjevima norme ISO/IEC 27001:2013

Ugovoreni pružatelj usluge edukacije članova radne skupine je u prostorima tvrtke održao trodnevnu edukaciju o zahtjevima norme ISO 27001:2013 te pratećih normativnih dokumenata čime su članovi radne skupine dobili potrebite informacije o smislu i značenju norme, ciljevima, zahtjevima koje norma definira te mogućim kontrolama koje tvrtka može implementirati u cilju osiguranja sigurnosti informacija.

Navedena edukacija je uključila i dodatni dan edukacije o metodologiji i načinu provedbe internih audita u tvrtki, čime je tvrtka dobila ukupno 5 osoba koje su educirane za provedbu internih audita prema zahtjevima norme.

Objektivni dokaz: Certifikat izdan djelatnicima o završenom seminaru „Zahtjevi norme ISO/IEC 27001:2013“ te „Primjena norme ISO 19011 u provedbi internih audita sustava upravljanja informacijskom sigurnosti.

4.2.4. Izrada dokumentacije sustava upravljanja informacijskom sigurnosti

Članovi radne skupine su vremenskom trajanju od 2 mjeseca radili na izradi dokumenata sustava upravljanja informacijskom sigurnosti.

U sklopu navedene aktivnosti izrađeni su dokumenti čiji je pregled dan u Tablici 7.

Tablica 7. Dokumentacija sustava upravljanja informacijskom sigurnosti

	DOKUMENT	SVRHA
1.	Opseg primjene sustava upravljanja	Tvrtka je dokumentirala opseg primjene sustava upravljanja, definirala fizičku lokaciju na kojoj djeluje, definirala djelatnost, kao i opseg aktivnosti koje su obuhvaćene sustavom upravljanja.

2.	Priručnik sustava upravljanja informacijskom sigurnosti	Izrađen je Priručnik sustava upravljanja kao temeljni dokument sustava. Priručnik spaja s jedne strane zahtjeve norme i s druge strane dokumente nižih hijerarhijskih razina u kojima je detaljno opisano i definirano postupanje tvrtke po svakom zahtjevu norme (postupci, radne upute).
3.	Kontekst organizacije s očekivanjima zainteresiranih strana	U dokumentu je tvrtka u cilju definiranja i prepoznavanja konteksta unutar kojeg djeluje, analizirala svoje jake i slabe strane te prepoznala čimbenike koji mogu negativno djelovati na sustav upravljanja informacijskom sigurnosti. Također, prepoznate su osnovne zainteresirane strane kao i njihova očekivanja spram sustava upravljanja informacijskom sigurnosti.
4.	Politika sustava upravljanja informacijskom sigurnosti	Vrhovni dokument sustava upravljanja informacijskom sigurnosti te ga donosi najviša uprava. Sadrži ciljeve sustava upravljanja informacijskom sigurnosti, opredjeljenje najviše uprave za ispunjenje zakonskih zahtjeva prilikom uspostave i održavanja sustava te opredjeljenje za neprekidno poboljšanje sustava upravljanja informacijskom sigurnosti. Politika je putem internetske stranice tvrtke učinjena javno dostupnom te putem oglasne ploče iskomunicirana sa zaposlenicima.
5.	Procedure sustava upravljanja	Procedure sustava upravljanja detaljnije opisuju odvijanje pojedinih dijelova sustava upravljanja informacijskom sigurnosti na način da jasno definiraju koja funkcija/osoba, kada, kako i na koji način provodi pojedine aktivnosti unutar uspostavljenog sustava. Jedna od funkcija

		procedura je jasno definiranje poslovnih procesa uz izbjegavanje potencijalnih preklapanja pojedinih funkcija te u konačnici jednoobraznost odvijanja poslovnih procesa bez obzira na to koja osoba provodi određenu aktivnost.
6.	Obrasci sustava upravljanja	Obrasci sustava upravljanja su predlošci koji su izrađeni kako bi se jednoobrazno pristupilo evidenciji odvijanja pojedinih koraka unutar uspostavljenog sustava jer osiguravaju uvijek jednak pristup njihovom ispunjavanju. Popunjavanjem obrasca nastaje zasebna kategorija dokumenata, a to su zapisi.
7.	Pravilnik o unutrašnjem ustroju s kriterijima kompetentnosti	Pravilnik o unutrašnjem ustroju s kriterijima kompetentnosti osigurava jasno prepoznavanje svih funkcija unutar tvrtke te njihovih pripadajućih odgovornosti unutar uspostavljenog sustava informacijskom sigurnosti. Uz svaku funkciju definirani su i pripadajući zahtjevi kompetentnosti u smislu potrebne naobrazbe, radnog iskustva, dodatnih vještina i znanja te sposobnosti kako bi se osiguralo da osobe imenovane na određene funkcije ispunjavaju unaprijed postavljene kriterije. Pravilnik o unutrašnjem ustroju predstavlja zasebni dokument s vlastitom oznakom te oznakom važećeg izdanja dokumenta.
8.	Analiza rizika informacijske sigurnosti	Izrađena je osnovna analiza svih potencijalnih rizika za informacijsku sigurnost. U analizi su identificirani prioritetni rizici na način da su svi rizici sagledavani i ponderirani umnoškom vjerojatnosti događaja i posljedice u slučaju ostvarenja pojedinog rizika. Iz same analize rizika

		proizlaze propisane mjere i kontrole kojim su prepoznati ključni rizici svedeni na najmanju moguću mjeru.
9.	Analiza prilika informacijske sigurnosti	U analizi prilika sagledani su svi čimbenici koji mogu pozitivno utjecati na informacijsku sigurnost. Rezultat analize prilika su jasno definirane odgovornosti, rokovi i resursi. Jedna od prepoznatih prilika je dobivanje novog velikog klijenta, a za ostvarivanje te prilike je bilo potrebno dobivanje certifikata ISO/IEC 27001:2013.
10.	Ciljevi informacijske sigurnosti	Izrađen je dokument koji sadrži ciljeve informacijske sigurnosti na godišnjoj razini te aktivnosti potrebne za njihovo ostvarivanje. Osim toga, definirane su odgovorne osobe za svaki od ciljeva te rok ispunjenja.
11.	Izjava o primjenjivosti	Izrađen je dokument u kojem su prepoznate i pobrojane sve kontrole iz Dodatka A, norme ISO/IEC 27001:2013, koje nisu primjenjive na djelatnost tvrtke.
12.	Pregled primijenjenih kontrola sustava upravljanja informacijskom sigurnosti	Izrađen je dokument u kojem su pobrojane sve kontrole iz Dodatka A, norme ISO/IEC 27001:2013, koje su primjenjive na djelatnost. Za svaku kontrolu izrađena je procedura, obrazac ili priručnik koji jasno opisuju kako je organizacija primijenila određenu kontrolu.

4.2.5. Aktivnosti na osiguranju fizičke sigurnosti

Kontrola A.7 Dodatka A norme ISO/IEC 27001:2013 definira kontrole koje se provode prije, tijekom i nakon zaposlenja u organizaciji.

Kontrola A.7.1 Dodatka A norme ISO/IEC 27001:2013: Prije zaposlenja

Propisana je procedura za odjel ljudskih resursa gdje voditelj/voditeljica ljudskih resursa ima obavezu prije zaposlenja provesti opću provjeru potencijalnog zaposlenika na temelju javno dostupnih informacija. Osim toga, svaka osoba prilikom zaposlenja dužna je potpisati dokument kojim se obavezuje na pridržavanje politika i procedura sustava za upravljanje informacijskom sigurnosti, da će ih primjenjivati u svakodnevnom radu i da je svjesna da kršenje istih povlači posljedice kao što su otkaz ugovora o radu ili pokretanje sudskog procesa

Kontrola A.7.2 Dodatka A norme ISO/IEC 27001:2013: Tijekom zaposlenja

Voditelj/voditeljica ima obavezu izrade godišnjeg plana edukacije zaposlenika. Plan uključuje održavanje internih radionica, edukacija i podsjetnika na području informacijske sigurnosti za sve zaposlenike. Također, u sklopu ove kontrole izrađen je etički kodeks, a potpisivanjem izjave iz kontrole 7.1. koju potpisuje svaki zaposlenik, izjavljuje da je upoznat i suglasan s eventualnim disciplinarnim procesom unutar organizacije. Etički kodeks definira posljedice u slučaju kršenja određene odredbe.

Kontrola A.7.3 Dodatka A norme ISO/IEC 27001:2013: – Nakon zaposlenja

Odjel ljudskih resursa izradio je proceduru kojom se definiraju aktivnosti koje se provode kada zaposlenih napušta organizaciju. Aktivnosti obuhvaćaju vraćanje imovine organizacije (mobilni uređaji, računala, uređaji za pohranu podataka, autorizacijske kartice) te ukidanje svih korisničkih računa.

Kontrola A.11 norme ISO/IEC 27001:2013 definira kontrole koje se odnose na uspostavljanje fizičke sigurnosti kako bi se spriječio neovlašteni i neautorizirani pristup informacijskoj imovini organizacije.

Kontrola A.11.1 Dodatka A norme ISO/IEC 27001:2013: Sigurnosne zone

Prostor organizacije podijeljen je u dvije sigurnosne zone. Druga sigurnosna zona obuhvaća cjelokupni prostor organizacije i pristup drugoj njoj mogu pristupiti svi zaposlenici organizacije. Prva sigurnosna zona obuhvaća server salu i arhivu. Prvoj sigurnosnoj zoni mogu pristupiti isključivo sistem administrator, voditelj/voditeljica ljudskih resursa, voditeljica financija i generalni direktor. Evidencija i kontrola pristupa prostorijama organizacije se provodi uporabom identifikacijskih kartica i čitača koji su postavljeni na ulazu u svaku prostoriju. Kako bi se spriječio neovlašteni ulazak trećih osoba u prostore organizacije, postavljen je video nadzor i alarm, a prostorije prve sigurnosne zone dodatno su osigurane protuprovalnim vratima te rešetkama na prozorima. Kako bi se informacijska imovina organizacije zaštitila od prirodnih nepogoda (poplava, požar, udar groma) prostorije u organizacije instaliran je protupožarni sustav i prenaponska zaštita. Također, serveri i police sa spisima u arhivi su podignuti od tla kao zaštita u slučaju poplave.

Kontrola A.11.2 Dodatka A norme ISO/IEC 27001:2013: Oprema

Sistem administrator izradio je proceduru za postupanje s opremom koja uključuje sljedeće politike:

- *Clear screen policy* – prilikom napuštanja radnog mjesta svaki zaposlenik je dužan zaključati računalo kako bi se spriječilo neovlašteno korištenje računala organizacije
- *Clear desk policy* – prilikom napuštanja radnog mjesta svaki zaposlenik je dužan ukloniti sve dokumente s radnog stola
- Zaposlenici ne smiju ostavljati uređaje koji sadrže podatke organizacije bez nadzora te moraju poduzeti sve mjere kako bi se spriječila njihova krađa ili gubitak
- Rashodovanje opreme provodi sistem administrator isključivo unutar prostora organizacije
- Rashodovanje računala se provodi na način da se prije predaje u elektronički otpad, tvrdi diskovi (i ostali mediji za pohranu podataka) unište na način da povrat podataka s njih nije moguć
- Sistem administrator je odgovoran za redovito ažuriranje i održavanje operativnih sustava na računalima, antivirusnog softvera, vatrozida i sl.

Kontrola A.8 Dodatka A norme ISO/IEC 27001:2013: Upravljanje imovinom

Slijedom zahtjeva kontrole za upravljanje imovinom, tvrtka je izradila središnji registar imovine koja može utjecati na informacijsku sigurnost, kao i mjesto na kojem se imovina nalazi, uključujući identifikaciju osoba koje se nalaze u posjedu ili su odgovorni za imovinu. Tvrtka posjeduje: 6 poslužitelja, 34 stolna računala, 8 prijenosnih računala, 10 mobilnih uređaja, 4 printera, 10 prijenosnih medija za pohranu podataka, 2 usmjernika te 4 preklopnika.

Uspostavljena je i dokumentirana procedura Upravljanje imovinom u kojoj su definirane odgovornosti te intervali provedbe inventure imovine tvrtke te opća pravila za postupanje s imovinom.

Izrađena je i procedura Povrat imovine tvrtke u kojoj je definiran hodogram aktivnosti s pripadajućim odgovornostima prilikom prekida ugovora o radu s nekim od zaposlenika kako bi se osiguralo da se sva imovina tvrtke koja se nalazila pod nadzorom zaposlenika vrati kako bi se osiguralo otuđenje ili da se zaboravi koja se sva imovina, na kojoj se mogu nalaziti informacije koje su obuhvaćene sustavom upravljanja informacijskom sigurnosti, nalazi u posjedu zaposlenika s kojim se prekida ugovor o radu.

Izrađena je i procedura Klasifikacija informacija tvrtke prema kojoj su uspostavljene razine klasifikacije podataka s definiranim razinama funkcija osoba unutar tvrtki koje imaju pravo pristupa pridruženim razinama klasifikacija informacija.

Unutar procedure Upravljanje imovinom opisano je postupanje s povratom i uništavanjem medija za pohranu koji se nalaze u uređajima ili u posjedu zaposlenika kako bi se osiguralo da svi takvi uređaji ne dođu u posjed neovlaštenih osoba koje bi na ovaj ili onaj način mogle doći u posjed informacija koje se eventualno na njima nalaze.

Ista procedura opisuje i postupanje s prijenosnim uređajima koji ne pripadaju tvrtki, a koje je zabranjeno koristiti na službenim računalima.

4.2.6. Aktivnosti na osiguranju računalne sigurnosti

Kontrola A.6.2 Dodatka A norme ISO/IEC 27001:2013: Mobilni uređaji i rad na daljinu

Uspostavljena je procedura kojom je jasno definirano postupanje s uređajima (mobilni uređaji, prijenosna računala) koji su u vlasništvu tvrtke. Dopuštena je uporaba samo odobrenog softvera, spajanje uređaja samo na poznate računalne mreže i sl. Procedura za rad na daljinu definira postupke pri radu izvan prostora tvrtke. Prilikom pristupanja računalnim podacima izvan lokalne mreže tvrtke, uspostavljene su dodatne mjere autorizacije u vidu SMS autorizacijskog koda. Također, pristup je moguć samo uz upotrebu VPN-a (engl. *Virtual Private Network*) s digitalnim certifikatom izdanim od strane tvrtke.

Kontrola A.9 Dodatka A norme ISO/IEC 27001:2013: Kontrola pristupa

Kontrola pristupa je postupak davanja ovlaštenim korisnicima prava na pristup informacijama uz sprečavanje pristupa neautoriziranim korisnicima. Kontrola A.9. Dodatka A norme ISO/IEC 27001:2013, o kontroli pristupa odnosi se na zahtjeve za kontrolu pristupa informacijskim sredstvima i mogućnostima za obradu informacija. Kontrole su usmjerene na zaštitu od slučajnih ili namjernih gubitaka, oštećenja, prijetnji itd. Kako bi se to ostvarilo izrađena je politika koja propisuje postupke kontrole, registraciju, uklanjanje i pregled prava korisnika, uključujući fizički pristup, pristup podacima u digitalnom obliku uz vođenje dnevnika pristupa dokumentima.

Kontrola A.12.2 Dodatka A norme ISO/IEC 27001:2013: Zaštita od zlonamjernog softvera

Sistem administrator je zadužen za implementaciju, konfiguraciju i održavanje antivirusnog softvera te vatrozida, na svim uređajima u tvrtki. Koristi se licencirani softver za koji tvrtka obnavlja licence jednom godišnje. Ažuriranje antivirusnog softvera se provodi automatski, svaki dan.

Kontrola A.12.3 Dodatka A norme ISO/IEC 27001:2013: Sigurnosna kopija

Podaci na svakom računalu se automatski sinkroniziraju s centralnim poslužiteljem. Stvaranje sigurnosne kopije podataka na poslužitelju se odvija dva puta dnevno (12:00 i 00:00).

Sigurna kopija podataka se pohranjuje na drugi poslužitelj koji koristi zrcalnu tehniku zapisivanja – podaci se zapisuju identično na dva tvrda diska.

Kontrola A.12.4 Dodatka A norme ISO/IEC 27001:2013: Dnevnik događaja i nadzor

U slučaju sigurnosnog incidenta, potrebno je utvrditi što se dogodilo, gdje, tko je izazvao incident i sl. Zbog toga je uspostavljena politika vođenja dnevnika događaja. Bilježe se podaci o pristupu podacima, radnjama korisnika, pogreškama događajima i sl. Svaka aplikacija koja se koristi na računalu tvrtke šalje zapise na središnji log poslužitelj. Na taj način je omogućeno centraliziranje svih zapisa na jednom poslužitelju. Zapisi na središnjem poslužitelju su kriptirani, a pristupiti im može samo sistem administrator. Sustavi registriraju radnje svih korisnika, bez obzira radi li se o običnom korisniku ili administratoru. Središnji poslužitelj služi i za sinkronizaciju vremena na svim računalima u tvrtki kako bi se u slučaju sigurnosnog incidenta, sve radnje mogle točno kronološki rekonstruirati.

Kontrola A.12.5 Dodatka A norme ISO/IEC 27001:2013: Kontrola operativnog softvera

Unutar tvrtke dopuštena je uporaba samo odobrenog softvera. Uz licencirani softver čije se korištenje plaća na godišnjoj razini, sistem administrator je izradio popis dopuštenog besplatnog softvera koji se koristi u svakodnevnom radu.

Kontrola A.12.6 Dodatka A norme ISO/IEC 27001:2013: Upravljanje ranjivostima opreme

Instalaciju softvera provodi isključivo ovlaštena osoba tj. sistem administrator. Na svim računalima dopuštena je uporaba medija za pohranu podataka koji su u vlasništvu tvrtke, a koji su kriptirani odgovarajućim softverom. Sadržaj nekriptiranog medija za pohranu podataka nije moguće pokrenuti na računalu tvrtke.

Kontrola A.13.1 Dodatka A norme ISO/IEC 27001:2013: Upravljanje zaštitom mreže

Izrađen je skup općih procedura, poput definiranja odgovornosti i postupaka za upravljanje mrežnom opremom, korištenje kriptografskih rješenja za zaštitu podataka u tranzitu i međusobno povezanih sustavi (npr. VPN), nadgledanje i bilježenje mrežnih aktivnosti (npr., pomoću sustava za otkrivanje neovlaštenog pristupa mreži), provjere autentičnosti i drugih načina za ograničavanje

pristupa i korištenja mrežnih resursa. Filtriranje i nadzor mrežnog prometa između lokalne mreže tvrtke i interneta odvija se korištenjem hardverskog vatrozida.

Kontrola A.13.2 Dodatka A norme ISO/IEC 27001:2013: Prijenos podataka

Cilj politike prijenosa informacija je kontrola protoka informacija na siguran način između organizacije i unutarnjih ili vanjskih subjekata. U modernom poslovanju svakodnevno se prenosi bezbroj različitih podataka koji su često osjetljive prirode. Svrha kontrole prijenosa podataka u je osigurati da se ti prijenosi odvijaju putem sigurnih protokola i da su osjetljivi podaci zaštićeni od neovlaštenog pristupa ili otkrivanja. Prijenos podataka unutar tvrtke se odvija korištenjem intranet mreže ili kriptiranih medija za pohranu podataka. Prijenos podataka između tvrtke i treće strane se vrši preko kriptirane VPN veze.

Kontrola A.14.2 Dodatka A norme ISO/IEC 27001:2013: Sigurnost razvojnog procesa i podrške

Izrađena je procedura postupanja koja definira zahtjeve u slučajevima kada je potrebno postojeći proizvod (softver) potrebno nadograditi ili ažurirati, s ciljem zadržavanja postojeće informacijske sigurnosti. Svaku izmjenu ili doradu je potrebno dokumentirati s informacijama tko je izmjenu napravio, na koji način i sa kojim ciljem. Sama izmjena ne smije ni na koji način negativno utjecati na postojeću sigurnost. U slučaju potrebe za angažiranjem treće strane, treća strana mora osigurati identične uvjete sigurnosti kao da je zaposlenik tvrtke.

Kontrola A.14.3 Dodatka A norme ISO/IEC 27001:2013: Testiranje s podacima

Izrađena je procedura koja propisuje na koji način se radi testiranje proizvoda sa stvarnim podacima te na koji način ti podaci osiguravaju. Procedura zahtjeva da se prilikom preuzimanja stvarnih podataka, osjetljivi podaci kao što su osobni podaci, korisnička imena i lozinke, zamjenjuju izmišljenim podacima. Na taj način se minimalizira šteta od eventualnog gubitka takvih podataka. Project manager se definira kao odgovorna osoba za provođenje ovog postupka.

Kontrola A.16.1 Dodatka A norme ISO/IEC 27001:2013: Upravljanje sigurnosnim incidentima

Izrađena je procedura kako bi se osigurao dosljedan i učinkovit pristup upravljanju sigurnosnim incidentima, uključujući komunikaciju o sigurnosnim događajima i slabostima. Sistem administrator je odgovoran sa stalno praćenje stanja u mreži, detekciju i odgovor na

sigurnosne incidente, prikupljanje dokaza nakon napada na mrežu te vođenje i ažuriranje baze znanja vezane uz sigurnosne incidente.

4.2.7. Interni audit

Interni audit je mehanizam interne provjere sustava upravljanja informacijskom sigurnosti od strane same organizacije, a za što je definiran zasebni zahtjev norme ISO/IEC 27001:2013. Navedeni zahtjev obvezuje tvrtku da u pravilnim vremenskim intervalima (najčešće jednom svakih 12 mjeseci) organizira i provede ocjenu usklađenosti dokumentacije sustava upravljanja s primjenjivim zahtjevima norme te usklađenosti internog postupanja s onim kako je to opisano kroz dokumentaciju sustava upravljanja.

Nalaz internog audita se koristi na način da se utvrđeni nedostatci i odstupanja otklanjaju odgovarajućim popravnim radnjama kako bi se osiguralo poboljšanje učinkovitosti sustava upravljanja te efikasnost samog sustava.

Interni audit provode prikladno educirani djelatnici tvrtke koji moraju posjedovati znanje o zahtjevima norme i primjenjivih kontrola te o metodologiji provedbe internog audita.
Tvrtka kroz postupak planiranja osigurava kompetentnost i nepristranost internih auditora pri čemu zahtjev nepristranosti znači da osoba ne može biti odgovorna za provedbu internog audita u onom dijelu tvrtke za koji je direktno odgovorna jer bi ju to dovelo u sukob interesa prilikom procjenjivanja vlastitog rada.

U konkretnom slučaju je tvrtka organizirala i provela interni audit u ukupnom trajanju od dva radna dana tijekom kojeg su 2 interna auditora, uz uvažavanje principa osiguravanja nepristranosti, provela interni audit tijekom kojeg je ocijenjena ukupna usklađenost sustava upravljanja sa zahtjevima norme ISO/IEC 27001:2013.

Tijekom internog audita je utvrđeno 8 nesukladnosti te 4 preporuke. Za utvrđene nesukladnosti provedene su popravne radnje kako bi se osiguravalo da se iste nesukladnosti ne ponove na nekom drugom mjestu u sustavu.

4.2.8. Upravina ocjena

Upravina ocjena je ocjena koju slijedom zasebnog zahtjeva norme donosi najviša uprava tvrtke, a u kojoj sljedeći zahtjeve norme daje osvrt i ocjenu funkcioniranja uspostavljenog sustava upravljanja informacijskom sigurnosti.

Upravinu ocjenu potpisuje direktor tvrtke, a u njoj obrazac zahtijeva komentiranje aktivnosti iz prethodne upravine ocjene (s obzirom da je ovo prva provedena upravina ocjena, ova će se točka moći komentirati tek u sklopu naredne upravine ocjene), promjene i situaciju po pitanju unutarnjih i vanjskih pitanja koja su relevantna za uspostavljeni sustav, povratne informacije o izvedbi sustava kroz sagledavanje popravnih radnji slijedom utvrđenih nesukladnosti, rezultata praćenja i mjerenja unutar sustava, rezultata internog audita, ispunjenje ciljeva sustava upravljanja informacijskom sigurnosti, povratne informacije zainteresiranih strana, rezultate analize rizika te tretiranja prepoznatih rizika te prilike za poboljšanje.

Izlazni rezultati upravine ocjene su uključili odluke koje se odnose na neprekidno poboljšanje sustava upravljanja te potrebne i planirane aktivnosti unutar sustava.

Upravina ocjena je dokumentirana te iskomunicirana među odgovornim osoba za sustav upravljanja informacijskom sigurnosti na različitim hijerarhijskim razinama tvrtke.

4.2.9. Certifikacija sustava

Tvrtka je putem javnog poziva objavila poziv zainteresiranim certifikacijskim kućama za provedbu postupka certifikacije tvrtke prema zahtjevima norme ISO/IEC 27001:2013. Kako bi se osigurala međunarodna prihvaćenost izdanog certifikata, jedan od zahtjeva tvrtke je bio da certifikacijska kuća bude akreditirana od strane međunarodno prihvaćenog akreditacijskog tijela te da ima minimalno 3 odrađena certifikacijska audita u području djelatnosti tvrtke. Zaprimljene su 3 ponude za usluge certifikacije te je između njih 3 odabrana najpovoljnija.

Odabrana certifikacijska kuća je u ukupnom trajanju od 5 dana provela postupak certifikacije tvrtke pri čemu je od spomenutih 5 dana, u ukupnom trajanju od 1,5 dan provedena ocjena dokumentacije sustava upravljanja, a u trajanju od dodatnih 3,5 dana ocjena na licu mjesta u samoj tvrtki.

Nalaz certifikacijske kuće je bio takav da su utvrđene 2 nesukladnosti te 4 preporuke. Nesukladnosti su otklonjene u naredna 3 tjedna dok su preporuke analizirane te će se u vremenu do idućeg audita certifikacijske kuće provesti radnje na unaprjeđenju sustava kako bi se prepoznate preporuke ugradile u sustav upravljanja.

Nakon otklanjanja nesukladnosti, tvrtki je dodijeljen certifikat ISO 27001:2013 s rokom valjanosti od 3 godine čime je projekt uvođenja sustava upravljanja informacijskom sigurnosti u tvrtku uspješno zaključen.

4.3. Kritični faktori implementacije norme

Brojni autori istraživali su kritične faktore implementacije u sustavima upravljanja prema različitim normama. Analizom istraživanja [14] došlo se do niza kritičnih faktora upravljanja kvalitetom no oni koji se ističu i zajednički su za sve sustave upravljanja uspostavljene prema nekoj od međunarodnih normi su:

- Opredijeljenost najviše uprave
- Uključenost zaposlenih
- Kontinuirano poboljšavanje

4.3.1. Opredijeljenost najviše uprave

Opredijeljenost najviše uprave smatra se jednim od ključnih čimbenika uspjeha organizacije u cjelini. To pokazuju i rezultati brojnih empirijskih istraživanja, dok o važnosti ovog faktora svjedoče i rezultati istraživanja u pojedinačnim tvrtkama diljem svijeta [14], kao što su: Asahi Breweries Ltd., Japan Xerox, Inc, USA, Dunlop, Ltd, Dow Coming-Pvt. Ltd, Australia itd.

Iz svih provedenih istraživanja zaključuje se da je upravo opredijeljenost najviše uprave presudna za uspješno upravljanje sustavom, jer kada menadžment organizacije uspostavi formalnu politiku upravljanja tada zaposlenici neće uspostavljati vlastite politike .
Drugim riječima, djelotvorno upravljanje sustavom počinje od vrha.

Od najviše uprave organizacije, norma ISO/IEC 27001 zahtijeva opredjeljenje i preuzimanje vodeće uloge u sustavu upravljanja informacijskom sigurnošću. Zahtjevi se odnose na:

a) vodstvo i opredjeljenje
b) politiku
c) zadatke, odgovornosti i ovlasti.

Najviša uprava je odgovorna da se dodijele odgovornosti i ovlaštenja za odgovarajuće zadatke te uloge u sustavu upravljanja informacijskom sigurnošću.

4.3.2. Uključenost zaposlenih

Uključenost zaposlenika u aktivnosti organizacije je nužan uvjet za poboljšanje kvalitete proizvoda i/ ili usluga. Ona pomaže zaposlenicima da unaprijede svoje sposobnosti, povećaju samopouzdanje, a isto tako ih obvezuje da uspjeh organizacije shvate kao vlastiti uspjeh. Unutar poduzeća treba raditi na tome da zaposlenici daju prijedloge i primjedbe za poboljšanje rada organizacije, pri čemu bi se najbolji prijedlozi posebno nagrađivali. Ostvariti puno sudjelovanje zaposlenika znači stvoriti pretpostavke za njihovu participaciju i uključenost u poslove što na kraju može dovesti do povećanja vrijednosti za kupce.

Osnovni preduvjet uspješne implementacije i održavanja sustava upravljanja informacijskom sigurnosti je osigurati da u funkcioniranje sustava budu uključeni svi zaposleni, da su svjesni svoje uloge te da aktivno doprinose poboljšanju sustava kroz davanje prijedloga za povećanje učinkovitosti i efikasnosti samog sustava.

4.3.3. Kontinuirano poboljšanje

Kontinuirano poboljšanje je filozofija unapređenja aktivnosti koje povećavaju uspjehe, a neuspjehe smanjuju. Koncepcijski temelj kontinuiranog poboljšanja nalazi se u Shewartovom ciklusu (Shewart Cycle), ili Demingovom krugu: planiraj-čini-provjeri-djeluj. Koncept neprekidnog poboljšanja procesa temelji se na pretpostavci da je svaki rad niz međusobno povezanih koraka i aktivnosti koji rezultiraju nekim izlazom. Stalna kontrola nad svakim korakom u radnom procesu, kao i stalno poboljšanje njegova izvršenja, smanjuje promjenjivost izlaza (proizvoda/usluge), poboljšava pouzdanost i raspoloživost procesa, odnosno osigurava konzistentnost izlaza.

Stalna poboljšanja procesa su nužna i zbog varijacija potreba i želja korisnika, pritisaka konkurencije, ali i optimizacije procesa u cilju smanjenja troškova. Poboljšanje se odnosi na sve procese u organizaciji, poslovne i tehnološke.

4.4. Koristi od implementacije norme u poslovanje

4.4.1. Unutarnje koristi od implementacije norme u poslovanje

Kad organizacija brzo raste, nakon kratkog vremena dođe do nesporazuma oko odgovornosti za informacijsku imovinu i sigurnost. ISO/IEC 27001:2013 pomaže organizacijama da postave jasne odgovornosti za informacijski rizik te na taj način osigurava siguran i učinkovit protok informacija unutar organizacije, pravovremenost i točnost informacija te sprječava gubitak, zlouporabu i neovlašteno mijenjanje podataka. Pomaže u upravljanju informacijama u svim oblicima, uključujući digitalni oblik, papirnati, intelektualno vlasništvo, podatke na uređajima, podatke u oblaku i osobne podatke, a u slučaju sigurnosnog incidenta omogućava brzu identifikaciju i reakciju na nastali incident. Norma ISO/IEC 27001:2013 poboljšava učinkovitost radnih praksi vezanih uz informacijsku sigurnost te pomaže zaposlenicima da razumiju rizike i provode sigurnosne kontrole kao dio njihove svakodnevne radne prakse, a osim toga, poboljšava sigurnosne aspekte odnosa s dobavljačima. Prema istraživanju koje je u jesen 2018. proveo Institut Ponemon , 56% organizacija doživjelo je sigurnosne incidente koje su uzrokovali njihovi dobavljači [15]. Prosječan broj trećih strana koje imaju pristup osjetljivim informacijama organizacije u stalnom je porastu [15]. Prekidom odnosa s dobavljačem, sigurnosni rizik ne nestaje što dodatno otežava upravljanje informacijskom sigurnosti. U konačnici implementacija norme ISO/IEC 27001:2013 dovodi do značajnih ušteda i poboljšanja učinkovitosti organizacije na svim razinama.

4.4.2. Vanjske koristi od implementacije norme u poslovanje

Certifikat ISO / IEC 27001:2013 pokazuje postojećim i potencijalnim kupcima da je organizacija poduzela sve potrebne korake za zaštitu svog poslovanja i dokaz je učinkovite interne sigurnosne prakse, što daje značajnu prednost u odnosu na konkurenciju koja nema implementiranu normu. Cyber prijetnje svakodnevno postaju sofisticiranije i nanose značajnu štetu ugledu i financijama pogođenih tvrtki. Prema nekim procjenama godišnje štete od cyber kriminala dosežu $600 milijardi USD, a vrlo vjerojatno te su brojke i znatno veće jer velik dio incidenata nikada nije evidentiran ili otkriven [16]. Osim negativne percepcije javnosti i potencijalno štetnog utjecaja na poslovanje dodatnu prijetnju predstavlja i sve veći broj zakonodavnih i regulatornih okvira koji od organizacija zahtijevaju odgovornije upravljanje

informacijskom sigurnošću te poduzimanje odgovarajućih mjera kako bi se umanjili rizici od potencijalnih cyber napada. Norma je u potpunosti u skladu sa strogim zahtjevima Opće uredbe o zaštiti podataka (GDPR) i Direktive o sigurnosti mrežnih i informacijskih sustava (NIS direktiva). Kao međunarodna norma, ISO/IEC 27001:2013 pruža organizacijama koje rade na globalnom tržištu priliku da pruže vjerodostojnost da njihovo poslovanje odgovara istim normama kao i normama njihovih partnera. Primjena norme ISO/IEC 27001:2013 pokazuje da organizacija održava sigurnosne prakse što će uvjeriti postojeće klijente da će organizacija poduzeti sve potrebne sigurnosne mjere kako bi zaštitila njihove povjerljive podatke i na taj način sačuvala njihovo povjerenje. Također, posjedovanje certifikata ISO/IEC 27001:2013 omogućuje organizaciji prijavu na natječaje koji zahtijevaju stroge kriterije informacijske sigurnosti te nerijetko uvjetuju posjedovanje certifikata.

5. Zaključak

Sve organizacije, bez obzira na tip, veličinu ili djelatnost posjeduju informacije koje predstavljaju osnovni resurs organizacije i koje za nju imaju iznimno veliku važnost.
U današnje vrijeme konkurentnih tržišta, otvorenih ekonomija, globalizacije i svakodnevnih prijetnji za informacije organizacije iz različitih unutarnjih ili vanjskih izvora, zaštita informacija od kompromitiranja i neovlaštenog pristupa predstavlja temeljni preduvjet opstanka i razvoja svake organizacije.

Sustav upravljanja informacijskom sigurnosti prema zahtjevima norme ISO/IEC 27001:2013 predstavlja skup zahtjeva i smjernica za zaštitu autentičnosti, jasno definiranje odgovornosti te osiguranje pouzdanosti kroz jasno definiranje prava i odgovornosti po pitanju pristupa te obradi informacija kojima organizacija raspolaže.

Prema podacima Međunarodne organizacije za normizaciju, broj certificiranih pravnih subjekata u svijetu po normi ISO/IEC 27001 u 2006. godini iznosio je 5797, 2012. godine taj broj je narastao na skoro 20 000, a 2017. godine se približio brojci od 40 000 izdanih certifikata. U očekivanju statističkih podataka za 2018. godinu, može se potvrditi da je na globalnoj razini vidljiv jasan porast značaja norme ISO 27001:2013, kao i potrebe za sustavnim, dokumentiranim, sveobuhvatnim i učinkovitim alatom upravljanja informacijskom sigurnosti u svim vrstama organizacija, bez obzira na njihovu veličinu, tip ili djelatnost kojom se bave.
Jasno definiranje odgovornosti i ovlaštenja po pitanju upravljanja, raspolaganja i osiguranja informacijske sigurnosti, siguran i učinkovit protok informacija unutar organizacije, pravovremenost i točnost informacija te sprečavanje gubitka, zlouporabe te neovlaštenog pristupa podataka temeljni su doprinosi norme ISO/IEC 27001:2013 organizaciji koja ju odluči implementirati u svoje poslovanje.

Prema van, certificirani sustav upravljanja informacijskom sigurnosti pokazuje i dokazuje postojećim i potencijalnim kupcima da je organizacija poduzela sve potrebne korake za zaštitu svog poslovanja, njihovih informacija i podataka te da je dokaz učinkovite interne sigurnosne prakse, a što organizaciji, u konačnici, osigurava konkurentsku prednost u odnosu na konkurenciju koja navedeni certifikat nema.

Tendencija da se posjedovanje certifikata sve više pojavljuje kao uvjet prijave na različite javne natječaje za dobivanje posla, jasno pokazuje da je sustavan pristup i osiguranje informacijske

sigurnosti prepoznato kao poželjan preduvjet poslovanja i gotovo pa uvjet međusobne ekonomske suradnje pravnih subjekata koji djeluju na globalnom ili lokalnom tržištu.

Norma ISO/IEC 27001:2013 je u potpunosti u skladu sa strogim zahtjevima Opće uredbe o zaštiti podataka (GDPR) te Direktive o sigurnosti mrežnih i informacijskih sustava (NIS direktiva) čime se osigurava ispunjenje i vrlo velikog postotka zahtjeva navedenih zakonskih dokumenata onda kada organizacija u svoje poslovanje uvede normu ISO/IEC 27001:2013.

Uvažavajući sve ranije izneseno, može se reći da važnost, prihvaćanje i prepoznatost norme ISO/IEC 27001:2013 u nacionalnim i međunarodnim okvirima postaje sve jasnija i važnija pretpostavka te uvjet za sve organizacije koje imaju jasnu želju i opredijeljenost za opstanak, razvoj i širenje kako na nacionalnom, tako i globalnom tržištu, slijedom čega implementacija norme ISO/IEC 27001:2013 u poslovanje organizacija predstavlja ne izuzetak ili poželjnu praksu, nego svojevrsni imperativ.

6. Literatura

[1] Hrvatska tehnička enciklopedija. Preuzeto sa: https://tehnika.lzmk.hr/tehnickaenciklopedija/standardizacija.pdf [Pristupljeno: svibanj 2020.]

[2] Hrvatski zavod za norme. Preuzeto sa: https://www.hzn.hr/default.aspx?id=90 [Pristupljeno: svibanj 2020.]

[3] Beck, N., & Walgenbach, P. (2005). Technical efficiency or adaptation to institutionalized expectations? The adoption of ISO 9000 standards in the german mechanical engineering industry. Preuzeto sa: https://journals.sagepub.com/doi/10.1177/0170840605054599 [Pristupljeno: svibanj 2020.]

[4] Brunsson N, Rasche A, Seidl D. The Dynamics of Standardization: Three Perspectives on Standards in Organization Studies. University of Zurich, 2012.

[5] Garud R, Jain S, Kumaraswamy A. Institutional Entrepreneurship in the Sponsorship of Common Technological Standards: The Case of Sun Microsystems and Java. 2002;45(1): 196-214.

[6] International Organization for Standardization. Preuzeto sa: https://www.iso.org/members.html [Pristupljeno: svibanj 2020.]

[7] IT governance. Preuzeto sa: https://www.itgovernance.co.uk/iso27000-family [Pristupljeno: svibanj 2020.]

[8] Advisera. Što je ISO 27001? Preuzeto sa: https://advisera.com/27001academy/hr/sto-je-iso-27001/ [Pristupljeno: svibanj 2020.]

[9] Gamma Secure Systems Limited. Preuzeto sa: http://www.gammassl.co.uk/27001/history.php [Pristupljeno: svibanj 2020.]

[10] The ISO Survey of Management System Standard Certifications – 2018 – Explanatory Note. Preuzeto sa: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_on_ISO_Survey_2018_results.pdf?nodeid=20719021&vernum=-2 [Pristupljeno: svibanj 2020.]

[11] International Organization for Standardization. Preuzeto sa: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 [Pristupljeno: svibanj 2020.]

[12] Hrvatski zavod za norme. Informacijska tehnologija – Sigurnosne tehnike – Sustavi upravljanja informacijskom sigurnošću – Zahtjevi (ISO/IEC 27001:2013), Zagreb, 2014.

[13] Fakultet organizacije i informatike. Preuzeto sa: https://security.foi.hr/wiki/index.php/Izgradnja_ISMS-a_i_certificiranje_po_normi_ISO_27001.html [Pristupljeno: lipanj 2020.]

[14] Šiško Kuliš M, Grubišić D. Kritični faktori uspjeha u sustavima upravljanja kvalitetom. Strojarstvo : časopis za teoriju i praksu u strojarstvu. 2011;53(5): 405-414

[15] RSA Conference. Preuzeto sa: https://www.rsaconference.com/industry-topics/blog/national-supply-chain-integrity-month-understanding-third-party-cyber-risk [Pristupljeno: svibanj 2020.]

[16] CNBC. Preuzeto sa: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html [Pristupljeno: svibanj 2020.]

POPIS SLIKA

Slika 1. PDCA model 5
Slika 2. Grafički prikaz razvoja norme ISO/IEC 27001:2013 9
Slika 3. Struktura dokumentacije sustava upravljanja informacijskom sigurnosti 20
Slika 4. Tlocrt prizemlja 32
Slika 5. Tlocrt 1. kata 33
Slika 6. Koraci implementacije norme ISO/IEC 27001:2013 34

POPIS TABLICA

Tablica 1. Broj izdanih certifikata u svijetu od 2006. do 2017. godine 9
Tablica 2. Usporedba izdanih certifikata u Hrvatskoj i nekim europskim zemljama 10
Tablica 3. Broj izdanih certifikata u Hrvatskoj u 2018. godini, po djelatnostima 12
Tablica 4. Pregled zahtjeva norme 13
Tablica 5. Pregled obaveznih dokumentiranih informacija u sustavu upravljanja informacijskom sigurnosti 21
Tablica 6. Kontrole iz Dodatka A norme ISO/IEC 27001:2013 28
Tablica 7. Dokumentacija sustava upravljanja informacijskom sigurnosti 36

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **UNAPRJEĐENJE SIGURNOSTI POSLOVNOG OKRUŽENJA IMPLEMENTACIJOM NORME ISO/IEC 27001:2013** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 14.09.2020.

Student/ica:

Zoran Malekovic

(potpis)