Standardi i okviri upravljanja sigurnošću informacijskih sustava

Pokorni, Marta

SVEUČILIŠTE JURJA DOBRILE U PULI

FAKULTET EKONOMIJE I TURIZMA „DR. MIJO MIRKOVIĆ“ PULA

MARTA POKORNI

STANDARDI I OKVIRI UPRAVLJANJA SIGURNOŠĆU INFORMACIJSKIH SUSTAVA

INFORMATION SECURITY MANAGMENT: FRAMEWORKS AND STANDARDS

ZAVRŠNI RAD

PULA, 2019.

SVEUČILIŠTE JURJA DOBRILE U PULI

FAKULET EKONOMIJE I TURIZMA „DR. MIJO MIRKOVIĆ“ PULA

STANDARDI I OKVIRI UPRAVLJANJA SIGURNOŠĆU INFORMACIJSKIH SUSTAVA

INFORMATION SECURITY MANAGMENT: FRAMEWORKS AND STANDARDS

ZAVRŠNI RAD

Kolegij: Elektroničko poslovanje

Mentor: prof. dr. sc. Vanja Bevanda

Studentica: Marta Pokorni

Studij: Preddiplomski studij informatičkog menadžmenta

JMBAG: 0242036660

Pula, rujan 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 17.09.2019. godine

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____Standardi i okviri upravljanja sigurnošću informacijskih sustava__ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 17.09.2019.

Potpis

_____

SAŽETAK

U modernom vremenu u kojem živimo važno je spoznati značaj informacijskih sustava te iste štititi na prikladan način. Kako su informacije glavni adut poslovanja logično je da postoje razni zakoni, institucije, standardi, procedure, pravila te mjere koji se koriste za zaštitu informacijskih sustava. Primjenom navedenih načina zaštite, informacijskih se sustav brani od neželjenih prijetnji, odnosno rizik se drži na optimalnoj razini kako bi se zaštitilo kompletni sustav.

Ključne riječi: sigurnost, informacijski sustavi, standardi i okviri sigurnosti, kontrola

SUMMARY

In the modern times we live in, it is important to understand the importance of information managment and to protect them in an appropriate way. As information is a major asset of business, it is logical that there are various laws, institutions, standards, procedures, rules and measures used to protect information systems. By applying these security methods, the information system is protected against unwanted threats, that is, the risk is kept at the optimum level to protect the complete system.

Keywords: security, information managment, security standards and frameworks, control

SADRŽAJ

1. UVOD

Pojam sigurnost u današnje se vrijeme olako shvaća; ne pridodaje se dovoljno pažnje jer postoji određena „prividna“ sigurnost. Primjerice sigurnost na internetu – smatra se kako je Internet veliko osigurano područje, te se na različitim web stranicama dijele osobni podaci, brojevi kartica i slično, pa kada s računa nestanu sredstva, nastaje panike i tek onda dolazi do pojedinca – koliko je doista sigurno dijeliti navedene podatke!?

Baš zbog navedenih problema koji su nastaju svakodnevno, a koji za sobom vuku određenu dozu nesigurnost, sve je više sustava i standarda koji garantiraju sigurnost i kvalitetu.

Kada bi promatrali gdje spadaju sami standardi, uvrstili bi ih pod kontrole provedbe sigurnosne informacijske politike, odnosno informatičke kontrole koje možemo razvrstati prema okvirima ili normama koje se koriste pri procjeni njihove učinkovitosti i efikasnosti. Tu se već radi o specifičnim pogledima na kontrolne informacijske sustave, a okviri i norme koje se u svjetskim razmjerima najčešće pri tome koriste su CobiT, ITIL I ISO 27000 norme.

2. OPĆENITO O SIGURNOSTI INFORMACIJSKOG SUSTAVA, POJMOVI

2.1. Sigurnost

Sigurnost je, kako navodi Cingula[1], „osjećaj pojedinca da je zaštićen (engl. safe, protected) od fizičke, društvene, duhovne, novčane, političke, ekonomske, osjećajne, profesionalne, psihološke, odgojne ili bilo koje druge prijetnje, opasnosti, štete, povrede ili bilo kakvog događaja koji se može tumačiti kao neželjen. Također, navodi da je sigurnost kontrola neizvjesnosti pri čemu se prepoznata opasnost svodi u granice prihvatljivog rizika.“

Bez obzira na definiciju, sigurnost nije proizvod ili završno stanje, već proces.

Kada se govorimo o sigurnosti i zaštiti informacijskih sustava i mreža, nekoliko principa danas vrijede kao osnovna načela:

- Sigurnost je proces. Sigurnost nije gotov proizvod, usluga ili procedura, već skup koji i sadržava, u još mnogo elemenata koje se stalno provode;
- Ne postoji apsolutna sigurnost;
- U različite metode te zaštite, treba imati u vidu i ljudski faktor, sa svi slabostima. Uz navedene principe u literaturi se nerijetko spominje i da je sigurnost način razmišljanja te da ona nije samo pitanje tehnologije i zaštite;

2.2. Informacijska sigurnost

Informacija se može definirati kao „podatak s određenim značenjem, odnosno saznanje koje se može prenijeti u bilo kojem obliku (pisanom, audio, vizualnom, elektronskom ili nekom drugom)”.[2]

Informacija se smatra jednom od najvažnije i najdragocjenije imovine odnosno resursa. Njezino posjedovanje i tajnost u pravom trenutku može biti od iznimne važnosti u

[1] Cingula M. : "KORPORATIVNA SIGURNOST - Pojam sigurnosti i temeljni srodni pojmovi", http://web.efzg.hr/dok/MAR/avuletic/01_Pojam%20sigurnosti.pdf

[2] Prof.dr.sc. Mario Spremić „Digitalna transformacija poslovanja“, Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet, 2017. godine

poslovanje svake organizacije. Ako ovo uzmemo u obzir, informaciju je potrebno zaštititi što je danas iznimno teško jer su informacije svima dostupne, te su samim time izložene raznim prijetnjama.

Pojam informacijske sigurnosti ne odnosi se samo na određene tehničke mjere zaštite kao korisnička imena, lozinke, prava pristupa i slično, već se odnosi i na administrativne i organizacijske mjere poput sigurnosne politike, pravilnika i raznih procedura. Informacija bi trebala uvijek biti adekvatno zaštićena, bez obzira o kojem se obliku radi. Kako bi informacijski sustav bio zaštićen, potrebno je pravilno uskladiti, implementirati i nadgledati odnosno pregledavati i poboljšavati sve potrebne mjere kako bi se osiguralo ispunjenje sigurnosnih i poslovnih zahtjeva organizacije. Osobe koje se bave ovim područjem svakako bi morale biti svjesne kako sigurnost informacija može biti izuzetno važna – zbog konkurentnosti, kako bi se osigurala profitabilnost, odnosno kako bi se poslovalo po zakonskim propisima, a samim time da se očuva poslovni ugled.

Pod pojmom informacijske sigurnosti[3] podrazumijeva se zaštita informacija od velikog broja prijetnji kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija.

Informacijska sigurnost uključuje:

- oporavak informacijskih sustava

- odvraćanje napada

- primjenu zakonskih propisa koji se odnose na privatnost, računalni kriminal i slično[4]

Također, u tome se kontekstu sve više spominje pojam osiguravanja informacija (engl. *Information Assurance*), kao sinonim za informacijsku sigurnost, najviše zbog preširokog poimanja riječi sigurnost. Osiguravanje informacija u tom smislu predstavlja

[3] Marijanović .: " UPRAVLJANJE SIGURNOŠĆU INFORMACIJA", FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA, SVEUČILIŠTE U ZAGREBU, ., http://sigurnost.zemris.fer.hr/ISMS/2006_marijanovic/Marijanovic.pdf

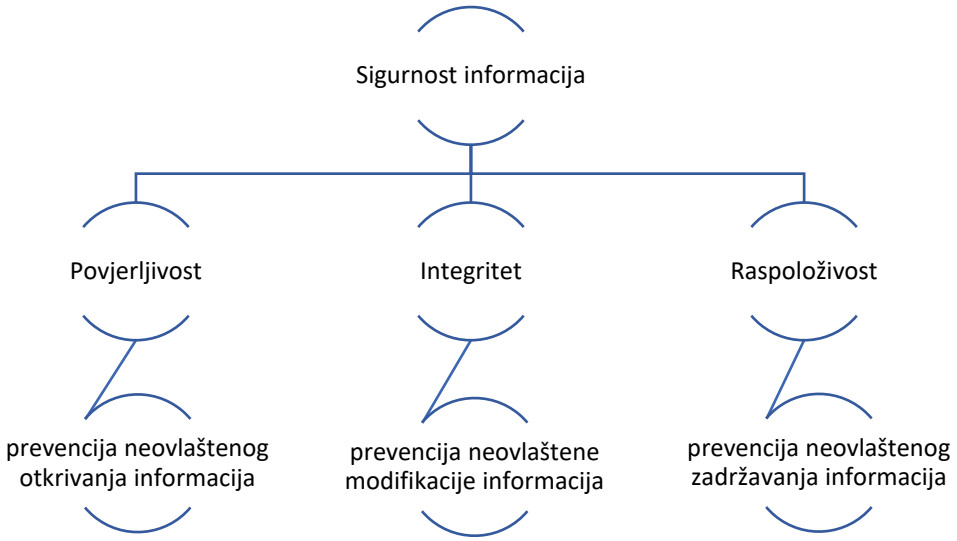
[4] https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf

međudjelovanje tehnologije i ljudi koji omogućavaju rad tehnologije u operativnoj uporabi.[5]

Informaciju je potrebno zaštiti na sljedeće načine: [6]

I. osigurati integritet
II. osigurati povjerljivost
III. osigurati dostupnost

Slika 1: Sigurnost informacija

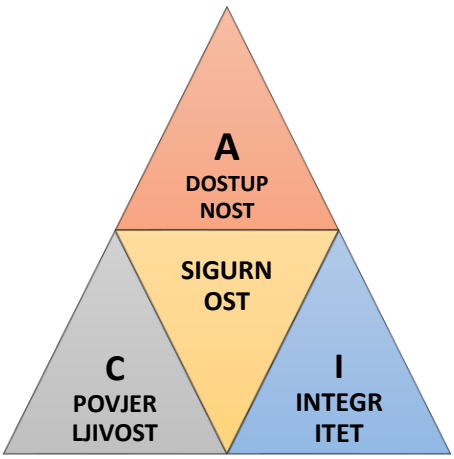


Izvor: izrada autora prema „Integralni okvir za sigurnost i pouzdanost“, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2001-03-02.pdf

U području informacijske sigurnosti ovo se označava kao očuvanje C-I-A, gdje je C – Confidentiality, I – Integrity, A – Availability (u prijevodu: povjerljivost, integritet i dostupnost).
U literaturi se ova tri pojma povezuju i prikazuju kroz tzv. Sigurnosni trokut (engl. *CIA triad*).

[5] Klaić A.: „Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodologija a upravljanja informacijsko sigurnošću”
[6] https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf

Slika 2: Sigurnosni trokut (CIA traid)



Izvor: izrada autora prema „CIA traid“ www.ibm.com

Jedan od primjera bio bi ID korisnika i lozinke. U ovom su slučaju jako bitne sigurnosne kopije. Integritet podrazumijeva održavanje dosljednosti, točnosti i pouzdanosti podataka u cijelom ciklusu. Povjerljivost je osmišljena kako bi se spriječilo da osjetljivi podaci ne dođu do pogrešnih ljudi. Dostupnost se odnosi na pravodobnu dostupnost informacija osobi koja je u datom trenutku treba.

3. SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU (ISMS)

Sustav upravljanja informacijskom sigurnošću (engl. *Information Security Managment System*) dio je sveukupnog sustava upravljanja, utemeljen na pristupu upravljanju rizicima, u cilju suprotstavljanja, provođenja, praćenja, revidiranja, održavanja i unaprjeđenja informacijske sigurnosti.[7]

Sustav zapravo opisuje i demonstrira svoj organizacijski pristup informacijskoj sigurnosti. Uključuje način na koji se ljudi, politike, kontrole i sustavi identificiraju, a zatim rješavaju mogućnosti i prijetnje koje se vrte oko vrijednih informacija i povezanih sredstava.

[7] HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005, www.hzn.hr, www.iso.org

Uspješno uspostavljanje ISMS-a je bitno zbog zaštite informacija kako bi organizacija:
- postigla veću garanciju sigurnosti

- kako bi održavala sveobuhvatni okvir za identifikaciju i procjenu rizika

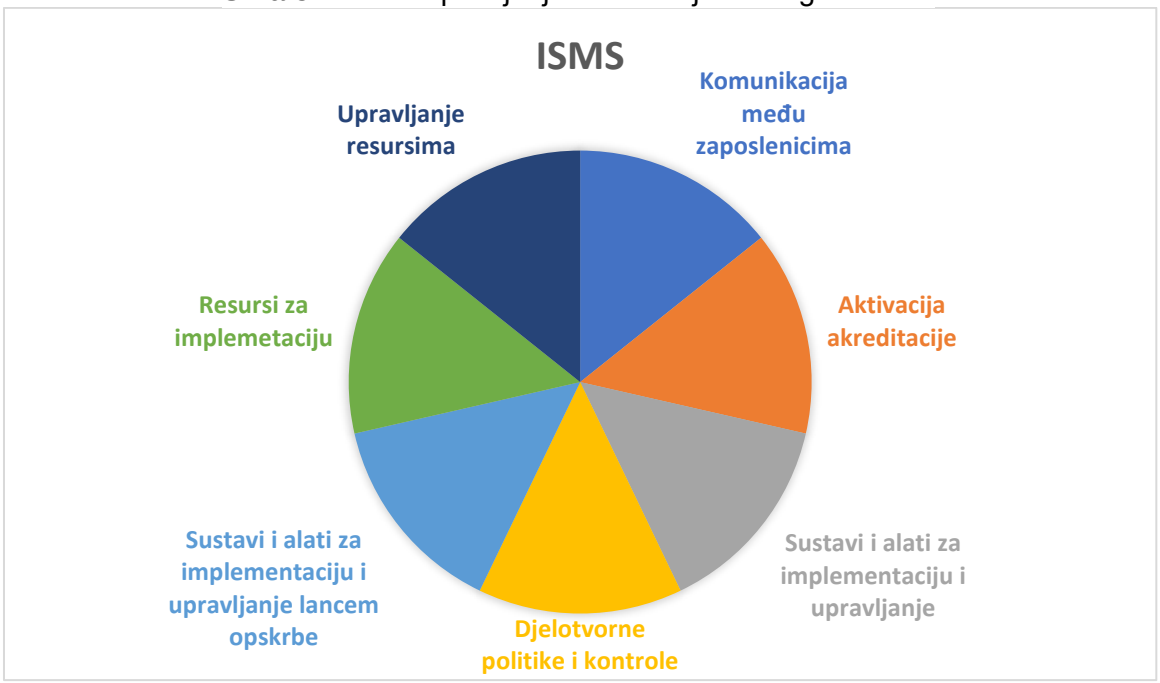
- kako bi konstantno mogla poboljšavati kontrolu okoline

- da bi postizala zakonsku i regulativnu usklađenost

Kako bi se postavio temelj informacijske sigurnosti i odredio njezin okvir, odnosno da bi se omogućilo razumijevanje sigurnosnih zahtjeva organizacije i potrebe za samim uspostavljanjem ciljeva na području sigurnosti, upotrebljavaju se standardi/norme o kojima će biti više riječi u poglavlju 4.

Učinkovit sustav upravljanja informacijskom sigurnošću sastoji se od sedam elemenata. Stvarna veličina tih dijelova dijagrama, u smislu vremena i troškova, ovisi o ciljevima organizacije, o početnoj točki te o opsegu koji se želi uključiti u ISMS. Ulaganje u jedan dio pomoći će smanjiti ili izbjeći mnogo veća ulaganja u ostale dijelove.

Slika 3: Sustav upravljanja informacijskom sigurnošću



Izvor: izrada autora prema http://isms.online/isms/

4. STANDARDI UPRAVLJANJA SIGURNOŠĆU INFORMACIJSKIH SUSTAVA

„Standard sadrži strukturirani set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću. Implementacija sigurnosnih kontrola po standardima ne samo da onemogućava previd pojedinih kontrola, već je i dokaz kvalitete uspostavljenih sigurnosnih kontrola.“[8]

„Norme su javno objavljivanje specifikacije koje u domeni informacijske sigurnosti daju metodologiju kako riješiti pojedine aspekte informacijske sigurnosti.“[9]

Nakon što se sagledaju zahtjevi vezani uz sigurnosti, te se izradi procjena rizika, potrebno je implementirati i odabrati ispravne kontrole kako bi se rizik doveo na prihvatljivu razinu. Odabir kontrola ovisi o organizaciji – o mogućnosti prihvaćanja rizika, načinu upravljanja rizikom, ali i o nacionalnim i međunarodnim zakonskim propisima i obvezama.

Međunarodni standardi, odnosno norme, koje se odnose na informacijsku sigurnost izrađeni su kako bi organizacijama pomogli da uspostave sustav upravljanja informacijskom sigurnošću. Organizacije koje se potrude i steknu certifikate koji potvrđuju sukladnost sa zahtjevima međunarodnih normi, mogu na taj način zadovoljiti zahtjeve zakonodavca, a istovremeno steći povjerenje poslovnih partnera i kupaca, što im daje poslovne prednosti na tržištu. Radi toga se spomenute organizacije kod kojih čitatelj može pronaći norme i standarde informacijske sigurnosti te mnoštvo korisnih uputa i savjeta o tome kako uspostaviti sustav upravljanja informacijskom sigurnošću.

Standardi koji su od velike važnosti za sigurnost informacijskih sustava su: ISO 27001 – Sustav upravljanja informacijskom sigurnošću i ISO 27002 – kodeks postupaka za upravljanje informacijskom sigurnošću. Kako bi se postigao kvalitetan sustav za upravljanje sigurnošću informacija, poželjno je korištenje oba standarda.

Ova dva standarda glavni su međunarodni standardi informacijske sigurnosti – objavila je Internacionalna organizacija za standardizaciju (ISO). Oni se smatraju najvažnijim s obzirom da su fleksibilni, da mogu definirati upravljački okvir, te ne ulaze u konkretnu

[8] Bogati, J., „Praktični menadžment“, str. 112-117, Zagreb, 2011. godina
[9] A. Kaić, „Općenito o standardima i normama“, https://www.cis.hr/www.edicija

tehničku implementaciju, pa se mogu primjenjivati u gotovo sve organizacije. One se konstantno mijenjaju i ažuriraju kako bi bile dio sustava u kojem se usklađuju s drugim normama (npr. s normom ISO 9001 – upravljanje kvalitetom poslovanja) i međusobno.

Uz ova dva glavna standarda, postoji i mnogo drugih koji su vezani uz probleme zaštite i sigurnosti informacijskih sustava, koji su do sada već doneseni ili su pak planirani u budućnosti:

- ISO 27000 – Rječnik termina koji se koriste unutar ISO 27000 serije standarda
- ISO 27003 – Vodič za implementaciju ISMS-a
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti
- ISO 27006 – Zahtjevi za postupkom analize i certificiranja standarda
- ISO 27007 – Upute za analizu ISMS-a
- ISO 27011 – Upute za uspostavu ISMS u telekomunikacijskom sektoru
- ISO 27031 – Specifikacije za ICT odjel pripremljenosti poslovne prekinutosti rada
- ISO 27032 – Upute za *cyber* sigurnost
- ISO 27034 – Upute za sigurnost aplikacija
- ISO 27799 – Sigurnosni sustav u zdravstvu

4.1. ISO 27001 – sustav upravljanja informacijskom sigurnošću

Međunarodni standard koji izdaje ISO i IEC; služi za upravljanje, implementiranje i održavanje sustava za upravljanje informacijskom sigurnošću.

Norma se bavi uspostavom sustava koji upravlja informacijskom sigurnošću, koji se označava kraticom ISMS. Najbolji svjetski stručnjaci na poljima informacijske sigurnosti napisali su ovaj standard. Također, oni propisuju metodologiju za primjernu upravljanja informacijskom sigurnošću u samoj organizaciji. U ovoj su normi ciljevi određeni kako bi organizacija mogla pratiti, odnosno kako bi postigla učinkovit sustav zaštite svojih podataka i informacija. Formalno ne propisuje posebne sigurnosne kontrole informacija, budući da se potrebne kontrole značajno razlikuju u širokom rasponu organizacija koje prihvaćaju standard. Kod ovog standarda organizacije mogu slobodno birati koje će specifične kontrole sigurnosti primjenjivati na njihove

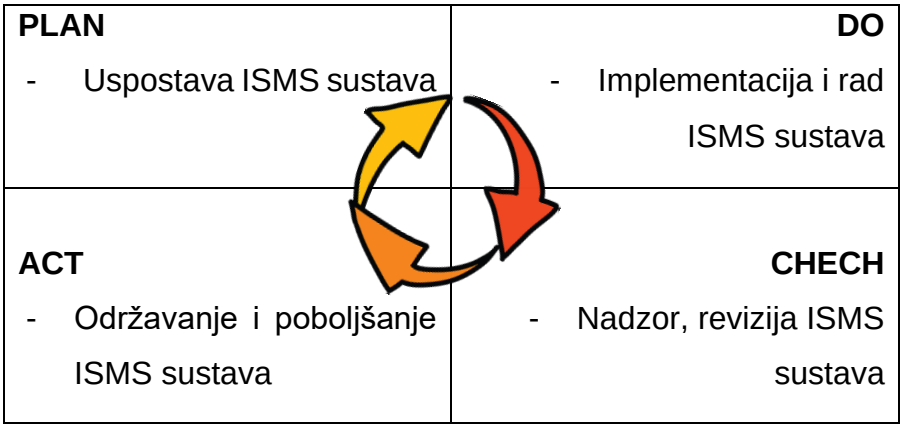
specifične rizike informacija, oslanjajući se na one navedene u izborniku i potencijalno ih dopunjavajući s drugim mogućnostima.

Standard može biti implementiran u bilo kojim organizacijama, bilo da se radi o profitnim ili neprofitnim, privatnim ili državnim, odnosno malim ili velikim.

Neovisno certifikacijsko tijelo daje potvrdu da je tvrtka implementirala informacijsku sigurnost, odnosno omogućava organizacijama dobivanje certifikata ISO 27001.

Za uspješnu provedbu zadataka ova norma koristi procesni pristup koji omogućuje razumijevanje sigurnosnih zahtjeva tvrtke i potrebu za ostvarenjem ciljeva na području informacijske sigurnosti. Na slici 4 prikazan je PDCA model kojeg koristi norma ISO 27001 za uspješno provođenje svojih zadataka.

Slika 4: PDCA model



Izvor: izrada autora prema Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str. 60

PDCA model sastoji se od četiri koraka: Plan, Do, Act i Check. Plan/planiranje označava uspostavu ISMS politike, ciljeva, procesa i procedura za upravljanje rizikom i poboljšanje informacijske sigurnosti. Do odnosno primjena veže se na implementaciju i rad ISMS kontrola, procesa i procedura. Check/provjera označava procjenu i mjerenje učinkovitosti procesa, kontrola i ciljeva te priprema izvještaja za reviziju ISMS sustava. Posljednji korak u ovom procesu je Act/djelovanje u kojem se poduzimaju preventivne mjere na temelju rezultata interne revizije i revizije uprave i ostalih relevantnih informacija u cilju poboljšanja ISMS sustav.[10]

[10] „Sigurnost informacijskih sustava: priručnik“, Zagreb, Algebra, 2010., str. 63

Važno je da model nikad ne dolazi do kraja, već se ove četiri faze moraju odvijati konstantno kako bi ISMS pravilno funkcionirao.

ISO 27001 je fokusiran na zaštitu cjelovitosti, provjerljivosti i raspoloživosti podataka u tvrtki. To postiže procjenom rizika – prepoznavanjem koji se mogući problemi mogu dogoditi podacima, te obradom rizika – definiranjem što treba poduzeti da se takvi problemi spriječe. Zapravo, temelj ISO 27001 je u upravljanju rizikom: prepoznavanje i sustavna obrada rizika.

Sigurnosne mjere koje će se implementirati su u formi politika, procedura i tehničke primjene (softver i oprema). U stvarnosti, većina poduzeća već ima potreban hardver i softver, samo što ih koristi na pogrešan, nesiguran način. Iz tih se razloga većina primjene ISO 27001 odnosi na pisanje dokumenata tj. uspostava organizacijskih propisa koji su neophodni da bi se spriječilo narušavanje sigurnosti. Znači, upravljanje informacijskom sigurnošću ne odnosi se isključivo na IT sigurnosti (zaštita od virusa, firewall i slično) nego i na upravljanje procesima, pravnu zaštitu, upravljanje ljudskim resursima, fizičku zaštitu…

4.2. ISO 27002 – kodeks postupaka za upravljanje informacijskom sigurnošću

ISO 27002 je norma koja pobliže opisuje način na koji će se provesti mjere zaštite iz ISO 27001. Ova norma predstavlja međunarodnu osnovu za razumijevanje i upravljanje informacijskom sigurnošću, a sastoji se od 11 domena koje opisuju sigurnosne kontrole. Navedene domene sastoje se od 39 kontrolnih ciljeva i ukupno 133 kontrola koje pomažu u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima su informacije svakodnevno izložene.[11]

Zapravo, norma ISO 27002 do 01. srpnja 2007. g. nosila je naziv Norma ISO/IEC 17799 koja je preuzeta iz prvog dijela BS 7799 standarda "Code of Practice for Information Security Management".

[11] Bogati, J., NORME INFORMACIJSKE SIGURNOSTI ISO/IEC 27K ,Praktični menadžment, Vol. II, br. 3, str. 112-117, 2011 godina

Da bi se kontrole i kontrolni mehanizmi izradili u skladu s uputama ISO 27001, potrebne su smjernice koje nudi norma ISO 27002. Ovo zapravo nije upravljačka norma stoga se po njoj ne može certificirati.

Sigurnosne mjere u normi ISO 27002 nose iste nazive kao i one u Aneksu A norme ISO 27001 pa tako u normi ISO 27002 mjera 6.1.5 ima naslov Sporazumi o tajnosti, te u normi ISO 27001 pod istim imenom A.6.1.5 Sporazumi o tajnosti. Razlika između ove dvije norme, zapravo je u količini detalja koji su posvećeni određenoj sigurnosnoj mjeri. Tako je za istu sigurnosnu mjeru u normi ISO 27001 objašnjeno tek jednom rečenicom, dok je u normi ISO 27002 detaljnije objašnjena ta ista sigurnosna mjera; toliko detaljnije da je zauzeta gotovo cijela stranica. Posljednja objavljena verzija standarda Sustava upravljanja informacijskom sigurnošću je - BS EN ISO / IEC 27001: 2017. Izdanje za 2017. nije utjecala na ISO verziju standarda (2013) i izmjene ne uvode nikakve nove zahtjeve.

4.3. ITIL

ITIL proces upravljanja informacijskom sigurnošću koji opisuje pristup i kontrolira mjeru IT sigurnosti unutar organizacije.

ITIL ISM proces je temelj procesa ITIL upravljanja sigurnošću. Primarni cilj upravljanja informacijskom sigurnošću, proces ITIL V3, je efikasna kontrola pristupa organizacijskim informacijama. ISM ima snažan odnos s drugim ITIL procesima kao što su upravljanje dostupnosti i upravljanja kontinuitetom IT usluga za taj resurs i za nepredviđene planiranje.

Također, koordinira i upravljanjem rizika zbog provjere bilo kojeg narušavanja sigurnosti. Isto tako koordinira se s postupkom upravljanja promjenama radi provjere i potvrđivanja svih predloženih promjena iz točke sigurnosti organizacije.

Primarni cilj procesa upravljanja informacijskom sigurnošću ITIL-a (ITIL ISM) je uskladiti IT sigurnost s poslovnom sigurnošću i osigurati da se informacijskom sigurnošću učinkovito upravlja u svim uslugama i poslovima upravljanja IT uslugama. Osigurava povjerljivost, integritet, dostupnost sredstava, informacija, podataka i IT usluga.

Prema ITIL-u V3, ISM ima četiri podprocesa; prikazano na slici 5.

I. Dizajn sigurnosnih kontrola

Odgovorna je za osmišljavanje odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala povjerljivost, integritet, sigurnost i dostupnost imovine, informacija, podataka i usluga organizacije. Može se svrstati u administrativnu, logičku i fizičku kontrolu.

II. Provjera sigurnosti i testiranje

Odgovoran je za redovita ispitivanja i provjeru učinkovitosti aktivnosti i implementacije IT sigurnosti.

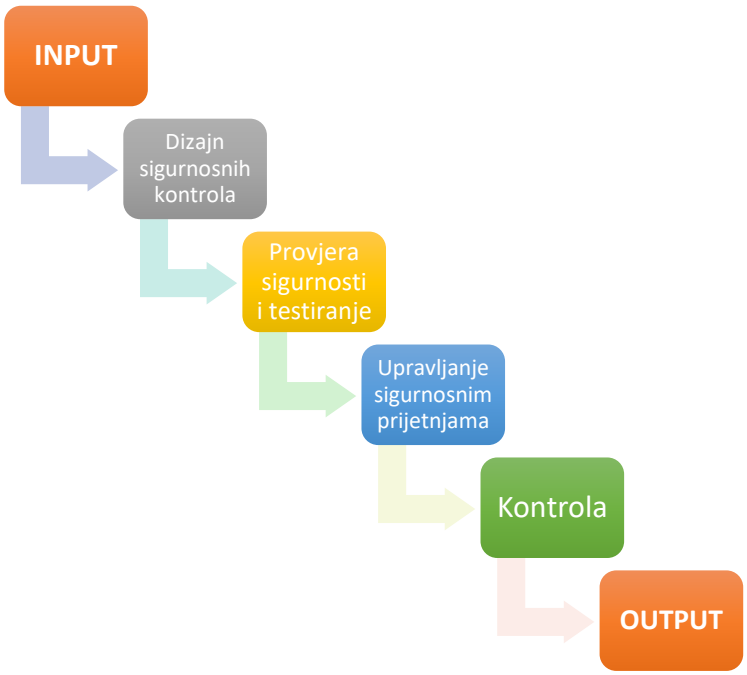
III. Upravljanje sigurnosnim prijetnjama

Otkrivanje i reakcije protiv sigurnosnih prijetnji odnosno minimiziranje štete nastale kršenjem sigurnosti.

IV. Kontrola

Preispitati jesu li mjere sigurnosti i postupci još uvijek u skladu s očekivanim rizicima poslovne strane, te provjeriti jesu li te mjere i postupci redovito održavani i testirani.

Slika 5: ITIL V3 proces



Izvor: Izrada autora prema https://www.certguidance.com/information-security-management-itil/

4.4. COBIT 5

COBIT 5 jedini je poslovni okvir za upravljanje IT poduzeća. To je proizvod globalne radne skupine i razvojnog tima ISACA-e - neprofitne, neovisne udruge koji broji više od 140.000 profesionalaca u području upravljanja, sigurnosti, rizika i osiguranja u 187 zemalja.[12]

COBIT 5 uključuje najnovija razmišljanja u upravljanju tehnikama poduzeća koja pruža globalno prihvaćena načela, prakse, analitičke alate i modele koji pomažu u povećanju povjerenja u informacijske sustave i njihove vrijednosti.

COBIT 5 se gradi i proširuje na COBIT 4.1 integrirajući ostale glavne okvire, standarde i resurse, uključujući ISACA-in Val IT i Risk IT, informacijske tehnologije (ITIL) i srodne standarde Međunarodne organizacije za standardizaciju (ISO).

Svakodnevno se pojavljuju novi zahtjevi korisnika, specifični propisi i razni rizici. Maksimiziranje vrijednosti intelektualnog vlasništva, upravljanje rizikom i sigurnošću i osiguranje usklađenosti kroz učinkovito upravljanje informatičkim tehnologijama i upravljanje nikada nisu bili važniji.

Niti jedan drugi okvir fokusiran na IT poduzeća ne nudi širinu ili prednosti COBIT-a. Pomaže tvrtkama svih veličina u:

- Održavanju visokokvalitetne informacije za podršku poslovnim odlukama
- Postizanje strateških ciljeva kroz učinkovitu i inovativnu upotrebu IT-a
- Postizanje operativne izvrsnosti pouzdanom i učinkovitom primjenom tehnologije
- Održavanju rizika vezanog za IT na prihvatljivoj razini
- Optimizacija troškova IT usluga i tehnologije
- Podržavanje i poštivanje relevantnih zakona, propisa, ugovornih sporazuma i politika[13]

COBIT 5 je općenit i koristan za poduzeća svih veličina, bilo komercijalnih, neprofitnih ili u javnom sektoru. Koriste ga globalno oni koji imaju primarnu odgovornost za poslovne procese i tehnologiju, ovise o tehnologiji relevantnih i pouzdanih informacija i pružaju kvalitetu, pouzdanost i kontrolu informacija i srodne tehnologije.

[12] „Cobit 2019.“, www.isaca.org/cobit
[13] „Cobit 2019.“, www.isaca.org/cobit

4.5. Usporedba ISO/COBIT/ITIL

Svaki od okvira i standarda sustava može ponuditi različite snage i slabosti. Ako odaberemo samo jedan od njih, propustit ćemo neke dobre strane ovog drugog, a sustavu upravljanja nedostajati će neke važne karakteristike.

Na primjer, primjena ITIL-a pruža puno detaljnih smjernica o provedbi procesa, ali je prilično slaba u pogledu upravljanja i postavljanja ciljeva. S druge strane, COBIT 5 iako je vrlo jak u upravljanju i postavljanju ciljeva ne daje puno detalja o provedbi procesa; a ISO, koji pruža sažetu informaciju o tome što bi IT organizacija trebala raditi, nudi malo smjernica o tome kako zapravo raditi.

U praksi, bilo bi potrebno da se organizacija sagleda kroz nekoliko stajališta, a ne kroz samo jedan. U budućnosti će biti mnogo jednostavnije, tratiti će se manje vremena, a samo poduzeće će biti učinkovitije kada zna u kojem se smjeru želi kretati, odnosno u kojim je područjima potrebno implementirati okvire i standarde.

Kako bi se pobliže shvatila i razumjela razlika između navedenih standarda, razlike su navedene u tablici ispod.

Tablica 1: Usporedba standarda ITIL, COBIT, ISO

	ITIL	COBIT	ISO
ŠTO JE?	Skup izdanja o najboljoj praksi za upravljanje IT uslugama	Poslovni okvir za upravljanje IT poduzećima	Međunarodni standard za zahtjeve sustava upravljanja IT uslugama
KOLIKO JE DUGAČKO?	5 temeljnih izdanja koje se sastoje od 1800 str. kompletnih izdanja	Temeljno izdanje sadrži 94 str + 230 str za omogućavanje procesa	1.dio ima 36 str; ima više nastavaka koji pokrivaju različita područja
KAKO IZGLEDA	ITIL se fokusira na internacionalne IT procese; u	COBIT dolazi iz povijesti revizije i poštivanja pravila;	ISO 27001 prikazuje primjernu upravljanja

NA TRŽIŠTU?	posljednjim izdanjima više se fokusira na vrijednosti i kupce	najnovija verzija prešla je na upravljanje IT sustavima	informacijskom sigurnošću
TKO GA KORISTI?	Sve organizacije koje pružaju IT usluge; najčešće u operativnom IT-u	Za velike IT organizacije; često ga koriste strateški timovi i ljudi odgovorni za reviziju i zakone	IT organizacije koje žele pokazati da ispunjavaju definirani standard
ZA ŠTO SE KORISTI?	Pomaže u definiranju operativnih procesa u pružanju IT usluga	Definiranje zahtjeva za revizijom i usklađivanje za IT	Pokazuje da IT organizacija ispunjava određeni standard

Izvor: Izrada autora

5. KONTROLA RADA INFORMACIJSKOG SUSTAVA

Svaki informacijski sustav obiluje brojnim informacijskim kontrolama, čija je učinkovitost važan čimbenik njegova uspješnoga upravljanja, a samim time i ostvarenja poslovnih ciljeva. Informacijski sustavi vrlo intenzivno koriste brojne digitalne tehnologije i svakako su itekako izloženi različitim *cyber* prijetnjama, pa je funkcioniranje informacijskih kontrola nužan uvjet za uspješnost poslovanja.

Sigurnost informacijskih sustava ostvaruje se osmišljavanjem i provedbom mjera zaštite tzv. informacijskih kontrola, koje se ugrađuju u mehanizme funkcioniranja informacijskih sustava, omogućuje njegovo neometano funkcioniranje i ublažavanje/smanjenje informacijskih rizika.

Informacijske kontrole su kontrole ugrađene u rad informacijsokg sustava koje predstavljaju sustav odnosno skupa međusobno povezanih komponeneti koje, djelujući jedinstveno i usklađeno, zapravo pomažu i omogućuju ostvarivanje ciljeva informacijskoga sustava. Kontrole koje zapravo predstavljaju mjere zaštite se usmjeravaju na neželjene događaje i procese u informacijskom sustavu koji mogu nastati, odnosno biti aktivirani iz raznih razloga koji se odnose na unutarnje djelovanje informacijskog sustava – npr. neovlaštena uporaba, netočni podaci, nedjelotvorni procesi, pogrešni algoritmi, neučinkoviti ulazi u sustav itd; ili uzroke iz njegove okoline – npr. napadi izvana, prirodne nepogode, pogrešan prijenos podataka, pogrešan tip podataka i sl.

Kontrole se primjenjuju kako bi se spriječili, otkrili i/ili ispravili neželjeni događaji i procesi.

Opća svrha informacijskih kontrola je smanjenje vjerojatnosti od samog nastupa nekog neželjenog događaja odnosno smanjenje očekivanog gubitka do kojeg bi došlo prilikom nekog neželjenog događaja.

Informacijske se kontrole dijele:

- Preventivna kontrola – smanjuje vjerojatnost neželjenih događaja
- Detektivna i korektivna kontrola – smanjuje ishod gubitka koji bi nastao zbog djelovanja neželjenih događaja

U svakom se informacijskom sustavu krije niz kontrola koje omogućuju bolje i kvalitetnije upravljanje samim sustavom. Kako su kontrole bolje i kvalitetnije ugrađene i programirane, smanjuje se rizik od različitih prijetnji. Tu se javljaju revizije informacijskih sustava koje provjeravaju o kojoj se informatičkoj kontroli radi te u kojoj je mjeri učinkovita. Revizija informacijskih sustava provodi se prema unaprijed utvrđenim smjernicama upravljanja rizicima, pa se testiraju razine učinkovitosti samih kontrola, potom se prikupljaju argumenti pomoću kojih je moguće procijeniti rizike za samo poslovanje te iz njih izvesti preporuke koje bi dovelo do smanjenje, odnosno do boljeg upravljanja informacijskim sustavom i samim poslovanjem.

Informacijske kontrole razvrstavamo prema sljedećim kriterijima:

I. NAČIN PRIMJENE	II. SVRHA
• automatske kontrole	• preventivne kontrole
• ručne kontrole	• detektivne kontrole
	• korektivne kontrole
III. HIJARARHIJSKA RAZINA	**IV. NAČIN FUKCIONIRANJA**
• korporativne kontrole	• organizacijske kontrole
• upravljačke i procesne kontrole	• tehnološke kontrole
• operativne kontrole	• fizičke kontrole

Za sve navedene vrste moguće je dati primjer te objasniti obilježje funkcioniranja.

I. Prema načinu primjene:

Automatske kontrole predstavljaju zaštitne mehanizme poslovnih procesa, omogućuju njihovo ispravno izvođenje i većinom su ugrađene u automatizam funkcioniranja informacijskih sustava. Npr. korisnik koji ima račun u banci ne može na bankomatu ili šalteru banke podići novac ako na računu nema dovoljan iznos - jer ga odgovarajuća automatska kontrola u tomu sprječava. Automatske kontrole u bankarskom poslovanju konstantno prate navike potrošača (korisnika) i prema unaprijed programiranim kontrolama može se predvidjeti radi li se o sumnjivoj transakciji te zatražiti od korisnika dodatnu provjeru, čime se osigurava sigurni proces kartičnoga poslovanja, odnosno omogućuje korisniku sigurna usluga. U ostalim područjima automatske kontrole javljaju se kod provjere duplih transakcija, za provjeru

ispravnosti prijenosa sadržaja među različitim aplikacijama, provjeru knjiženja i računovodstvenih evidencija, provjere kod funkcioniranja informacijskih sustava i slične kontrole bez kojih ne možemo zamisliti učinkovito funkcioniranje poslovanja.

Ručne kontrole se odnose na ručne provjere funkcioniranja poslovnih procesa. Bazni primjeri mogu biti inventurno stanje, ručno prebrojavanje zaliha, vizualni pregled opreme i slično.

II. Obzirom na svrhu (cilj) djelovanja razlikujemo sljedeće vrste informatičkih kontrola:

Preventivne kontrole (prethodne i procesne) čiji je osnovni zadatak otkriti probleme ili neželjene događaje prije nego što se pojave, predvidjeti ih, prevencijom pokušati spriječiti propuste i, konačno, stalno pratiti aktivnosti informacijskoga sustava, najvažnije operacije, procese, ulaze, izlaze i uočavati anomalije.[14] Npr. zapošljavanje obrazovanih , kvalificiranih zaposlenika, određivanje organizacijskih tijela kojima se nadzire rad informacijskog sustava (upravljački odbor za informatiku), ustrojavanje odjela za unutarnju reviziju informacijskog sustava.

Detektivne kontrole predstavljaju kontrole koje otkrivaju pogrešku, propust ili ugrozu bilo kojega dijela informacijskih sustava, kao primjerice razne opće informatičke kontrole, kontrole unosa podataka, autorizacijske kontrole, fizičke i logičke kontrole pristupa sustavu i podacima, procedure stalnoga nadzora mrežnog prometa i svih događaja u informacijskome sustavu…

Korektivne kontrole koje imaju za cilj minimizirati učinak prijetnje za informacijski sustavu, pri čemu one traže uzrok problema te automatizmom izvršavaju posebne akcije kako bi se uočene pogreške ispravile. Npr. procedura kopiranja i arhiviranja podataka, kontrole prijenosa podataka.

III. Prema načinu funkcioniranja, kontrole su:

Organizacijske se kontrole najčešće javljaju kod internih aktova kojima se propisuju željena ponašanja pri korištenju svih komponenti informacijskog sustava. Internim aktima se određuju pravila za upotrebu informacijskog sustava i pripadajućih uređaja i tehnologije. Tako se na strateškoj razini upravljanja interni akti najčešće odnose na

[14] Prof.dr.sc. Mario Spremić „Digitalna transformacija poslovanja“, Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet, 2017. godine

politike, strategije I metodologije npr. Politika informacijske sigurnosti, Politika ulaganja u informatiku, Strategija informacijskog sustava…

Na jednak način, na operativnoj razini upravljanja postoje procedure i radne upute koje predstavljaju interne akte kojima su detaljno propisani organizacijski, tehnološki I ostali detalji provedbe neke kontrolne mjere, npr. Procedura oporavka podataka, Radne upute za nadzor ključnih uređaja itd.

Fizičke kontrole su kontrole kojima se neovlaštenim osobama sprječava pristup uredima, radnim prostorima, postrojenjima, ali i podacima, važnoj informatičkoj opremi, uređajima ili infrastrukturi. Fizičkim kontrolama se štite svi oni informatički i ostali poslovni resursi koji se mogu vidjeti, dodirnuti ili ukrasti. Fizičke kontrole se najčešće provode: ograničavanjem pristupa do ureda, prostorija i mjesta gdje su pohranjeni važni informatički resursi (uređaji, oprema, infrastruktura, podaci). Ovu kontrolu provode većinom određene čuvarske službe, fizička identifikacija pri ulazu, zaštitna vrata kojima se pristupa unosom šifre ili elektroničkom identifikacijom i slično. Struktura zaštite računalnih mreža sastoji se od fizičke zaštite mrežnih i računalnih resursa, obrazovanja autoriziranih korisnika; pri tome se upotrebljavaju različiti alati koji služe za kriptiranje podataka, autentifikaciju korisnika, detekciju napada, ispitivanje stabilnosti i sigurnosti računalnih sustava i mreža, zaštitu od virusa, zaštitu prijenosa podataka, zaštitna pravila za pravo pristupa podacima i resursima.

Tehnološke kontrole predstavljaju kontrole mrežne infrastrukture, podataka i opreme, alata i algoritama koje su, najčešće u vidu automatskih kontrola, ugrađene u pojedine komponente informacijskog sustava s ciljem nadzora njihova rada.

IV. Obzirom na razine upravljanja razlikujemo sljedeće vrste informatičkih kontrola:

Korporativne (strateške) kontrole - informatičke kontrole na najvišoj razini upravljanja koje čine sastavni dio sustava internih kontrola poslovanja, a odnose se na kontrole provedbe strategije informacijskog sustava, kontrole planova ulaganja u informatiku, ustrojavanje i funkcioniranje ključnih tijela zaduženih za upravljanje informatikom (Odbor za informatiku, engl. IT Steering Committee), kontrole kvalitete informacijskih sustava i aktivnosti sustavnog provođenja interne kontrole i revizije informacijskih sustava..

Upravljačke i procesne (opće) kontrole su kontrole koje se odnose na razvoj i kupnju poslovnih aplikacija, kontrole instalacije aplikacija, kontrole nad podacima koje te aplikacije i pripadajući poslovni procesi koriste, kontrole promjena softvera, kontrole testiranja softvera, kontrole pristupa programima i podacima, sigurnosne kontrole, kontrole kontinuiteta poslovanja (engl. Business continuity), kontrole oporavka nakon prekida rada (engl. Disaster recovery)…

Aplikacijske kontrole i operativne kontrole informatičkih servisa (usluga) se odnose na razne kontrole rada poslovnih aplikacija, kontrole provedbe informatičkih aktivnosti i operacija (jesu li transakcije točne, potpune, cjelovite, podjela dužnosti i kontrola, autorizacija, itd.) i kontrole informatičkih servisa (dostupnost i funkcionalnost mreže, infrastrukture, podataka, opreme, itd.). U ovu kategoriju spadaju i brojne kontrole samog poslovnog softvera, poput kontrole operacijskoga sustava, kontrole instalacije i održavanja softvera, kontrole softvera za prijenos podataka, kontrole isporuke informatičke usluge, kontrole funkcionalnosti aplikacija i informatičkih usluga (to se posebno odnosi na ugovor o razini kvalitete usluge, engl. Service level agreement, SLA), kontrole dostupnosti sustava (mreže, opreme itd.).

6. STANDARD NA PRIMJERU – ITIL u *Walt Disney Company*

U članku pod nazivom „Disneyevo putovanje kroz ITIL“, Glen Taylor, potpredsjednik tehnologije za tematske parkove i odmarališta (Walt Disney Company) opisuje kako je temeljito zagovarao usvajanje ITIL-a u kompaniji za postizanje izvrsnosti u upravljanju IT uslugama. Prema financijskom izvještaju Walt Disney Company za 2016. godinu, Theme Parks and Resorts njihov je drugi najveći generator prihoda – koji je generirao prihod od 16.974,000,000 USD u 2016. Disney je jedna od najpoznatijih tvrtki koja je usvojila ITIL, no pitanje koje se nameće je zašto je uopće Disneyu bio potrebno ITIL?

Cilj Taylora je jasan, a to je pružanje gostima savršeno iskustvo. Za IT, to je značilo 100% dostupnost, pouzdanost i održivost.

Taylor je čvrsto vjerovao da najbolja praksa ITIL-a može pružiti to iskustvo. ITIL pruža sveobuhvatan i dosljedan skup najboljih praksi upravljanja informatičkim uslugama i promovira kvalitetan pristup postizanju poslovne učinkovitosti i efikasnosti u korištenju informacijskih sustava. Usvajanje ITIL-a može korisnicima ponuditi ogroman niz pogodnosti koje uključuju poboljšane IT usluge, smanjene troškove, poboljšano zadovoljstvo korisnika kroz profesionalniji pristup pružanju usluga, poboljšanu produktivnost, poboljšanu uporabu vještina i iskustva i poboljšanu isporuku pomoćnih službi.

Gotovo 45% aplikacija posvećeno je tematskim parkovima i odmarališima. Neke od njih su:

- Mobilna aplikacija Disneyland - ova aplikacija sadrži interaktivnu kartu s omogućenim GPS-om s vremenom čekanja i atraktivnim mjestima; to je presudno za njihovo upravljanje IT uslugama, jer je okrenuto kupcima i mora biti ažurno i precizno
- Ručni uređaji za praćenje inventara na mobilnim kolicima - omogućuje brzu narudžbu kada zalihe smanjene

- Globalni sustav upravljanja kostimom, koji se koristi s radiofrekvencijskom identifikacijom - omogućuje članovima glumaca da s lakoćom pronađu prave kostime i zakažu zamjene

Vjerujući u obećanja ITIL-a, Taylor je predvodio njegovo usvajanje. Ovaj proces promjene i prilagođavanja trajao je dosta vremena, ali sve je to vrijedilo.

Prvo, njegov se tim fokusirao na marketing ITIL-a s izvršne razine i iskorištavanje postojećih projekata kako bi stvorio i podigao svijest o trenutnim problemima s kojima se tvrtka suočava i kako ITIL može riješiti ta pitanja. Potom su pokrenuli obrazovni program od više razine prema dolje, a od 250 ljudi obučenih u ITIL *Foundation*, 50% ih se odlučilo za certificiranje. Konačno su odabrali 20 ljudi iz cijelog TP&R-a kako bi promovirali vrijednost koju ITIL donosi pružajući sjajno iskustvo gosta.

Kao što je već rečeno, proces je bio spor, ali Taylor je bio siguran da će ITIL postići ciljeve tvrtke. Uspio je jednostavnije olakšati prijelaze koji su uključeni u usvajanje ITIL-a. Kroz ovaj postupak Taylor se uspio potaknuti još više ljudi što je kao rezultat imalo još više zagovornika ITIL-a.

Poznato je kako je u svakoj organizaciji pružanje najboljeg iskustva kupcima ključ za osiguravanje podrške i lojalnosti, dok tehnologija igra presudnu ulogu u tome da ovo iskustvo postane vrijedno.

7. ZAKLJUČAK

Poslovni sustav za koji želimo reći da je uspješan trebao bi sadržavati niza informacija potrebnih za poslovanje, a kako bi se pravilno koristile te informacija unutar poslovnog sustava javlja se informacijski sustav.

Kako bi se same informacije pretvorile u podatak koristi se informacijski sustav, koji obrađuju te interpretira informacije na način koji poslovanje zahtjeva.

Zbog uspješnosti poslovanje organizacije počeli su se javljati sigurnosni informacijski sustavi, čiji se broj uvelike povećao od uvođenja modernije i informatički složenije provedbe poslovanja unutar organizacije. Baš zbog povećane uporabe interneta, te većeg dijeljenje podataka, povećava se i potreba za pojačanom zaštitom povjerljivih informacija.

Organizacija može dovesti u opasnost svoju sigurnost i konkurentnost ako ne pridodaje pažnju sigurnosti informacijskih sustava. Ako uzmemo u obzir da sigurnost ubiti nije niti konačni proizvod ili stanje, već proces logično je da i sigurnost informacijskih sustava predstavlja konstantne radnje i cjelokupan proces zaštite. Pa samim time ne može biti dovoljno jednom odabrati odgovarajući informacijski sustav, već ga je potrebno konstantno nadograđivati i pratiti kako bi se održavala optimalna razina rizika koja prijeti sustavu, a samim time i cjelokupnom sustavu u globalu.

U samom sustavu i organizaciji postoji niz dijelova koje je potrebno štititi, međutim informacijska sigurnost brine se za tri osnovna dijela očuvanja povjerljivosti, integriteta te dostupnosti informacija. Kroz ta tri aspekta i pravilnu zaštitu istih moguće je dovesti do napretka poslovanja neke organizacije. Velik je broj raznih procedura, zakona, pravila, metoda i mjera zaštite informacija u Hrvatskoj i upravo zbog te gomile „pravila“ teško je snaći se i pravilno postupati.

Uz institucije i zakone koji djeluju, javljaju se i određene norme za zaštitu informacijske sigurnosti, a najpoznatije su: ISO 27001:2005 – Sustav upravljanja informatičkom sigurnošću, te ISO 27002:2013 – Kodeks postupaka za upravljanje informacijskom sigurnošću. U Hrvatskoj postoji mnogo organizacija koje se bave zaštitom informacijskih sustava prema provedenim anketama niti zaposlenici, niti vlasnici a ni ostali korisnici neke tvrtke nisu dovoljno upoznati sa zakonskom regulativom Republike

Hrvatske koja se tiče sigurnosti informacijskih sustava. Iz toga proizlazi činjenica kako zaposlenici namjerno ili nenamjerno izvršavaju određene zadatke kojima zapravo informacije prosljeđuju na mjesta gdje ne bi trebali te se na taj način ugrožava sigurnost informacijskih sustava.

Svaki informacijski sustav obiluje brojnim informatičkim kontrolama, čija je učinkovitost važan čimbenik njegova uspješnoga upravljanja, a samim time i ostvarenja poslovnih ciljeva. Informacijski sustavi vrlo intenzivno koriste brojne digitalne tehnologije i svakako su itekako izloženi različitim *cyber* prijetnjama, pa je funkcioniranje informatičkih kontrola nužan uvjet za uspješnost poslovanja.

Smatram kako su brojna poduzeća unazad nekoliko godina shvatila da je sigurnost nužna za uspješno poslovanje. Mnogi su se odlučili na investiranje, iako treba izdvojiti pozamašna sredstva, kako bi ostali konkurentni na tržištu te kako bi prvenstveno zaštitili sebe i svoje podatke, a samim time i podatke svojih korisnika.

LITERATURA

Knjige:

1. Bogati, J., „Praktični menadžment“, str. 112-117, Zagreb, 2011. godina
2. Prof.dr.sc. Mario Spremić „Digitalna transformacija poslovanja“, Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet, 2017. godine
3. Prof.dr.sc. Mario Spremić „Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije“, Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet, 2017. godine

Web:

1. „ITIL Information Security Management“; https://www.certguidance.com/information-security-management-itil; 18.02.2018 - Ayan Brahmachary; preuzeto: 10.08.2019.
2. „Izvješće o izvršenju godišnjeg programa rada i poslovanja hrvatskog zavoda za norme“; www.hzn.hr; travanj 2017. Hrvatski zavod za norme; preuzeto: 08.08.2019.
3. „Sigurnost informacijskih sustava“ – B. Vukelić; https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf; preuzeto: 10.08.2019.
4. Cingula M. : "KORPORATIVNA SIGURNOST - Pojam sigurnosti i temeljni srodni pojmovi"; http://web.efzg.hr/dok/MAR/avuletic/01_Pojam%20sigurnosti.pdf; preuzeto: 02.08.2019
5. Klaić A.: „Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodologija a upravljanja informacijsko sigurnošću”, preuzeto: 11.08.2019.
6. Marijanović .: " Upravljanje sigurnošću informacija", Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu; http://sigurnost.zemris.fer.hr/ISMS/2006_marijanovic/Marijanovic_diplomski.pdf
7. www.iso.org; preuzeto: 08.08.2019.
8. Axelos „Disneyevo ITIL putovanje“; preuzeto: 28.08.2019.; https://www.axelos.com/case-studies-and-white-papers/disneys-itil-journey-case-study

POPIS SLIKA

POPIS TABLICA