SISTEM UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU PREMA STANDARDU ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT SYSTEM ACCORDING TO STANDARD ISO/IEC 27001

Džemal Kulašin
Faruk Unkić
Dalila Goran

SAŽETAK

Poslednje manifestacije cyber kriminala u formi ransomware-a gdje je nepovratno enkriptiran ogroman broj računara u gotovo svim zemljama svijeta, dodatno je ukazao na (ne)očekivane slabosti informacijske sigurnosti, čak kada su u pitanju i renomirani poslovni sistemi. Time je dodatno osnažen značaj organizacijskog pristupa informacijskoj sigurnosti, odnosno nužnost uspostavljanja odgovarajućeg sistema upravljanja posvećenog isključivo zaštiti informacija, bilo u digitalnom, bilo u klasičnom obliku.Takav sistem poznat je pod imenom Sistem upravljanja informacijskom sigurnošću, odnosno Information Security Management System (akronim ISMS).
Naravno, za uspostavljanje ovakvog sistema potrebne su odgovarajuće podloge, a najkvalitetnijim se smatraju zahtjevi međunarodnog standarda ISO/IEC 27001. U ovom radu, predstavljaju se osnove Sistema upravljanja informacijskom sigurnošću upravo na podlogama standarda ISO/IEC 27001, gdje je akcenat na implementaciji ISMS-a prema standardu "najbolje prakse" te benefitima koje uspješna implementacija donosi.

Ključne riječi: Informacijska sigurnost, Sistem upravljanja informacijskom sigurnošću ISO/ IEC 27001.

SUMMARY

Recent manifestations of cyber crime as a ransomware, where an immense number of computers all over the world has been encrypted, additionally indicate (un) expected weaknesses of information security even with branding business systems. This intensified the significance of organizational approach to information security and the necessity of establishing adequate system of managing the protection of both digital and typical information. That system is known as Information Security Management System (ISMS).
For establishing this type of system, certain bases are needed, and the best ones are those ISO/IEC 27001international standard requirements. This paperwork is about the basics of Information Security Management System (ISMS) with ISO/IEC 27001 standard bases whereas the focus is on the implementation of ISMS according to "the best practice" standard and benefits that a successful implementation would provide.

Keywords: Information security, Information Security Management System, ISO/IEC 27001

UVOD

Važnost i kompleksnost očuvanja informacijske sigurnosti u okolnostima tehnološki turbulentnog okruženja primorava organizacije na regulatorno ustrojstvo informacijske sigurnosti, gdje se kao rješenje koristi tzv. Sistem upravljanja informacijskom sigurnošću - ISMS (eng. Information Security Management System). Ovaj koncept predstavlja sistemski pristup u upravljanju informacijskom sigurnošću u organizacijama koji uključuje procese, uposlenike, IT sistem i sigurnosnu politiku kojim se osigurava očuvanje ključnih aspekata informacijske sigurnosti poznato kao sigurnosni triangl C-I-A (Confidentiality-Integrity-Availability)[1].

Informacijska sigurnost se, ovakvim pristupom, postiže primjenom odgovarajućih kontrola (tj. sigurnosnih mjera) koje se odnose na politiku sigurnosti, poslovne procese, procedure, strukturu organizacije i funkcije hardvera i softvera. Sve navedene kontrole potrebno je osmisliti, implementirati, nadzirati, preispitivati i unapređivati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahtjeva. Očito, potrebna je odgovarajuća podloga za uspostavljanje sistema upravljanja informacijskom sigurnosti, gdje se najkvalitetnijom smatra međunarodni standard ISO/IEC 27001.

Međunarodni standard ISO/IEC 27001[2]"... specificira zahtjeve za uspostavu, primjenu, održavanje i stalno poboljšavanje sistema za upravljanje sigurnošću informacija u kontekstu organizacije". Što je veoma važno, naglašava se i da su "... postavljeni zahtjevi opći i namjenjeni za primjenu u svim organizacijama, bez obzira na njihov tip, veličinu ili oblik.[3] No, dosadašnja praksa pokazuje da je standard ISO/IEC 27001 najviše zastupljen u sektorima tehnologije, finansija, sektoru poslovnih usluga, vladinim tijelima državnog ili lokalnog nivoa te telekomunikacijama, dok ostali sektori bilježe udio od svega 8% certifikata ovog standarda[4].

STRUKTURA STANDARDA ISO 27001

Standard ISO 27001 karakterizira sveobuhvatnost strukture, gdje razlikujemo: (1) informatički aspekt, gdje se analiziraju i definiraju performanse IT opreme, prava pristupa, kriptovanja, lozinke, protokoli, politike sa aspekta pojave rizika po sigurnost podataka i informacija, (2) administrativni aspekt, gdje se definiraju jasna uputstva, politike i procedure za generiranje informacija, njihovu distribuciju, čuvanje (skladištenje) i (3) fizički aspekt, gdje se utvrđuje fizička kontrola pristupa, evidencija zaposlenih, video nadzor, zaštita radnih prostorija i sl. Dakle, standard ISO 27001 ne pokriva samo sigurnost IT područja, kako se često pogrešno tumači, već pokriva i "... upravljanje fizičkom i tehičkom zaštitom, ljudskim resursima, odnosima sa dobavljačima, partnerima i klijentima, zakonskim i regulatornim obavezama, kontinuitetom poslovanja i sl."[5]

Standard je struktuiran u 11 poglavlja i Aneks A, gdje su prva tri poglavlja uvodna, dok su preostala poglavlja obavezna, odnosno zahtjevi u ovim poglavljima moraju biti implementirani u organizaciji koja uspostavlja ISMS na podlogama ovog standarda. Pri tome, primjetno je da su poglavlja imenovana kao u drugim sistemima upravljanja (npr. ISO 9001:2015) što olakšava njihovu međusobnu integraciju, a što je sukladno Aneksu SL ISO/IEC Direktive Međunarodne Organizacije za Standardizaciju. Poglavlja standarda ISO 27001 su sljedeća[6]:

0: Uvod (Introduction). Objašnjava svrhu ISO 27001 i njegovu kompatibilnost sa

1 Akronim C-I-A je: povjerljivost ili tajnost (Confidentiality), integritet ili cjelovitost (Integrity) i dostupnost ili raspoloživost informacija (Availability)

2 U BiH standard nosi i nacionalni prefiks, te se označava kao: BAS ISO/IEC 27001:2015

3 Institut za standardizaciju BiH, zvanični web sajt: http://www.bas.gov.ba/pages/page_1369.html

4 https://www.itgovernance.co.uk/download/ISO27001-Global-Report-2016.pdf

5 http://www.consalta.ba/en/Sistemi-upravljanja/isms-iso-27001

6 http://www.iso27001security.com/html/27001.html

drugim standardima upravljanja.
1: Opseg (Scope). Specificira opće zahtjeve ISMS-a primjenjive u različitim tipovima organizacija.
2: Upućivanje na norme (Normative references). Upućuje na ISO/IEC 27000 kao standard esencijalan za uspostavljanje ISMS-a. Ostatak ISO27k je opcionalan.
3: Pojmovi i definicije (Terms and definitons). Upućuje na ISO/IEC 27000 gdje su navedeni potrebni pojmovi i definicije.
4: Kontekst organizacije (Context of the organization). Specificira organizacijski kontekst, potrebe i očekivanja "zainteresiranih strana", te definira opseg ISMS-a.
5: Rukovođenje (Leadership). Specificira da najviši menadžment mora demonstrirati liderstvo i posvećenost ISMS-u, definirati sigurnosnu politiku, odrediti uloge i odgovornosti.
6: Planiranje (Planning). Definira uvjete za procjenu rizika, obradu rizika, izjavu o primjenjivosti (SoA), plan obrade rizika uz pojašnjavanje ciljeva informacijske sigurnosti.
7: Podrška (Support). Definira uvjete za dostupnost resursa, nadležnosti, informisanost, komunikaciju i kontrolu dokumenata i zapisa.
8: Djelovanje (Operation). Definira modele za spovođenje procjene i obrade rizika, kao i sigurnosne mjere i druge procese potrebne za postizanje sigurnosti podataka.
9: Ocjena učinaka (Performance evaluation). Definira uvjete za praćenje, mjerenje, analizu, procjenu, unutrašnju reviziju i pregled menadžmenta.
10: Poboljšanja (Improvement). Definira uvjete za usklađenost, ispravke, korektivne mjere i trajna poboljšanja ISMS-a.

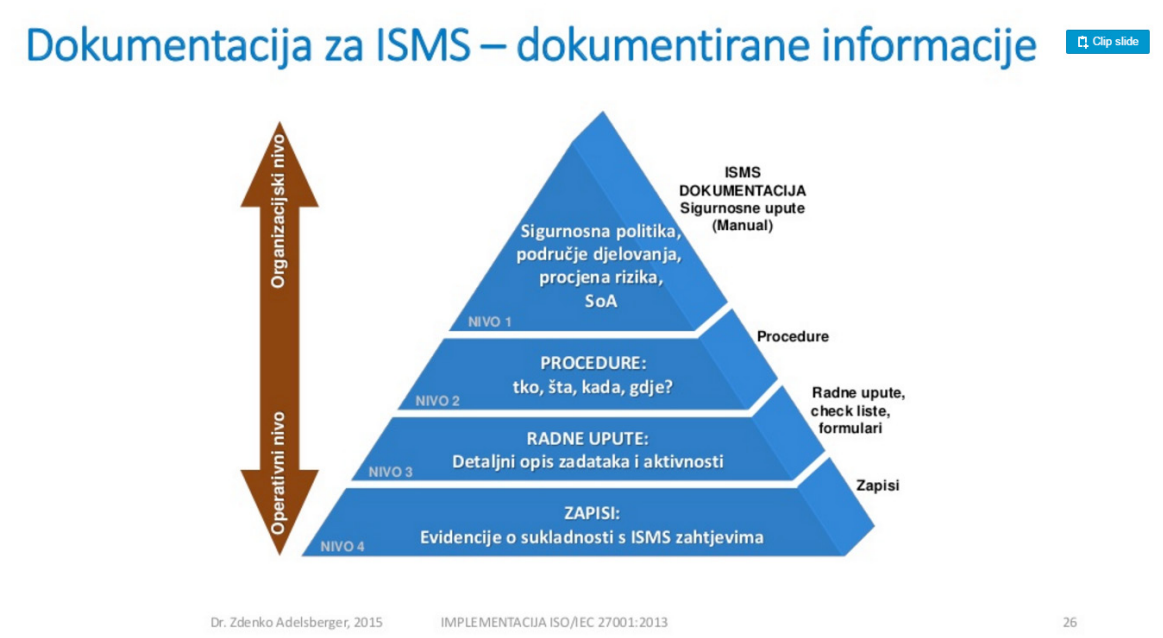
No, zanimljivo je da krucijalni dio standarda ISO 27001 predstavlja, u stvari, Aneks A, jer sadrži široki set sigurnosnih kontrola koje je potrebno primjeniti kako bi se informacije zaštitile [6].

Sigurnosne kontrole Aneksa A (tačnije, 114 kontrola) raspoređene su u 14 sekcija, kako slijedi[7]:
A.5. Politike informacijske sigurnosti (Information security policies) - 2 kontrole
A.6. Organizacija informacijske sigurnosti (Organization of information security) - 7 kontrola
A.7. Sigurnost ljudskih resursa (Human resource security) - 6 kontrola
A.8. Upravljanje imovinom (Asset management) - 10 kontrola
A.9. Kontrola pristupa (Access control) -14 kontrola
A.10. Kriptografija (Cryptography) - 2 kontrole
A.11. Fizička sigurnost i sigurnost okoline (Physical and environmental security) - 15 kontrola
A.12. Operativna sigurnost (Operations security) - 14 kontrola
A.13. Sigurnost komunikacija (Communications security) - 7 kontrola
A.14. Nabavka sistema, razvoj i održavanje (System acquisition, development and maintenance) - 13 kontrola
A.15. Odnosi sa dobavljačima (Supplier relationships) - 5 kontrola
A.16. Upravljanje incidentima informacijske sigurnosti (Information security incident management) - 7 kontrola
A.17. Aspekti informacijske sigurnosti kontinuiteta poslovanja (Information security aspects of business continuity management) - 4 kontrole
A.18. Usaglašenost (Compliance) - 8 kontrola

Kako se može vidjeti, pojedine sekcije Aneksa A imaju različit broj sigurnosnih kontrola, i prema njihovom broju vidimo i „težinu" pojedine sigurnosne sekcije zastupljene u ISMS-u prema ISO 27001. Naravno, u svakoj organizaciji se ne moraju provoditi sve sigurnosne mjere predviđene ovim Aneksom, jer njihov izbor zavisi od rezultata procjene rizika, kao jednog od koraka u uspostavi ISMS-a.

7 https://advisera.com/27001academy/what-is-iso-27001/

Svakako, u okviru strukture ISMS-a prema standardu ISO 27001 posebno treba istaknuti njegovu dokumentiranost, koja je izraženija u odnosu na druge sisteme upravljanja. Globalno gledano, ISMS prema standardu ISO 27001 sastoji se od niza dokumenata, gdje je na vrhu Poslovnik politike sigurnosti (Sigurnosna politika), Procedure, Instrukcije, odnosno Radne upute i Zapisi (Slika 1).



Slika 1: Nivo dokumentacije ISMS-a prema standardu ISO 27001 [2]

IMPLEMENTACIJA ISMS-A PREMA ISO 27001

Standard ISO 27001 je fokusiran na zaštitu tajnosti, integriteta i raspoloživosti podataka u organizaciji (C-IA). To se postiže prepoznavanjem potencijalnih problema koji se mogu dogoditi podacima, tj. procjena rizika, te definiranje što treba poduzeti da se takvi problemi spriječe, tj. obrada rizika. Dakle, temeljna filozofija ISMS-a koji se implementira prema ISO 27001 zasniva se na upravljanju rizicima. Na osnovu procjena rizika, a shodno cilju implementacije sistema ISO 27001, osiguravaju se neophodne kontrole u cilju zaštite informacija i podataka "zainteresovanih strana"; zainteresovane strane kojima je ovaj sistem menadžmenta upućen mogu biti klijenti, organizacije i kompanije, zaposleni, saradnici, ali i društvo u širem smislu. Drugim riječima, okvir (eng. framework) ISO 27001 čine procjena i obrada rizika (eng. Risk assessment and treatment) te implementiranje sigurnosnih mjera (eng. Safeguard implementation).

Kako je implementacija ISMS-a prema standardu ISO 27001 složen, dugoročan i kontinuirani proces, mora se provoditi u koracima, prema određenom redoslijedu. Ključni koraci implementacije ISMS-a prema standardu ISO 27001 mogu biti sljedeći [3]:

1. Odluka uprave o uspostavi ISMS-a
2. Snimak stanja informacijske sigurnosti,
3. Imenovanje tima za uspotavu ISMS-a
4. Edukacija tima,
5. Opseg i granice uvođenja sistema,
6. Politika informacijske sigurnosti,
7. Popis imovine i vrednovanje,
8. Procjena rizika
9. Upravljanje rizikom i implementacija planiranih kontrola
10. Izrada dokumentacije
11. Edukacija djelatnika i podizanje svijesti o informacijskoj (ne)sigurnosti.

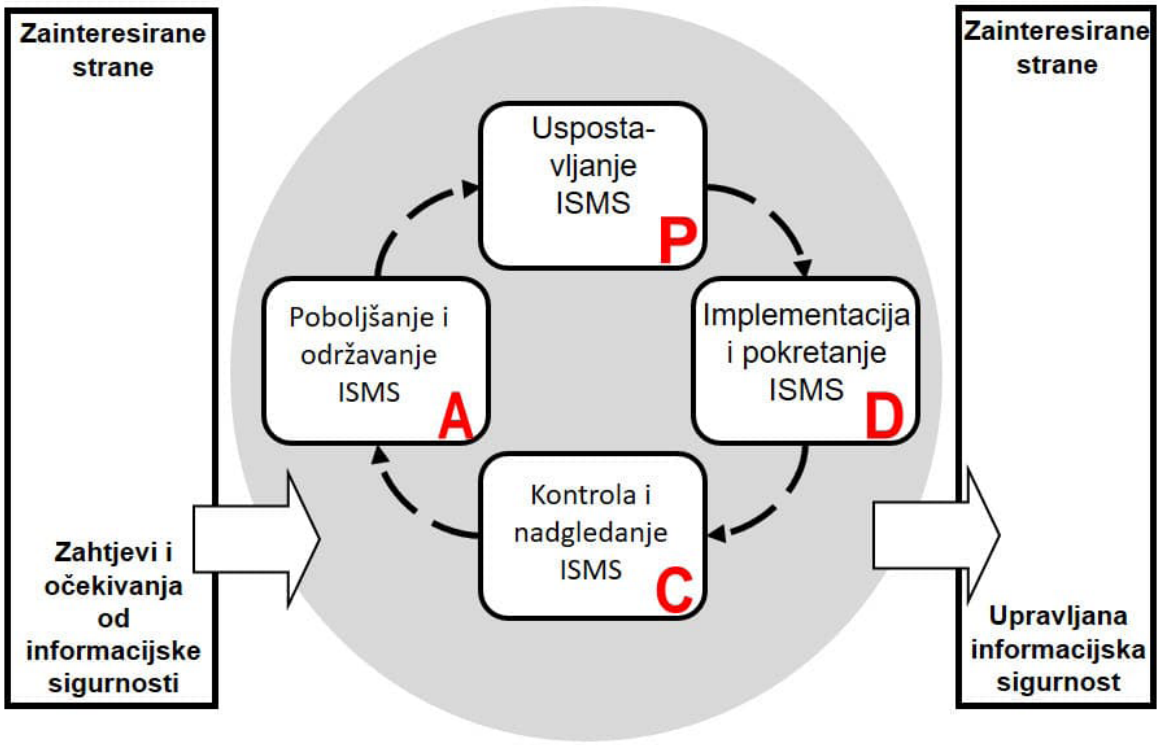
Stvarna implementacija ISMS-a u neku organizaciju je, u biti, provođenje sigurnosnih kontrola odabranih shodno procjeni rizika koja se provodi na temelju sigurnosne

politike organizacije. Inače, dokument u kojem se to navodi i službeno potpisuje označava se kao Izjava o primjenjivosti (eng. SoA - Statement od Applicability), kako je striktno navedeno u zahtjevu standarda ISO 27001. Tako, ako je procjena rizika kvalitetna, te se i provede što je planirano, može se očekivati i kvalitetno uspostavljeni ISMS u kojem se postiže planirani nivo C-I-A. S druge strane, ako je procjena rizika loše ili djelimično napravljena (recimo, samo na dijelu imovine informacionog sistema), sigurno je da kako god kvalitetno se provedu planirane sigurnosne mjere, uspostavljeni ISMS nije dobar.

IMPLEMENTACIJA ISMS-A PREMA ISO 27001

Kvalitetan i uspješan ISMS prema standardu ISO/IEC 27001 karakteriziran je i tzv. PDCA ciklusom (Plan-Do-Check-Action) koji se, inače, sreće u svim sistemima upravljanja temeljenim na seriji ISO standarda kao svojevrsnom motoru stalnog poboljšavanja. Za ISMS koji pokriva područje informacijsko-komunikacijske tehnologije (IKT), ovakav pristup je prijeko potreban zbog brzine tehnoloških promjena i čestih sigurnosnih incidenata iniciranih kako iznutra, tako i izvan sistema. Bliže značenje pojedinih faza PDCA ciklusa u ovom kontekstu je sljedeće:

- Planiranje (Plan): Politika sistema menadžmenta za sigurnost informacija, zajedno sa ciljevima sistema menadžmenta za sigurnost informacija i definiranim mjerama na unapređenju sistema u pogledu poboljšanja sigurnosti informacija čine "Plan - Planiraj" dio sistema menadžmenta za sigurnost informacija prema zahtjevima standarda ISO 27001. Na osnovu iskazanih zahtjeva korisnika i kroz uspostavljanje politike ISMS organizacija, ulazi u fazu uspostavljanja odnosno planiranja sistema za upravljanje sigurnošću informacija (ISO 27001). U ovoj fazi se provode i aktivnosti na definisanju kriterijuma za ocjenu rizika, definiše se prilaz i metodologija za ocjenu rizika, definišu se nivoi prihvatljivosti rizika i dr.
- Provođenje (Do): Sprovođenje planiranog su akcije na primjeni prethodno odabranih upravljačkih mehanizama i ciljeva, izrada, uvođenje i primjena plana snižavanja rizika, obuka za ostvarivanje svijesti o primjeni ISMS, upravljanje resursima ISMS i dr. Struktura i odgovornosti, obuka, kompetentnost i svijest, dokumentacija i kontrola dokumenata, kontrola nad operacijama i spremnost na reagovanje u vanrednim situacijama i odgovor na njih čine "Do - Izvedi" dio sistema menadžmenta za sigurnost informacija prema zahtjevima standarda ISO 27001.
- Provjeravanje (Check): Ova faza je preispitivanje ISMS-a na osnovu definiranih procedura za preispitivanje, mjerenje efektivnosti upravljačkih mehanizama, sprovođenja internih provjera, ažuriranje planova za snižavanje rizika i dr. Dio "Check - Provjeri" sistema menadžmenta za sigurnost informacija prema zahtjevima standarda ISO 27001 se sastoji od praćenja i mjerenja, vrednovanja usaglašenosti, korektivnih i preventivnih akcija, upravljanja zapisima i internih provjera sistema.
- Poboljšanje (Action): Ovaj dio sistema menadžmenta za sigurnost informacija prema zahtjevima standarda ISO 27001 se ostvaruje kroz preispitivanje od strane rukovodstva koje zaokružuje cijeli ciklus performansi sistema menadžmenta i vraća ga na planiranje (Plan) koje treba da rezultira kontinuiranim poboljšanjem. Kao završna faza u ovom kontinuiranom ciklusu poboljšavanja egzistira faza održavanja i poboljšavanja ISMS-a koja se sprovodi kroz uvođenje poboljšanja, preuzimanje korektivnih i preventivnih mjera, provjeravanje da li su provedena poboljšanja održiva i sl.



Slika 2: PDCA kao pokretač stalnog poboljšanja ISMS-a

PDCA ciklus može se uočiti i u pojedinim poglavljima (tj. zahtjevima) standarda ISO 27001[8]:

- Poglavlja 4. Kontekst organizacije 5. Rukovođenje i 6. Planiranje dio su PDCA faze Planiranje (Plan),
- Poglavlje 8. Djelovanje dio je PDCA faze Provođenje (Do),
- Poglavlje 9. Ocjena učinaka dio je PDCA faze Provjeravanje (Check) te
- Poglavlje 10. Poboljšanja dio je PDCA faze Poboljšanje (Act).

BENEFITI ISMS-A PREMA STANDARDU ISO 27001

Serija standarda ISO/IEC 27000 daje harmonizirani pristup upravljanju rizicima kojim su izložene informacione vrijednosti u organizaciji kroz razvoj, implementaciju i održavanje ISMS-a kao menadžment sistema informacijske sigurnosti. Njegovim krajnjim certificiranjem organizacije stiču kako interne tako i eksterne prednosti, kao što su:

1. stvaranje povjerenja u informacioni sistem organizacije,
2. komplementarnost sa pravnom regulativom koja je vezana za informacione tokove jer se radi o standardu koji ima jasnu fleksibilnost,
3. usmjerenost na jasna kontinuirana poboljšavanja procesa kojima se obezbjeđuje informaciona sigurnost, povećanje preventivnog djelovanja kroz smanjenje "uskih grla" u mreži,
4. smanjenje incidenata i bolje razumijevanje uzroka,
5. općenito razvijanje svijesti zaposlenih u smislu značaja zaštite informacija[9], itd.

Efekti implementiranja ISMS-a česta su tema različitih istraživanja u svijetu, gdje svi pokazatelji afirmativno govore o benefitima uspostavljenog sistema upravljanja informacijskom sigurnošću. Jedno od tih

8 Košutić, D, 2014, Has the PDCA Cycle been removed from the new ISO standards, Advisera, dostupno na: https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/

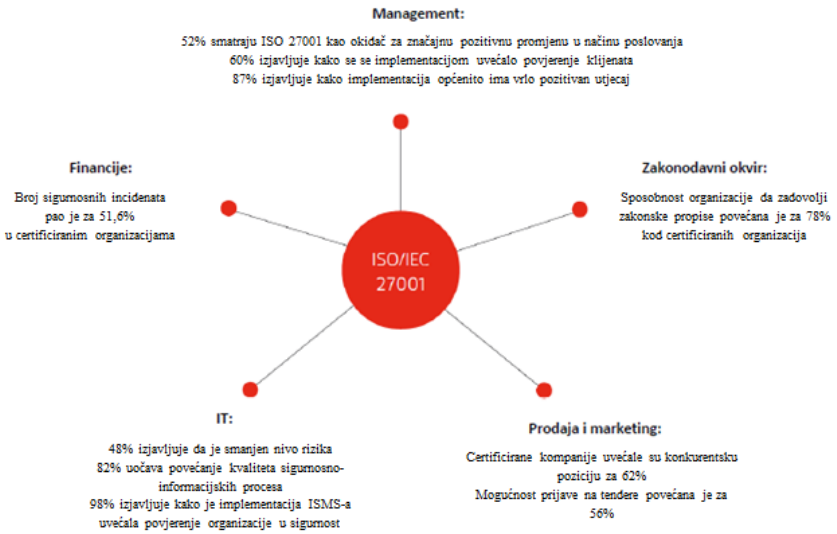
9 https://chapters.theiia.org/ bermuda/ Events/ Chapter Documents/ Information %20Security%20 Management%20System%20%28ISMS%29%20Overview.pdf

istraživanja predstavlja benefite podijeljene prema pojedinim sektorima organizacije, poput menadžmenta, finansija, prodaje i marketinga i IT sektora (Slika 3) [2].

No, sudeći po zvaničnim podacima međunarodne organizacije za standardizaciju (ISO) koja jedanput godišnje objavljuje pregled ISO certifikata, u našoj zemlji (ni) u ovom pogledu ne postoji potreban nivo korporativne svijesti. Naime, prema posljednjem ISO Survey-u[10], zaključno sa decembrom 2015. godine u Bosni i Hercegovini izdano je svega 13 certifikata za uspostavljeni ISMS-a prema standardu ISO 27001[11]. Za usporedbu, vrijedi navesti podatke istog izvora da je u susjednim zemljama izdano daleko više certifikata: u Sloveniji 58 certifikata, u Hrvatskoj 96, dok je u Srbiji izdato čak 103 certifikata.

ZAKLJUČAK

Organizacijsko uspostavljanje sistema upravljanja posvećenog isključivo zaštiti informacija, tj. sistem upravljanja informacijskom sigurnošću (ISMS), sve više dobija na značaju jer se u cijelom svijetu svakodnevno manifestiraju sve teži i raznovrsniji oblici cyber kriminala. Dramatični finansijski gubici, koji se na godišnjem svjetskom nivou izražavaju u stotinama milijardi dolara (!?) često su uvjetovani (unutarnjim) ljudskim faktorom, neprovođenjem redovnih sigurnosnih kopija (eng. backup), neažurnošću u provođenju update-a hardvera i softvera, i sl. Uspješnim implementiranjem sistema upravljanja informacijskom sigurnošću (ISMS) na podlogama standarda ISO/IEC 27001, sigurnosni rizici se svode na projektovani prihvatljivi nivo, jer se harmonizira složeni organizacijski sistem zaštite tajnosti, integriteta i raspoloživosti podataka (C-I-A). Prema iskustvima brojnih svjetskih kompanija, krajnjim certificiranjem ISMS-a prema ISO/IEC 27001 stječu se brojne prednosti, kako interne, tako i eksterne, što u konačnici ne samo da maximalizira nivo sigurnosne zaštite, već poboljšava i ukupnu organizacijsku učinkovitost. No, projekat implementacije ISMS-a je složen i zahtjevan projekat, koji ishodište ima u jasnom i čvrstom opredjeljenju top menadžmenta a potom na stalnim intelektualnim i infrastrukturnim naporima poboljšavanja postojećeg sistema.



Slika 3: Efekti implementiranja ISMS-a prema ISO 27001 [2]

10 http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

11 BAS ISO/IEC 27001 stekli su: Centralna banka Bosne i Hercegovine, Lutrija Bosne i Hercegovine, BH Telekom, Institut za privredni inžinjering Zenica, itd.

LITERATURA

[1] [1] ACCVIS ISO 27001, 2015, Sistem menadžmenta zaštite i bezbednosti informacija, dostupno na: http://accvis.com/iso-27001-2015-iec/

[2] Adelsberger, Z. 2015, Implementacija ISMS prema ISO /IEC 27001/2013, ICT Security Kladovo, 14.-16.maj 2015, dostupno na: http://www.slideshare.net/dejanjeremich/adelsberger-zdenko-implementacija-iso27001-2013

[3] Hofer, D., 2014, Implementacija sustava upravljanja informacijskom sigurnošću prema ISO 27001:2013 - Koraci i prednosti, STEP Osiguranje kvalitet Zagreb, dostupno na: https://issuu.com/kvaliteta.net/docs/hdk_14_konferencija_2014.157-163

[4] Košutić, D, 2014, Has the PDCA Cycle been removed from the new ISO standards, Advisera, dostupno na: https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/

[5] IT Governance, 2016, ISO 27001 Global report - 2016, dostupno na: https://www.itgovernance.co.uk /download/ISO27001-Global-Report-2016.pdf

[6] Raković, R., 2013, Sistem bezbednosti informacija - iskustva i preporuke information security system - experiences and recommendations, dostupno na http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/071.pdf /

[7] Terroza, S.K.A, 2015, Information Security Management System - Overview, The institute of internal auditor, dostupno na: https://chapters.theiia.org/ bermuda/Events/Chapter Documents/ Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf

[8] https://www.kvalis.com/implementacija-isms-prema-isoiec-270012013/

[9] https://advisera.com/27001academy/what-is-iso-27001

[10] https://www.iso.org/the-iso-survey.html

[11] http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

[12] http://www.iso27001security.com/html/27001.html

[13] http://www.consalta.ba/en/Sistemi-upravljanja/isms-iso-27001