Primena standarda ISO/IEC 27001 kao faktora konkurentske prednosti organizacija

Momčilo Kokić
Katedra za industrijski menadžment i informatiku
Fakultet za menadžment
Sremski Kralovci, Srbija
momcilo.kokic@famns.edu.rs

Petar Tasevski
Fakultet za menadžment
Sremski Kralovci, Srbija
petar.tasevski@gmail.com

Sadržaj— **Osnovna premisa standarda ISO/IEC 27001 kaže da je informacija imovina koja kao i svaka druga imovina ima svoju vrednost. Ta vrednost može biti iskazana u finansijskim iznosima ali i kroz vrednost ciljeva koji se žele postići. Zbog toga napadači nastoje naneti štetu narušavanjem bezbednosti informacija koja se manifestuje obično kroz neovlašćenu izmenu i manipulaciju informaciom. Po mnogim istraživanjima u svetu, a i kod nas praksa na žalost, to svakodnevno potvrđuje. Nebezbedno upravljanje informacijama može dovesti do gubitka poslovanja, poslovne reputacije i takođe dovesti egzistenciju organizacije u opasno stanje. Iz tog razloga su mnoge organizacije usvojile standard ISO/IEC 27001, da im pomogne da bezbedno upravljaju svojim informacijama. Sertifikat ISO/IEC 27001 pokazuje postojećim poslovnim partnerima a i klijentima da je organizacija aktivirala efikasne mere zaštite informacionih resursa. Ovo organizacijama obezbeđuje bolju tržišnu poziciju, odnosno organizacije čini konkurentnijim pri istim ostalim tržišnim uslovima.**

Ključne reči:1; ISO 27001, 2;Upravljanje bezbednošću informacija, 3;Implementacija ISMS-a,

I. UVOD

Bezbednost informacija se postiže primenom odgovarajućih aktivnosti koje se odnose na politiku bezbednosti, poslovne procese, procedure, strukturu organizacije, definisanje odgovarajućeg hardvera i softvera. Aktivnosti važne za organizaciju sa zakonske tačke gledišta su vezane za zaštitu informacija i tajnost ličnih podataka, čuvanje izveštaja i poštovanje prava intelektualnog vlasništva.

Efektivna implemetnacija ISMS-a podrazumeva da je menadžment tim posvećen procesima koji informacije čine bezbednim i da su na raspolaganju odgovarajući resurs koji će da podrže procese koji su potrebni organizaciji da postigne odgovarajući nivo bezbednost informacija. Ovo neminovno podrazumeva procese koji se odnose na upravljanje sistemom, procese obuke i podizanja svesti korisnika sistema. Naglasak je na procesu upravljanja rizikom koji determiniše izbor zaštitnih mera i kontrola koje ako su korektno implementirane, obezbeđuju da sistem evoluira ka sistemu upravljanja promenama u poslovanju u bezbednom okruženju.

Mišljenja mnogih internih revizora i konsultanata o samoj primeni standarda su veoma pozitivna. Oni imaju kratko ali razumljivo rešenje implementacije ISMS-a. Politika ISMS-a zajedno sa ciljevima ISMS-a i definisanim merama na unapređenju sistema u pogledu poboljšanja bezbednosti informacija predstavlja prvi korak sistema za upravljanje bezbednošću informacija prema zahtevima standarda. Na osnovu iskazanih zahteva korisnika i kroz uspostavljanje politike ISMS-a organizacije, započinje faza uspostavljanja, odnosno planiranja sistema za upravljanje bezbednošću informacija. U ovoj fazi se sprovode aktivnosti na definisanju kriterijuma za ocenu rizika, definišu se prilaz i metodologija za ocenu rizika, definišu se nivoi prihvatljivosti rizika i dr. Sledeća faza je sprovođenje planiranog, odnosno akcije na primeni prethodno odabranih upravljačkih mehanizama i ciljeva, izrada, uvođenje i primena plana snižavanja rizika, upotreba kontrola, obuka za podizanje svesti, upravljanje resursima ISMS-a i dr. Treća faza je preispitivanje ISMS-a na osnovu definisanih procedura za preispitivanje, merenje efektivnosti upravljačkih mehanizama, sprovođenja internih provera, ažuriranje planova za snižavanje rizika i dr. Četvrta faza se ostvaruje kroz preispitivanje od strane rukovodstva, koje zaokružuje ceo ciklus sistema upravljanja i vraća ga na planiranje koje treba da rezultuje kontinuiranim poboljšanjem koje se sprovodi kroz definisanje i preduzimanje korektivnih i preventivnih mera na osnovu internih i eksternih provera uspostavljenog sistema.

ISO/IEC 27001 je značajan standard za organizacije koje se bave uslugama u oblastima koje su na bilo koji način povezane sa informacionim tehnologijama i potrebom za očuvanje tajnosti informacija. Njegova implementacija i primena omogućavaju bolju saradnju sa sličnim organizacijama širom sveta koje posluju po ovom modelu. Primenom Standardom ISO/IEC 27001 organizacije demonstriraju svojim korisnicima i ostalim zainteresovanim stranama da poslovne procese realizuju na bazi principa sigurnosti i da je poslovna politika usmerena na stalna poboljšavanja sistema upravljanja bezbednošću informacija i procesima povezanim sa njima.

II. STANDARD ISO/IEC 27001

ISO/IEC 27001, formalno nazvan “Informacione tehnologije – Bezbedonosne tehnike – Sistemi za upravljanje bezbednošću

informacija – Zahtevi" (Information Technology – Security Techniques – Information Security Management Systems – Require-ments), objavljen je oktobra 2005. godine. On je zamenio prethodni BS7799-2 standard. Standard navodi specifične zahteve koji su ključni u uspostavljanju, implementaciji, nadzoru, preispitivanju, održavanju i unapređenju sistema upravljanja. Nije usmeren ka specifičnim zahtevima bezbednosti informacija u pojedinim tipovima organizacijama, već je opšteg karaktera, te je primenljiv na različite tipove i veličine organizacija i institucija.

ISO/IEC 27001 navodi tri aspekta bezbednosti informacija:

- Organizacioni – politika bezbednosti, organizacija bezbednosti informacija, upravljanje sredstvima, bezbednost ljudskih resursa, operativne procedure i odgovornosti, upravljanje pružanjem usluga, upravljanje incidentima, upravljanje kontinuitetom poslovanja.
- Tehnički – fizička kontrola pristupa, evidencija zaposlenih, video nadzor, zaštita radnih prostorija.
- Informacioni – analizira i definiše performanse IT opreme, prava pristupa, kriptovanja, lozinke, protokole, politike sa aspekta pojave rizika po bezbednost podataka i informacija, usluge elektronske trgovine, rukovanje medijima, upravljanje bezbednošću mreža, razvoj i održavanje.

Utvrđujući zahteve sva tri aspekta, ISO/IEC 27001 definiše okvir za kreiranje ISMS-a, koncipiranog da pruži potpunu zaštitu informacija.

ISO/IEC 27001 daje mogućnost izbora odgovarajućih sistema upravljanja zaštitom i stvaranje poverenja kod svih zainteresovanih strana. Naime, kako je primenljiv za različite tipove i veličine organizacija i institucija, pogodan je za nekoliko različitih tipova primene, uključujući sledeće [1]:

- pri formulisanju sigurnosnih zahteva i ciljeva,
- kao osiguranje da je upravljanje sigurnosnim rizicima efikasno,
- da bi se osiguralo poštovanje zakona i ostalih regulacionih propisa,
- kao okvir procesa za implementaciju i rukovođenje kontrolom, kako bi pojedinačni sigurnosni ciljevi u toj organizaciji bili ispunjeni,
- pri definisanju novih procesa u rukovođenju bezbednošću,
- kada je potrebna identifikacija i razjašnjenje postojećih procesa upravljanja bezbednošću informacija,
- koristi ga rukovodstvo organizacija kako bi se odredio status aktivnosti koje se odnose na upravljanje bezbednošću informacija,
- pri oceni od strane internih i eksternih revizora organizacije kako bi se odredio stepen poštovanja politika, direktiva i standarda koje je organizacija prihvatila,
- koa dokaz poslovnim partnerima i drugim organizacijama sa kojima se sarađuje – ili iz komercijalnih razloga ili da bi se obezbedile relevantne informacije o pravilima bezbednosti informacija, direktivama, standardima i procedurama, itd.

III. KORACI IMPLEMENTACIJE ISMS-A U ORGANIZACIJAMA

Standard ISO/IEC 27001 je pripremljen da bi obezbedio model za uspostavljanje, implementaciju, održavanje i stalno poboljšanje sistema upravljanja bezbednošću informacija (ISMS). Sistematskim pristupom i uspostavljanjem sistema upravljanja bezbednošću informacija u skladu sa standardom ISO/IEC 27001 ostvaruje se poverenje u sigurnost i pouzdanost potrebnih informacija. Pouzdanost i poverenje u sam sistem upravljanja bezbednošću informacija, s druge strane, ptvrđuje sertifikacijom u odnosu na taj sistem. Tokom sertifikacije, kao postupka ocenjivanja usaglašenosti, različitim aktivnostima se potvrđuje ispunjenost zahteva koji se odnose na ISMS i koji su navedeni u ISO/IEC 27001[3].

ISMS je važan, kako za javni tako i za privatni poslovni sektor. U bilo kojoj grani industrije, ISMS omogućava i podržava poslovanje i od suštinskog je značaja za aktivnosti upravljanja rizikom. Međusobno povezivanje javnih i privatnih mreža i deljenje informacija i informacionih sredstava otežava kontrole pristupa i rukovanja informacijama. Pored toga, sve veća distribucija mobilnih uređaja umanjuje efikasnost tradicionalnih kontrola. Kad organizacije usvoje ISMS, sposobnost primene doslednih i uzajamno – prepoznatljivih principa bezbednosti informacija, može se pokazati poslovnim partnerima i drugim zainteresovanim stranama [3].

Pre implementacije ISMS-a, najvažnije je da rukovodstvo u potpunosti razume prednosti uvođenja sistema upravljanja bezbednošću informacija i da podržava njegovo uvođenje, a da pri tome bude svesno mogućih problema i prepreka koje se mogu pojaviti. Kako bi se uspešno ispunili ciljevi i zahtevi bezbednosti informacija, važno je da rukovodstvo organizacije preuzme inicijativu i pruži punu podršku delu organizacije koji će sprovoditi procese. Predloženi koraci za implementacione faze su prikazani u tabeli 1.

Menadžment mora da preuzme odgovornost za uspostavljanje, planiranje, rad, nadzor, pregled, održavanje i implementaciju ISMS-a. Posvećenost menadžmenta mora obuhvatiti aktivnosti kao što su: obezbeđivanje raspoloživosti odgovarajućih resursa za rad na ISMS-u i da svi zaposleni pod uticajem ISMS-a imaju odgovarajuću obuku, razvoj svesti i kompetentnosti.

TABELA 1: MAPIRANJE ISO/IEC 27001

Koraci i faze implemenatacije ISMS-a u organizacijama	
ISO/IEC 27001 Predloženi koraci	***Implementcione faze***
Definisanje ISMS politike Definisanje obima ISMS-a	Faza 1 – Identifikovanje poslovnih ciljeva Faza 2 – Dobijanje podrške menadžmenta Faza 3 – Izabrati odgovarajući obim implementacije
Izvršiti procenu bezbedonosnog rizika Upravljanje identifikovanim rizikom Odabir kontrole koje će biti primenjene i implementirane Priprema SOA dokumenta	Faza 4 – Definisati metod procene rizika Faza 5 – Popis informacionih sredstava prema klasifikaciji rizika baziranom na osnovu procene rizika Faza 6 – Upravljati rizikom i napraviti plan tretmana rizika Faza 7 – Podesiti politike i procedure za kontrolu rizika Faza 8 – Alocirati sredstva i obučiti osoblje
Preispitivanje menadžmetna i interna revizija Registracija i sertifikacija	Faza 9 – Praćenje implementacije ISMS-a Faza 10 – Priprema za sertifikaciju
Unapređenje ISMS-a	Faza 11 – Sprovođenje periodične revizije ponovne procene i kontinuirano unapređenje

Usvajanje ISMS-a je strateška odluka za organizaciju i neophodno je da ta odluka bude u skladu sa potrebama organizacije. Dizajn i implementacija ISMS-a organizacije zavisi od potreba i ciljeva organizacije, bezbednosnih zahteva, poslovnih procesa, veličine i strukture organizacije. ISMS takođe naglašava važnost razumevanja zahteva organizacije i potrebe da uspostavi politike i ciljeve bezbednosti informacija, implementaciju kontrola radi upravljanja rizicima bezbednosti informacija, nadziranja, evidentiranja incidenata i preispitivanja performansi i efikasnosti ISMS-a, a sve u cilju stalnog poboljšanja poslovanja.

IV. POLITIKA BEZBEDNOSTI INFORMACIJA

Politika bezbednosti informacija organizacije ili institucije prilagođava se potrebama i poslovnim procesima, pa samim tim nije jednaka za sve organizacije. Politikom se ne određuje na koji način zaštititi informacioni sistem već samo šta zaštititi. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sistem. Upravo zbog toga, jednom ustanovljena politika se mora redovno analizirati, menjati i ažurirati kada god se za to ukaže potreba[4].

Bezbednosnom politikom definisana su pravila koja se odnose na:

- svu informatičku opremu organizacije (hardver i softver),
- osobe odgovorne za administraciju informacionog sistema,
- sve zaposlene i korisnike sistema, odnosno osobe koje imaju pravo pristupa,
- spoljne saradnike.

Osnovni zahtevi za bezbednost informacija trebaju biti definisani i navedeni u obliku bezbednosne politike od strane menadžmenta. Bezbednost informacija definisana od strane ISO/IEC 27001 standarda, kao očuvanje tajnosti, integriteta i raspoloživosti informacija su ključni parametri na bazi kojih svaka politika bezbednosti mora biti izgrađena.

Sadržaj bezbedonosne politike zaštite informacionog sistema (ISMS politika), pored uloge i odgovornosti za bezbednost u organizaciji obuhvata i sledeće:

- fizičku zaštitu sistema (zaštita objekata, računarske opreme, sobe sa serverima);
- autentifikaciju (zahteve za udaljeni pristup, mrežni pristup, Internet vezu i dr.);
- autorizaciju i kontrolu pristupa (model po kojem se vrši autorizacija i kontrola pristupa);
- zaštitu tajnosti (koji objekti informacija na računaru, serveru ili mreži zahtevaju zaštitu tajnosti);
- zaštitu integriteta (koji objekti informacija na računaru, serveru ili mreži zahtevaju zaštitu integriteta);
- zaštitu raspoloživosti (koji objekti informacija na računaru, serveru ili mreži zahtevaju zaštitu raspoloživosti)
- upravljanje incidentom (kako detektovati napad, upravljati incidentima i odgovoriti na incidente)

Razvoj i pravilna implementacija bezbedonosne politike je veoma korisna, jer u naporima organizacije da obezbedi svoje komunikacije, ne samo da će pretvoriti zaposlene u učesnike, već će pomoći da se smanji rizik od potencijalnog narušavanja bezbednosti preko grešaka ljudskog faktora. Pored toga, proces izrade politike bezbednosti će takođe pomoći u definisanju kritičnih sredstava organizacije i načinu njihove zaštite [5].

Kako su zaposleni odgovorni za bezbednost informacija, ta odgovornost mora biti jasna u ugovoru o radu. Uputstvo za zaposlene treba sadržati kodeks ponašanja i sankcije koje su nametnute u slučaju nepoštovanja i ako kao rezultat nastanu incidenti. Za ispravan opis radnih mesta odgovoran je menadžer i stoga je odgovoran za različite aspekte koji se odnose na informacije u različitim pozicijama. Organizacija treba imati rigorozne procedure kada osoblje napušta i stupa u radni odnos ili kada promene posao u okviru organizacije. Ne sme se zaboraviti promena ili ukidanje prava, prikupljanje opreme i propusnica [6].

V. PROCENA RANJIVOSTI SISTEMA

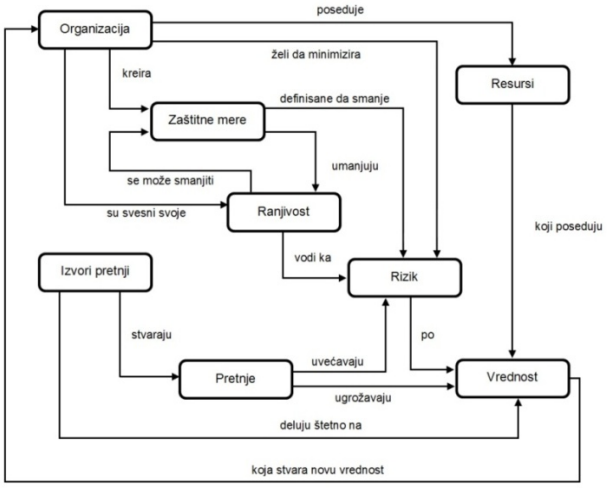
Procena ranjivosti je proces identifikacije i kvantifikacije ranjivosti u sistemu. To je uglavnom ono što iz tehničke perspektive, rade bezbedonosne organizacije – da procenjuju i dokumentuju moguće ranjivosti i da preporuče mere za ublažavanje i unapređenje. Potrebno je da organizacije sastave listu pretnji koje su prisutne u celoj organizaciji i da koriste ovu listu kao osnovu za sve aktivnosti upravljanja rizikom. Lista pretnji organizacije je od neprocenjive vrednosti jer obezbeđuje doslednost, ponovljivost i rešavanje pretnji.

Analiza i procena rizika je postupak kojem je cilj da se ustanove ranjivosti sistema, uoče potencijalne pretnje (rizici) i na odgovarajući način ublaže moguće posledice kako bi se mogao odabrati najprimereniji način zaštite, odnosno proceniti opravdanost uvođenja dodatnih mera.

Svaka organizacija radi kvalitativnu procenu rizika. Rezultat kvalitativne analize iskazuje samo relativan odnos vrednosti šteta nastalih delovanjem neke pretnje i uvođenja mera.
Analizom rizika moraju se utvrditi sledeće činjenice:

- kritični resursi i pretnje i verovatnoća njihove pojave,
- potencijalni gubici koje uzrokuje ostvarenje te pretnje,
- preporučene mere i njihova vrednost,
- nadzor i zaštita.

Ako se analiza rizika procenjuje za ljudske pretnje, uzima se u obzir motivacija napadača, sposobnosti i resursi. Gubitak od realizovane pretnje očigledno zavisi od konkretne pretnje i može da bude gubitak tajnosti podataka (neovlašćenog otkrivanja), gubitak integriteta podataka (neovlašćena modifikacija) ili gubitak raspoloživosti (smanjena funkcionalnost sistema). Potrebno je napomenuti da ISO/IEC 27001 ne nudi specifičnu metodologiju za identifikovanje rizika, dok je ISO/IEC 27005 dizajniran da pomaže u zadovoljavanju implementacije bezbednosti informacija baziranoj na pristupu upravljanja rizikom. Standard podržava opšte pojmove navedene u ISO/IEC 27001 i pruža struktuirani i rigorozan proces za analizu rizika i kreiranju plana postupanja sa rizikom.
Prema novoj reviziji ISO/IEC 27001 potrebno je identifikovati rizike povezane sa tajnošću, integritetom i raspoloživošću informacija. Naime, smisao je u tome da se dopusti više slobode u samom načinu identifikacije rizika.



Slika 1: Upravljanje rizikom [7].

ISO/IEC 27001 zahteva da se mora utvrditi koji se incidenti mogu dogoditi (sprovesti procenu rizika), a zatim pronaći najprikladnije načine da se izbegnu takvi incidenti (tretiranje rizika). Ako se procenom rizika utvrdi neprihvatljiv rizik ISO/IEC 27001 propisuje mere (kontrole) za smanjenje rizika. Uz procenu rizika potrebno je odrediti kako postupati s rizicima.

Mogući postupci uključuju:

- ugrađivanje odgovarajućih kontrola koje smanjuju rizik,
- svesno i objektivno prihvatanje rizika, udovoljavajući bezbednosnoj politici,
- organizaciju kriterijuma prihvatljivog rizika,
- izbegavanje rizika zabranama, tj. onemogućavanjem akcija koje prouzrokuju rizik,
- prenošenje rizika na drugo lice (npr. osiguravajućim kompanijama).

Za rizike čiji postupci uključuju implementaciju odgovarajućih kontrola, te kontrole moraju biti odabrane i implementirane zadovoljavajući zahteve definisane procenom rizika. Izjava o primenljivosti (SOA) je dokument koji navodi sve ISO/IEC 27001 kontrole. Ovo zahteva identifikovanje onih kontrola koje su primenljive i daju obrazloženje za izbor konkretne kontrole. Obrazloženje takođe treba dati za onu kontrolu koja nije izabrana za implementaciju.
Ovaj dokument zapravo pokazuje bezbedonosni profil organizacije – na osnovu rezultata tretmana rizika trebaju biti navedene sve kontrole koje su implementirane. Ovaj dokument je takođe veoma važan jer ga revizor za sertifikaciju koristiti kao glavnu smernicu za reviziju [8].

VI. REVIZIJA I UNAPREĐENJE ISMS-A

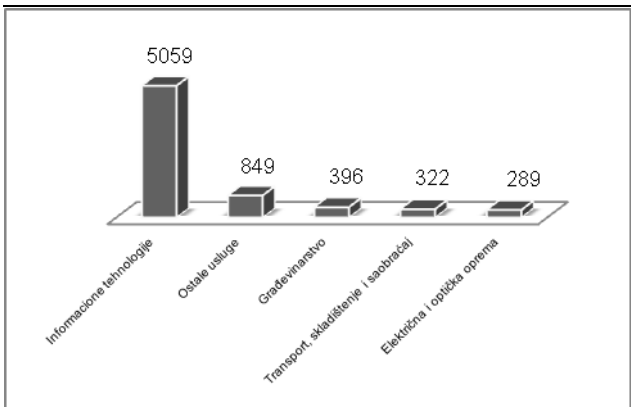
Da bi organizacija bila sertifikovana, neophodno je da sprovede pun ciklus internih revizija i pregleda menadžmenta, koji će ostaviti dokaze o odgovorima na rezultate tih pregleda i revizija. ISMS obuhvata procenu rizika, plan tretmana rizika, izjavu o primenljivosti, politike i procedure koje se preispituju najmanje jednom godišnje [9]. Spoljni revizor će prvo ispitati ISMS dokumentaciju da bi utvrdio obim i sadržaj ISMS-a. Cilj pregleda i revizije je da obezbedi dovoljno dokaza, koji će pokazati efikasnost i efektivnost implementiranog ISMS-a u organizaciji i njenim poslovnim jedinicama. Da bi potvrdili da ISMS nastavlja da radi kao što je navedeno i namenjeno, održavanje sertifikacije zahteva ponovnu periodičnu reviziju. Kada se ISMS progam usvoji, IT sektor ga implementira. Očuvanje procesa provere i kontinuirano nadgledanje poboljšava program. Unapređenje procesa predstavlja smanjenje rizika, prilagođavanjem novim pretnjama i ranjivostima, nakon što su otkrivene, pomaže da se identifikuju moguće slabosti ili nedostatak bezbedonosnih mera koje treba da se dodaju ili poboljšaju u ISMS-u.

Uvođenje ISMS-a zahteva mnogobrojne promene u organizaciji, od promena u procesima i procedurama do promena u čitavoj filozofiji poslovanja i celokupnoj kulturi organizacije. Organizacija implementira sistem za upravljanje bezbednošću informacija efikasno samo ako postoji kultura razumevanja vrednosti informacija i njene zaštite. Ovo zahteva vidljivu posvećenost rukovodstva, kao i obuke u cilju podizanja svesti zaposlenih. Bez toga ISMS ne bi bio efikasan, a samim tim informacije ne bi bile adekvatno zaštićene. Pored toga, širenje informacija bezbednosne politike, standarda i najbolje prakse kao dela svesti o bezbednosti je od vitalnog značaja. Iako svest o bezbednosti informacija može postojati među zaposlenima, kada je reč o stvarnom ponašanju, često zaposleni doživljavaju kontrole bezbednosti informacija kao prepreku ka njihovoj normalnoj rutini.

VII. ORGANIZACIONE DOBITI OD SERTIFIKATA ISO/IEC 27001

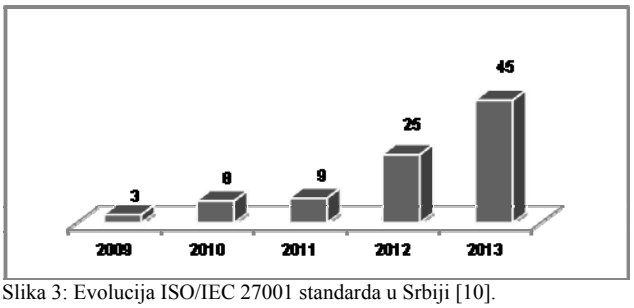
ISO/IEC 27001 je doživeo impresivan rast u poslednjih nekoliko godina, kako u pogledu broja organizacija dobrovoljnog usvajanja standarda i njegovog širenja širom sveta. Standard je prepoznat kao najbolja praksa za bezbednost informacija, međutim, mnoge organizacije traže sertifikat jer ga smatraju sredstvom sticanja konkurentske prednosti u okviru njihovih tržišta. Bez obzira na veličinu i delatnost organizacije, svi usvajaju standard prepoznat kao dobra praksa u bezbednosti informacija. Prvih 5 vodećih industrijskih sektora u svetu po broju ISO/IEC 27001 sertifikata su prikazani na slici 2.

U primeni standarda u svetu su dominantne organizacije koje se bave informacionim tehnologijama. Razlog za to je što informacije u elektronskom poslovanju poseduju kvalitativnu odrednicu kapitala i postaju podjednako značajne kao i finansijski kapital. Zbog toga je i njihova bezbednost sve kompleksnija. Iz tog razloga standard ISO/IEC 27001 pruža pomoć organizacijama bez obzira na njihovu prirodu, tip i veličinu, u razvijanju i primeni sistema za upravljanje bezbednošću informacija i pripreme za nezavisno ocenjivanje (sertifikaciju) tog sistema. ISO/IEC 27001 pruža organizacijama i svim njenim akterima nivo poverenja u meri koja je srazmerna upravljanju bezbednošću informacija.



Slika 2: Prvih 5 industrijskih sektora po broju ISO/IEC 27001 sertifikata za 2013. godinu [10].

Prateći savremene trendove koji se ogledaju u globalizaciji tržišta i težnji za standardizacijom u oblasti sistema bezbednosti informacija, nameće potrebu i obavezu da se i u našim uslovima i okruženjima sprovedu koraci u pravcu implementacije i unapređenja sistema bezbednosti informacija. Iz tog razloga implementacija standard ISO/IEC 27001 doživljava rast iz godina u godinu u pogledu broja organizacija u Srbiji. Samu tokom 2014. godine ima više od 100 sertifikata što je znatno više nego za ceo period od 2009, kada su zabeležene prve organizacije sa sertifikatom, pa zaključno sa 2013. godinom, prikaz na slici 3. U različitim delatnosti i veličinama organizacija se standard primenjuje npr. finansijske institucije, zdravstvene ustanove, IT sektor, telekomunikacije, trgovina, elektrane, a što se tiče veličine, koriste ga i male i velike organizacije.



Slika 3: Evolucija ISO/IEC 27001 standarda u Srbiji [10].

Statistički podaci pokazuju da većina organizacija koje poseduju sertifikat ISO/IEC 27001, takođe posluju u skladu sa standardom ISO 9001, što dovodi do zaključka da je sistem menadžmenta kvalitetom u praksi dobra osnova za uvođenje sistema za bezbednost informacija. Implementacijom ISO/IEC 27001 standarda i sertifikacijom tog sistema, organizacije ostvaruju brojne dobiti i to:

- Poverenje klijenata (kod budućih ili postojećih klijenata stvara se poverenje u informacioni sistem u organizaciji čime se sa klijentima ostvaruju poverljivije i čvršće veze, jer su njihovi podaci bezbedni)
- Smanjenje rizika u poslovanju (obezbeđuje se sistem koji je posebno orijentisan na upravljanje rizikom i kroz upotrebu kontramera, smanjenje rizika na prihvatljiv nivo).
- Poboljšanje poslovnih odnosa (obezbeđuje se naprednije razumevanje informacionih tokova u organizaciji čime se ostvaruje značajna dobit i u poboljšanju poslovnih procesa)
- Unapređenje bezbednosti (obezbeđuje se jasan protok i raspoloživost informacija)

Cilj svake organizacije je postizanje i održavanje konkurentske prednosti. Jedan od načina da organizacija to ostvari je da zadovolji potrebe i očekivanja klijenata i saradnika. Uspešno implementiran sistem upravljanja bezbednošću informacija je organizaciji pouzdan temelj za efektivno i efikasno poslovanje. Interne koristi uspešne implementacije standarda u organizacijama su:

- poboljšana komunikacija organizacije i zaposlenih (prijava rizika i pravovremeno reagovanje na pojavu rizika, smanjenje incidenata i bolje razumevanje uzročnika)
- povećanje operativne efikasnosti (definisanje odgovornosti zaposlenih, bolja komunikacija),
- viši nivo kvaliteta usluga/proizvoda (poverenje kupaca i postizanje konkurentnosti)
- bezbednije poslovanje (poboljšana bezbednost mreža, povećana zaštita informacija)
- razvijenija svest zaposlenih (razumevanje vrednosti informacija i njihove zaštite).

Sve ovo znatno doprinosi konkurentnosti proizvoda i usluga sertifikovanih organizacija na tržištu roba i usluga.

VIII. ZAKLJUČAK

Sertifikacija po standardu ISO/IEC 27001 pruža značajne prednosti i služi kao javna izjava o sposobnosti organizacije za upravljanje bezbednošću informacija. To pokazuje partnerima i klijentima da je organizacija implementirala adekvatne kontrole bezbednosti informacija i poslovnog kontinuiteta. Takođe, pokazuje posvećenost organizacije razvoju i prilagođavaju promenama oblika rizika njenog sistema za upravljanje bezbednošću informacija (ISMS) i politike bezbednosti. Sertifikacija je znak razlikovanja koji postavlja organizacije na nivo odvojenog od njihove konkurencije i obezbeđuje partnerima, akcionarima i klijentima veće pouzdanje.

Važan cilj svake organizacije je bezbednost poslovanja, koje u velikoj meri zavisi od zaštite informacionih i ostalih poslovnih resursa. S tim u vezi, uvođenje sistema upravljanja bezbednošću informacija predstavlja sprovođenje potrebnih mera za postizanje zadovoljavjućeg nivoa informacione bezbednosti unutar organizacije. Time se omogućava nesmetanost odvijanja delatnosti organizacija, ali organizacija postaje prepoznatljiva kao pouzdan i moderan poslovni partner, koja se suočava sa sigurnosnim pretnjama ali sistemski i na vreme reaguje na njih, što za posledicu ima bolju tržišnu poziciju.

LITERATURA

[1] Pleskonjić, D., Maček N., Đorđević, B., Carić, M., „Sigunost računarskih mreža i sistema“, Mikro knjiga, Beograd, 2007.

[2] ISO/IEC 27000:2014, “Information technology – Security techniques – Information security management systems “– Overview and vocabulary, Third edition, ISO/IEC 2014.

[3] Živković, V., Krnjaić, D. „Sistem menadžmenta bezbednošću informacija - uloga i značaj sertifikacije i akreditacije“. Jun 6, 2014. http://www.ats.rs/sites/default/files/download/ISMSVidaZivkovicDejan Krnjaic.pdf

[4] „Politika informacione bezbednosti u Crnoj Gori“. Ministarstvo za informaciono društvo, Podgorica, 2009.

[5] Danchev, D., “Building and Implementing a Successful Information Security Policy”, Jun 6, 2014. ttp://www.windowsecurity.com/pages/security-policy.pdf

[6] Baars, H., Hintzbergen, K., Hintzbergen, J., & Smulders, A. “The basics of information security” - a practical handbook 2009. www.innovanube.com/docs/ISFS_book_English_Final_incl_index.pdf

[7] “ISO 27001”, TQM Constalting, Jun 1,2014. http://www.tqmkonsalting.com/usluge/standardi/sistemi-menadzmenta/iso-27001.html

[8] “ISO 27001:2005 - Sistem menadžmenta za bezbednost informacija”, CIM Grupa, Jun 15, 2014. http://www.cimgrupa.eu/cim/sr/ShowConsulting.aspx?ctrlConsultingDisplay=47

[9] Pelnekar, C. : “Planning for and implementing ISO 27001”, Isaca journall volume 4., 2011.

[10] ISO Survey 2014, Oktobar 2, 2014. http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=iso%209001&countrycode=af

[11] Petar, T. ”Primena ISO/IEC 27000 standarda u domaćim organizacijama”, magistarski rad. Fakultet za menadžment, Sremski Karlovci, 2015.

ABSTRACT

Abstract - The basic premise of ISO/IEC 27001 standards is that information is an asset which as any other asset has its value. This value can be expressed in financial amounts but also through the value of the goals to be achieved. Therefore, attackers seek to do harm by distorting information’s security that is usually reflected through unauthorized modification and manipulation of information. According to many studies conducted in the world and in our country, the practice unfortunately confirms this on daily bases. The insecure information management can lead to loss of business, business reputation and also put the future existence of the organization in a dangerous condition. For this reason, many organizations have adopted ISO/IEC 27001 standard, to help them securely manage their information. To the existing business partners and customers, ISO/IEC 27001 certificate shows that the organization has mobilized effective measures to protect information resources.

IMPLEMENTATION ISO/IEC 27001 AS A FACTOR OF COMPETITIVE ADVANTAGES OF ORGANIZATION

Momčilo Kokić, Petar Tasevski