

JOŽE KNEZ, mr. sc.

SIQ, Ljubljana

joze.knez@siq.si i

GORAN BUDIŠELIĆ, dipl. ing.

SIQ CROATIA, Zagreb

goran.budiselic@siq.hr

SIGURNOST INFORMACIJA PO NORMI ISO/IEC 27001 U POSTOJEĆIM SUSTAVIMA UPRAVLJANJA

Sažetak

U današnjem konkurentskom okruženju rastu potrebe, zahtjevi i očekivanja svih zainteresiranih strana za informacijama kao najvažnijom pogonskom snagom svake organizacije. Kod korisnika se povećava potreba za osiguravanjem raspoloživosti, povjerljivosti i cjelovitosti informacija, koje se pojavljuju u najrazličitijim oblicima.

Područje informatike kao potporni proces u svim organizacijama pridobiva s vremenom u očima najvišega vodstva sve veću važnost. Iako je njemu naložena zadaća za cjelovitu primjenu zahtjeva ISO/IEC 27001, zapravo je to zadaća i skrb svih zaposlenih u organizaciji na svim njenim razinama i područjima rada.

Kod integracije više sustava upravljanja potrebno je prepoznati ona područja, procese ili zahtjeve norma, koja se potpuno združuju u jedinstven oblik i zahtjeve, koji u integriranom sustavu ostanu samostalni. Najvažnije načelo, koje vodi do uvođenja i integracije sustava upravljanja je načelo korisnosti. Neke koristi su direktne, a ostale su indirektno, gdje se rezultati pokazuju tek kroz neko vrijeme.

Pridobivanje ISO/IEC 27001 certifikata ne znači kraj zbivanja na području sigurnosti informacija, već je samo početak cjelovitog upravljanja informacijama.

Ključne riječi: *informacije, sigurnost informacija, integrirani sustav upravljanja, norma ISO/IEC 27001:2005.*

1. UVOD

U današnjem konkurentskom okruženju, zahtjevi i očekivanja svih zainteresiranih strana za boljim i kvalitetnijim proizvodima i uslugama se neprestano povisuju. S tim rastu očekivanja i potrebe za informacijama kao pokretačkim snagama svake organizacije. Kod korisnika se povećava potreba za osiguravanjem raspoloživosti, povjerljivosti i cjelovitosti informacija, koje se pojavljuju u najrazličitijim oblicima.

S ovisnošću o informacijskim tehnologijama povećavaju se i prijetnje i ranjivosti, kojima su izloženi informacijski izvori, što neupitno utječe na povećanje informacijskih rizika. Značajka sustava upravljanja sigurnošću informacija je u upravljanju rizicima. Sama provedba ocjenjivanja rizika organizaciji omogućuje prepoznavanje rizika s kojima se susreće. Upravljanje rizicima označava odabir i uvođenje primjerenih sigurnosnih kontrola (eng. Control) i mjera kojima se rizici smanjuju na prihvatljivu razinu.

Područje informatike kao potpornog procesa svim zainteresiranim strankama pridobiva, iako polako, sve veću važnost u očima najvišeg vodstva. Još prije 10 i više godina dana im je zadaća za implementaciju zahtjeva norme ISO/IEC 27001, iako je to zadaća i briga svih zaposlenika organizacije na svim njezinim razinama i područjima.

Sustav upravljanja sigurnošću informacija po zahtjevima norme ISO/IEC 27001 sadrži glavne elemente odnosno zahtjeve kao i ostali sustavi upravljanja kvalitetom, okolišem i sigurnošću na radu. Zahtjevi najvažnijih elemenata, kao što su: upravljanje dokumentima i zapisima, odgovornost uprave, unutrašnje prosudbe, upravina ocjena i neprekidno poboljšavanje, uključujući preventivne i korektivne radnje, nema smisla (unutar iste organizacije) voditi odvojeno jer se međusobno dopunjuju i tvore jedinstven INTEGRIRAN sustav upravljanja.

Razlike između sustava upravljanja su prvenstveno na stručnom dijelu - u pokazateljima, koje koristimo za mjerenje zadanih ciljeva i u metodama kojima te pokazatelje mjerimo, pratimo i ocjenjujemo njihovu učinkovitost i djelotvornost. Prilikom upravljanja sigurnošću informacija crvena nit i pokazatelj sigurne organizacije je ocjenjivanje informacijskih rizika. Pokazatelj učinkovitosti sustava upravljanja kvalitetom je zadovoljstvo kupca, ne samo onih koji će naš proizvod ili uslugu koristiti, već prije svega internih kupaca u procesima unutar organizacije, kojima najčešće dajemo premalo naglaske i pozornosti. Pokazatelj učinkovitosti sustava upravljanja okolišem ili okolišu prihvatljive organizacije je broj prepoznatih utjecaja na okoliš.

2. NORME ISO/IEC 27001:2005 I ISO/IEC 17799:2005 I NJIHOVA POVIJEST

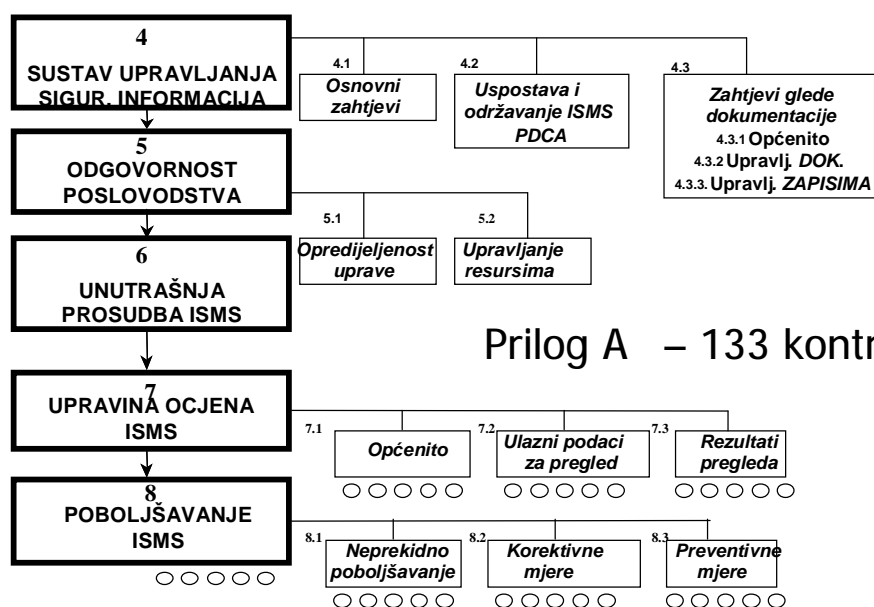
Na samom početku norma BS 7799 nastala je pod okriljem British Standards Institute. To je i od poslovodstva i od pojedinih tehnoloških rješenja neovisan alat, koji nudi cjelovit pogled na upravljanje sigurnošću informacija. Norma je prvi put izašla 1995. godine kao kodeks dobre prakse, a tijekom godina je nadopunjavana da bi 1999. bila podijeljena na dva dijela BS 7799-1 i BS 7799-2.

Normu BS 7799-1 je preuzela međunarodna organizacija za standardizaciju ISO i izdala ju pod imenom ISO/IEC 17799 2005 godine. Ta norma nudi izbor mogućih mjera odnosno sigurnosnih rješenja, koje organizacije mogu koristiti s ciljem smanjivanja sigurnosnih rizika. Takva sigurnosna rješenja su se kroz godine korištenja u različitim organizacijama diljem svijeta pokazale kao učinkovita i dobra praksa. 133 kontrole, koje su namijenjene za ostvarivanje 39 ciljeva, razvrstane su unutar jedanaest poglavlja:

5. Politika sigurnosti informacija
6. Organizacija sigurnosti informacija
7. Upravljanje sredstvima
8. Osiguranje ljudskih resursa
9. Fizička zaštita i zaštita okoliša
10. Upravljanje komunikacijama i proizvodnjom
11. Nadzor dostupa
12. Kupovina, razvoj i održavanje informacijskih sustava
13. Upravljanje incidentima u zaštiti informacija
14. Upravljanje kontinuitetom poslovanja
15. Sukladnost

U normi ISO/IEC 27001:2005 (prethodno izdanje BS 7799-2) opisani su pojedini elementi sustava upravljanja sigurnošću informacija (slika 1), i procesi uspostave takvog sustava u praksi, i to u obliku Demingovog kruga PDCA (PLAN - DO - CHECK - ACT)). Norma je napisana u obliku zahtjeva, koje sustav treba ispunjavati, te omogućava ocjenjivanje bilo interno ili vanjsko, od neovisne certifikacijske institucije. Sadrži i neka pojašnjenja i upute za korištenje.

Slika 1: Zahtjevi norme ISO/IEC 27001:2005.



Prilog A – 133 kontrole

Da ponovimo, sustav opisan u ovoj normi je prije svega poslovni alat, koji je neovisan o pojedinačnim tehničkim rješenjima. Cjelovitost norme je i u tome što ne obrađuje samo informacijske tehnologije i informacije u elektroničkom obliku, već i informacije u različitim oblicima i na različitim medijima. Većina opisanih kontrola je sasvim organizacijske prirode i nisu povezana ni sa kakvom tehnologijom. Tako su npr. klasifikacija informacija, politika praznog stola, fizička zaštita objekata ili opis sigurnosti informacija u ugovorima o zaposlenju. Kako je razvoj informacijskih tehnologija ono što je omogućilo svladavanje tolikog opsega informacija, razumljivo je da je veliki dio kontrole povezan s informacijama u elektroničkom obliku npr. zaštita od zlonamjerne programske opreme, nadzor dostupa do mreže, sigurnost sistemskih datoteka, upotreba kriptografije za šifriranje podataka, besprekidnog napajanja ili požarnih zidova.

3. USPOSTAVLJANJE I IZVOĐENJE SUSTAVA UPRAVLJANJA SIGURNOSTI INFORMACIJA

Kao što i sama norma ISO/IEC 27001 navodi, primjena sustava znači da organizacija planira, izvodi, provjerava i djeluje prema načelima Demingovog kruga.

U fazi PLAN organizacija definira: opseg i politiku, metodologiju ocjenjivanja rizika, definira rizike, ocjenjuje ih, pronalazi i vrednuje moguće ispravke, odabire kontrole, priprema dokument Statement of applicability i pridobiva odobrenja uprave. Zbog takve kompleksnosti i važnosti ocjena rizika za uspostavljanje cjelokupnog sustava prvi korak pri

uvođenju sustava upravljanja sigurnošću informacija je odabir primjerenog pristupa. To uključuje jasnu raspodjelu zadataka i odgovornosti te izbor primjerene metodologije za ocjenjivanje rizika. Bitno je da ocjenjivanje rizika daje uporabljive rezultate. Njezina osnovna namjena nije vrednovati sve rizike, kojima je neka organizacija izložena, već prepoznati ona područje poslovanja, koja su prema jedinstvenim mjerilima podložna najvećim rizicima. Tako se u praksi pokazuje da izračun očekivanog iznosa godišnjeg gubitka može biti vrlo zahtjevan i da ga je vrlo teško ocijeniti s točnošću većom od reda veličine. Veliki broj organizacija, koje su već certificirale svoj sustav upravljanja sigurnošću informacija, upotrijebilo je pragmatičan i jednostavan pristup razvrstavanja rizika u nekoliko opisnih razreda (npr, od „vrlo nisko“ do „vrlo visoko“).

U fazi DO organizacija: oblikuje, planira upravljanje rizicima, vodi procese i resurse, izvodi postupke, politiku, upute i izvodi osposobljavanje i osvještavanje svih zaposlenih i zainteresiranih strana.

U fazi CHECK organizacija: izvodi nadzorne postupke, redovno pregledava učinkovitost sustava, pregledava preostale i prihvatljivi rizike, redovito izvodi unutrašnje prosudbe, provodi upravine ocjene, i bilježi djelovanja / događaje / incidente koji mogu utjecati na sustav upravljanja sigurnošću informacija.

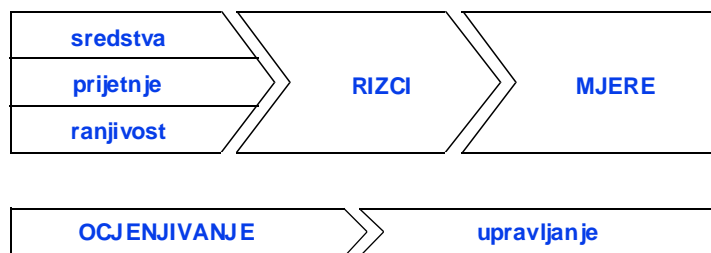
U fazi ACT organizacija: uvodi prepoznata poboljšanja, djeluje korektivno i preventivno, komunicira i savjetuje se te se pobrine da poboljšanja dostignu svoje ciljeve.

4. UPRAVLJANJE RIZICIMA

Upravljanje rizicima (risk management) ima početke u osiguranju iz ranih 1950-ih. Namjena mu je smanjiti i otkloniti određene vrste rizika, povezanih s poslovanjem, a njegov osnovni problem je donošenje odluka u uvjetima nesigurnosti.

Na jednoj strani upravljanje rizicima je znanost jer pri rješavanju problema koristi teoriju odlučivanja i znanstvene metode za upravljanje. Znanstveni pristup predstavlja prepoznavanje alternativnih rješenja i izbor onih s najvećim mogućnostima za uspjeh. S druge strane, upravljanje rizicima je spretnost, jer je vrlo važan osjećaj za situaciju i volja za odlučivanje iako nisu raspoložive sve informacije. Upravljanje rizicima može se u grubo podijeliti na dva dijela: ocjenjivanje rizika (risk assesment) i izvođenje mjera što se vrlo često naziva i upravljanje rizicima (risk management) (slika2).

Slika 2: Pojednostavljeni model upravljanja rizicima



Veličinu rizika definiraju vjerojatnost neželjenog ishoda i veličina (vrijednost) gubitka, do kojeg bi došlo u slučaju tog ishoda. Vjerojatnost je kombinacija opasnosti i ranjivosti. Opasnost je uzrok gubicima, dok je ranjivost položaj koji može ostvariti ili povećati mogućnost za gubitak zbog dane opasnosti. Stupanj poslovnog rizika izražavamo kroz očekivanu vrijednost gubitka, koja je umnožak vjerojatnosti događaja i vrijednosti gubitka.

S prepoznavanjima i mjerenjima rizika moramo se na neki način suočiti. Djelovanje (ili nedjelovanje) predstavlja drugi dio upravljanja rizicima. Možemo postupati na više načina: prepustimo se rizičnim situacijama, rizike umanjimo (spriječimo ili smanjimo mogućnost pojavljivanja ili nadziremo velike gubitke ukoliko do njih dođe), prenesemo ih na druge (osiguranje) ili raspodijelimo. Ukoliko ne postoje bolje alternative možemo se i sprijateljiti s njima. To je možda najčešći i često najbolji način, naravno ukoliko su mogućnosti gubitka male. Glavna vodilja pri izboru pravog načina reagiranja je troškovna učinkovitost. Primjerenim načinom želimo dosegnuti situaciju u kojoj je vrijednost preostalog rizika i cijena mjera minimalna.

5. DOBRE PRAKSE U UPRAVLJANJU INFORMACIJSKIM RIZICIMA

Norma ISO/IEC 27001 ne zahtjeva poslovnik sustava upravljanja kao ISO 9001. Zato su organizacije, koje već imaju uspostavljen neki od sustava upravljanja u prednosti. U okviru postojećih procesa, postupaka i dokumenata većinom su obuhvaćeni i zahtjevi norme ISO/IEC 27001, koji su navedeni u poglavljima od 4 do 8. Preostali specifični zahtjevi u obliku 133 kontrole nalaze se u prilogu A, a organizacije ih po potrebi mogu uključiti u postojeće ili novonastale dokumente i postupke.

Koliko, kakve i kako opsežne će te dopune biti, u najvećoj mjeri ovisi o ocjeni informacijskih rizika, koji su crvena nit zahtjeva i uputa norme. Opsežnost ocjene rizika ovisi o kompleksnosti i značaju informacija u poslovanju organizacije. Na osnovu analize rizika organizacija će, s namjerom njihovog snižavanja na željenu razinu, uključiti zahtjeve iz dobre prakse. Oni su opisani u 133 kontrole, navedene kao sažetak u prilogu A norme ISO/IEC 27001. Detaljniji opis pojedine kontrole, smjernice za provedbu i druge informacije nalaze se u normi ISO/IEC 17799.

Uz preporučene 133 kontrole organizacija može uvesti i dodatne kontrole, koje koristi u svojem poslovanju. Kao primjer dobre prakse prethodno spomenuti dokument zasnovan je tako da pri svakoj kontroli s poveznicama „linkovima“ navedemo, gdje odnosno u kojem dokumentu očekujemo odgovor na nju, odnosno gdje je opis razloga ispuštanja, koji se odnose na prilog A.

6. INTEGRACIJA ZAHTJEVA U POSTOJEĆI/E SUSTAV/E UPRAVLJANJA

U organizaciji gdje se uprava odluči za integraciju sustava upravljanja, potrebno je prepoznati područje različitih sustava koji se integriraju. Pri tome je potrebno prepoznati ona područja, procese ili zahtjeve normi koji se potpuno integriraju u jedinstveni oblik i zahtjeve koji u integriranom obliku ostaju samostalni.

Iz godine u godinu povećava se broj organizacija, koje upotrebljavaju i združuju različite sustave upravljanja (sustavi upravljanja kvalitetom, okolišem, sigurnošću i zdravljem na radu, sigurnošću informacija) u jedan združen - integriran sustav upravljanja. Najvažnije načelo, koje vodi k uvođenju i integraciji takvih sustava upravljanja je načelo koristi. Neke od njih su direktne, ostale su indirektno, gdje se rezultati pokažu u određenom vremenskom periodu.

7. NEKOLIKO PRIMJERA DOBRE PRAKSE PRI UKLJUČIVANJU NOVIH ZAHTEJEVA U POSTOJEĆI SUSTAV

Preporučljivo je, da se poslovnik sustava upravljanja kvalitetom preimenuje u „Poslovnik sustava upravljanja“, a kojega je potrebno dopuniti specifičnim zahtjevima i povezati ga s novonastalim dokumentima po normi ISO/IEC 27001.

Dokument »Sigurnosna politika« može biti samostalan dokument i povezan s poslovníkom sustava upravljanja, pri čemu njegov sadržaj može biti uključen u poslovnik ili se može uključiti u postojeću politiku sustava upravljanja.

Zahtjev »4.3.2 Upravljanje dokumentima« je na primjer s normama ISO 9001 i ISO 14001 potpuno jednak, osim u zahtjevu da je upravljanje dokumentima različitih sigurnosti definirano njihovim zahtjevima. Spomenuti zahtjev se navede u dokumentiranom postupku organizacije sa već postojećim sustavom upravljanja.

Zahtjev »4.3.3 Upravljanje zapisima« se od ISO 9001 ne razlikuje.

Zahtjev »6 Unutrašnje prosudbe ISMS« se u usporedbi s ostalim sustavima upravljanja načelno ne razlikuje. Zbog toga je preporučljivo da se unutrašnje prosudbe sustava izvode kao integrirana aktivnost s ostalim sustavima upravljanja prema zahtjevima norma ISO 19011, s tim da se provjere specifični zahtjevi ISO/IEC 27001.

8. ZAŠTO SE CERTIFICIRATI?

Razlozi su različiti. Uspostavljen i certificirani sustav prema zahtjevima norme ISO/IEC 17799 i ISO/IEC 27001:2005 organizaciji donosi više koristi. U trenutku pridobivanja certifikata kroz nepristrani vanjski pogled nudi pogled na poslovanje i otkriva mogućnosti za poboljšavanje. Pridobiven certifikat povećava povjerenje poslovnih partnera i drugih interesnih skupina. Često predstavlja i prednost pred konkurencijom i moguće ga je iskoristiti i u marketinške namjene.

Navodimo neke od poslovnih koristi:

- smanjivanje sigurnosnih rizika,
- prepoznavanje i smanjivanje sigurnosnih rizika na željenu razinu,
- poboljšavanje poslovnih odnosa (veće povjerenje u međusobno razmjenjivanje informacija),
- investicije na prava akutna mjesta,
- optimizirana poslovna partnerstva,
- upravljanje sigurnošću,
- upravljanje procesima sigurnosti informacija.

SIQ u suradnji s certifikacijskom kućom CIS iz Beča može dodijeliti akreditirani certifikat prema zahtjevima norme ISO/IEC 27001:2005.

9. ZAKLJUČAK

Pridobivanje certifikata ISO/IEC 27001 ne predstavlja kraj nastojanja na području informacijske sigurnosti, već je početak u cjelovitom upravljanju informacijama i kvalitetom. Glavni razlog za uvođenje i kasnije za pregled od strane neovisne institucije je svakako sve važnija uloga, koju informacije imaju u svakodnevnom poslovanju. Udio usluga u gospodarstvu stalno raste, djelatnosti vezane uz informacije (u što se ubrajaju i banke i osiguravajuća društva) doseže visoku dodanu vrijednost. Sve to nas upozorava koliko je važno znati dobro upravljati i osiguravati informacije, koje za organizaciju predstavljaju sve veći značaj.

Uspostavljen i održavan sustav upravljanja sigurnošću informacija osigurava vam prije svega uvjete za neprekinuto poslovanje i odvijanje svih procesa i odnosa zainteresiranih strana, odnosno uvjete za njihovo učinkovito i djelotvorno upravljanje.

Literatura:

- ISO/IEC 27001:2005 Information Security Management Systems - Requirements,
- ISO/IEC 17799:2005 Information technology - Code of practice for information security management,
- ISO 19011:2002 Smjernice za prosudbu sustava upravljanja kvalitetom i/ili okolišem,
- ISO/IEC TR 13335-3:1998 Information technology – guidelines for the management of IT security. Part 3: Techniques for the management of IT security.

INFORMATION SECURITY UPON ISO/IEC 27001 STANDARD AND EXISTING MANGEMENT SYSTEMS

Summary

In today's competitive surroundings the needs, requirements and expectations of all interested parties for information, as the driving force of every organization, are rising. Users need for ensuring availability, confidentiality and integrity of information, which appears in many forms, is growing.

The field of information science as a supporting process in all organizations is gaining importance with time in the eyes of top management. Although it has been given the task of fully implementing the requirements of ISO/IEC 27001, it is in fact the task of everyone employed in the organization, on all its levels and fields of activity.

During integration of different management systems it is important to recognize those fields, processes or standard requirements, which fully join into a unique form and requirements, which remain independent in the integrated system. The most important principle, which leads to implementation and integration of management systems, is the principle of usefulness. Some of benefits are direct, while others are indirect, where the results are shown after a certain time.

Gaining the ISO/IEC 27001 certificate does not mean the end of activities in the field of information security, it is only the beginning of total information management.

Key words: *information, information security, integrated management system, standard ISO/IEC 27001:2005.*