Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 005.6
DOI: https://doi.org/10.24867/02GI06Maletic

IMPLEMENTACIJA SISTEMABEZBEDNOSTI INFORMACIJAISO/IEC 27001 U KOMPANIJI „FMS“ BEOGRAD, SA OSVRTOM NA PROCENU RIZIKA

IMPLEMENTATION OF ISO/IEC 27001 INFORMATION SECURITY SYSTEM, WITH RESPECT TO RISK ASSESSMENT, IN THE COMPANY „FMS“ BEOGRAD

Siniša Maletić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – INDUSTRIJSKO INŽENJERSTVO i MENADŽMENT

Kratak sadržaj – *U radu je opisana implementacija standarda ISO/IEC 27001 na primeru studije slučaja preduzeća „FMS" Beograd. Implementacijom ovog standarda obuhvaćena je procena rizika kao i primena svih kontrola u politici bezbednosti.*

Abstract *–This tthesis describes the implementation of ISO / IEC 27001 standard on the case studyof company„FMS“ Belgrade. The implementation of this standard includes risk assessment as well as the application of all controls in the security policy.*

Ključne reči: *ISO/IEC 27001, quality management, risk assessment.*

UVOD

Organizacije utvrđuju sve više potrebu za ovim standardom kako bi informacije koje poseduju bile adekvatno zaštićene. Sistemi postaju sve robusniji, složeniji, aplikacije sve neophodnije. Gubitak podataka često može biti fatalan i nepovratan za organizaciju. Stoga se ozbiljno mora shvatiti proces upravljanja i zaštite podataka. ISO/IEC 27001 [1] je zvanično objavljen 2005 i u njemu su definisani zahtevi za upravljanje sistemom bezbednošću informacijama i okviri kako se njegova implementacija sprovodi. U ovom radu je posebno definisan osvrt na analizu rizika. Rizik bi trebalo definisati kao „Mogućnost bilo kog ishoda koji nije očekivan“ [2]. U taj ishod svakako spada mogućnost gubitka informacija odnosno, koji su ključni za upravljanje organizacijom koja je analizirana u radu

1. METODOLOGIJA NAUČNOG ISTRAŽIVANJA

Cilj istraživanja ovog rada je dokumentovanje, odnosno usaglašavanje sistema menadžmenta organizacije „FMS“ doo sa zahtevima standarda ISO/IEC 27001. Organizacija „FMS“ doo, koja se analizira, bavi se uvozom i distribucijom opreme za praćenje potrošnje goriva, kao i opremom za praćenje vozila. Implementacijom sistema ISO/IEC 27001 omogućava se dalji razvoj kompanije kao i posedovanje sertifikata.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Milan Delić, docent.

Analizom poslovanja kompanije „FMS“ doo, dolazi se do zaključka o potrebi uvođenja ISO/IEC 27001 standarda, sa ciljem zaštite informacione imovine kompanije. Jedan deo poslovanja organizacijevezan je za kancelariju (prodaja, podrška, razvoj), drugi deo za teren (prilikom ugradnje senzora i obuke). S obzirom na brojne projekte i aktivnosti koje organizacija obavlja.

2. PROCESNI PRISTUP

Procesni pristup je jedan od osnovnih okvira upravljanja kvalitetom. Ovaj pristup daje smerniceza dobro funkcionisanje organizacije tj. za stalno poboljšanje njenih procesa.Kako bi se ostvarivali ciljevi, neophodno je uspostaviti nekoliko koraka koje procesni pristup od nas zahteva, a to su: “uspostavljanje, implementacija, praćenje i merenje, preispitivanje, održavanje i stalno poboljšanje našeg sistema” [3].

Temelje procesnog pristupa uspostavio je Edvard Deming kroz poznati PDCA model ili Demingov krug.Standard ISO/IEC 27001 je razvijen na bazi modela PDCA (plan-do-check-act) ciklus stalnog unapređenja. Proces upravljanja rizikom je izuzetno složen proces. Potrebno je utvrditi kontekst organizacije i uspostaviti ga. To podrazumeva aktivnosti koje se bave pitanjem šta treba preduzeti u odnosu na postavljene ciljeve.

Identifikacija rizika podrazumeva aktivnosti koje određuju šta se može dogoditi, kada, kako izbog čega. Iz postavljenih pitanja sledi analiza rizika.Ocenjivanje utvrđenih rizika predstavlja sledeći korak u procesu upravljanja rizicima u organizaciji. Delovanje na rizike, odnosno, kako najbolje delovati na njih, krajnja je aktivnost prilikom upravljanja rizikom.

3. O STANDARDU ISO/IEC 27001

Standard koji se primenjuje za očuvanje zaštite informacija i podataka je ISO/IEC 27001. Dobre strane implementacije standarda su:

- Usklađenost sa zakonskim regulativama iz oblasti bezbednosti informacija,
- Njegovim uvodjenjem obezbeđuju se konstantna poboljšanja performansi procesa,
- Određivanjem politike informacione sigurnosti, teži se postizanju ciljeva, definišu se procedure i upustva,
- Analiziraju sei indentifikuju potencijalni rizici za sve procese unutar i izvan organizacije.

3.1 Osnovni gradivni elementi ISO/IEC 27001

Prikazana su tri osnovna elementana iz kojih se standard ISO/IEC 27001 sastoji:

- Poverljivost: Veoma bitan element standarda u kojem se naglašava da informacije nisu dostupne trećim licima, kao ni procesi.To znači da je posebna pažnja posvećena očuvanju bezbednosti sistema.
- Integritet: Za svaku informaciju koja sekoristi u sistemu, pretpostavlja se da mora da bude tačna, kao i njen sadržaj.
- Dostupnost: Informacije moraju da budu pristupačne za obradu, osobama kojima je to odobreno, shodno definisanim procedurama.

Potencijalni rizici i pretnje po sistem se svode na minimalnu meru, ukoliko se na vreme indentifikuju i predlože mehanizmi za njihovo smanjenje. Konstantnom edukacijom i obukama o značaju ovog standarda i informacionog bezbednosti, stvara se svest o finansijskoj dobiti i smanjenju grešaka. Ukoliko se incidenti smanje na vreme bolje će se identifikovati aktivnosti nadzora nad poslovnim procesima.

4. O RIZICIMA

„Hazard je izvor, situacija ili postupak koji mogu dovesti do štete u vidu povrede ljudi, narušavanja njihovog zdravlja ili gubitka imovine bitne za organizaciju" [4].
Posebno vrstom opasnosti smatramo one koju su neposredno vezane zaživot i rad organizacije. Podele su vezane često za tehniku, finansije kvalitet, upravljanje resursima i samom organizacijom. Samo ime hazard dolazi od arapskog jezika „AZ-AZHAR" koji označava igranje sa dve kocke ili kockanje (gde su se gubila, gube i gde će se gubiti ne samo imanja već i još mnogo toga). Zato se danas pojam „Hazard" povezuje sa mestom ili uzorkom potencijalne opasnosti. Pojam "rizik" dolazi iz Starogrčkog jezika gde ima značenje "Hrid, litica, opasnost". Prvi moderan oblik primene reči rizik nalazi se u „Oxford English Dictionary" iz 1621. Godine i glasi: „Rizik je mogućnost gubitka, ozlede ili drugih štetnih ili neželjenih okolnosti". Standard ISO 31000:2008 i upustvo koje ga prati, definišu rizik kao "Efekat nesigurnosti na ciljeve". Serija standarda OHSAS definiše rizik kao proizvod verovatnoće postojeće opasnosti (hazarda) kod nastupa neželjenog događaja sa ozbiljnošću posledice takvog događaja. U području Standarda za informaciju sigurnost ISO/IEC 27005:2018 rizik je proizvod tri elementa: Pretnje, ranjivosti i posledice neželjenog događaja(čemu je proizvid pretnji i ranjivosti jednak vevovatnoći nastupa neželjenog događaja).

5. ZNAČAJ i ANALIZA RIZIKA

Kao što smo napomenuli rizik je mogućnost gubitka ili ishoda koji ne očekujemo, ali moramo da ga predvidimo. Njegovom detaljnom analizom mi bi smo jasno definisali sve moguće situacije i kako da reagujemo ukoliko se ista pojavi. U uvodnom poglavlju ćemo samo napomenuti na koji način se pristupa njegovoj proceni i kako se indentifikuje u skladu sa ISO/IEC 27001. U daljem poglavlju rada ćemo prikazati primer izveštaja o proceni rizika kao i plan njegovog tretiranja. Sve informacione vrednosti koje su identifikovane tokom analize faza sprovođenja procesa su podvrgnute analizi uticaja na poslovanje (BIA-Busines inpact analisyst), u sladu sa potrebom procene rizika. Da bi se sastavio popis informacione imovine, zaposleni u okviru projekta moraju biti anketirani o tome koja informaciona imovina im je potrebna za obavljanje posla. Nakon što je popis informacione imovine završen, menadžer sistema bezbednosti informacija će analizirati rezultate i kategorizovati imovinu sličnih poslovnih procesa, zajedno sa identifikovanim grupama imovine.

Računanje se vrši prema formuli:

(Analiza uticaja na poslovanje (BIA) vrednosti grupe imovine) * pretnja * ranjivost = Rezultat rizika.

Da bi se sastavio popis informacione imovine, zaposleni u okviru projekta moraju biti anketirani o tome koja informaciona imovina im je potrebna za obavljanje posla. Nakon što je popis informacione imovine završen, MSI-Menadžer sistema bezbednošću informacija (u daljem tekstu MSI) će analizirati rezultate i kategorizovati imovinu sličnih poslovnih procesa, zajedno sa identifikovanim grupama imovine.

Redovna preispitivanja popisa imovine i poslovnih rizika su sastavni deo procene bezbednosnih rizika u skladu sa SRPS ISO/IEC 27001, ta delatnost omogućuje usklađenost sa bezbednosnim pravilima koja treba proveriti, kao i delotvornost sprovedenih kontrola. Informaciona imovina je grupisana na takav način, da sve nove informacije koje su primljene ili nastale, budu lako prepoznatljive i dodate u odgovarajuću informacionu grupu.

MSI će uporediti podatke dobijene tokom identifikacije informacione imovine i analize uticaja na poslovanje (BIA) i sprovesti analize pretnji, ranjivosti i verovatnoće događaja u grupama informacione imovine, kod kojih je pređen ranije utvrđen prag rizika/štete. Pretnje i ranjivosti se identifikuju na osnovu informacija koje se nalaze u tabeli procene rizika.

6. O KOMPANIJI

Kompanija „FMS" doo se nalazi u Beogradu. Njena delatnost je uvoz i prodaja uređaja za pozicioniranje vozila, kao i uredjaja za smanjenje potrošnje goriva. Kupac šalje organizaciji zahtev za ponudu usluge. Kompanija obrađuje zahtev i njihovi komercijalisti šalju ponudu, koja sadrži cenu uređaja, cenu ugradnje i garantne rokove. „FMS" doo nije jedina kompanija koja se bavi uvozom i distribucijom uređaja, sondi za krađu goriva. Međutim, za vrlo kratko vreme postaje jedan od lidera na teritoriji Srbije. Zloupotrebe sa gorivom postaju sve veće, shodno širenju kapaciteta logističkih kompanija. Tradicionalni način evidencije goriva omogućuje brojne zloupotrebe. Mnogi korisnici se odlučuju na upotrebu dodatne senzorske opreme kao i opreme za praćenje vozila, kako bi imale daleko bolje evidencije zloupotreba, a samim tim i ušteda. „FMS" je generalni uvoznik i distributer „Omnicomm" senzorske opreme.

7. CILJEVI INFORMACIONE SIGURNOSTI

Ciljevi koje organizacija uspostavlja, zasnovani su na politici kvaliteta. Obično su zasnovani na načinu na koji se mogu preispitivati i meriti. Razmatranjem ciljeva organizacija ujedno preispituje performanse procesa, usluge i zadovoljstvo svojih klijenata.

1. Prekid primene sistema upravljanja informacione sigurnosti, ne može biti više od 4 sata godišnje (uticaj na dostupnost),
2. Tajni podaci se ne odaju neovlašćenim i trećim osobama (Uticaj na poverljivost i integritet).
3. Moguć je najviše jedan incident godišnje , kada neovlašćene osobe udju u prostor „FMS“ doo (uticaj na poverljivost),
4. Najviše 4 incidenta godišnje, gde IT sistem ne može da odgovori na zahteve organizacije (uticaj na integritet),
5. Nema gubitka dokumentacije ili zapisa (uticaj na integritet i dostupnost),
6. Obuka najmanje jednog Menadžera bezbednosti informacija internog ocenjivača (uticaj na dostupnost),
7. Nema uspešne pojave virusa (ili zlonamernog koda) ili detektovanje i otklanjanje u najbržem mogućem roku (uticaj na integritet, raspoloživost i dostupnost),
8. Nema narušanjava sigurnosti poslovanja (uticaj na integritet, raspoloživost i dostupnost).

Definisanjem ciljeva organizacija sebi postavlja zadatke koje mora ispuniti, kako bi što efikasnije i efektivnije poslovala na tržištu.

8. POSLOVNIK

Poslovnikom definišemo celokupnu dokumentaciju sistema mednadžmenta kao i njegov opis. U radu su prikazani njegovi najvažniji delovi. Analiza rizika je izuzeta iz poslovnika jer je definisana u uvodnom poglavlju i kroz izveštaj o proceni rizika. „FMS“ Beograd ima zadatak da uspostavi, implementira, upravlja, nadzire, pregleda, održava i poboljšava dokumentovani ISMS-sistem menadžmenta bezbednosti informacija (u daljem tekstu ISMS) unutar celokupnog poslovanja organizacije i u okviru rizika sa kojima se suočava. Za potrebe ovog međunarodnog standarda, procesi koji se koriste zasnivaju se na modelu "planirajte-uradite-proverite-delujte“. Područje koje je obuhvaćeno ISMS primenom standarda SRPS ISO/IEC 27001:2014 je od pomoći u promovisanju i raspodeli ciljeva „FMS“ Beograd i trenutnog poslovnog plana u sigurnom okruženju. Celokupno „FMS“ Beograd osoblje, realizatori poslova i učesnici treće strane se nalaze u sistemu ISMS i dobijaće informacije vezane za svoju ulogu i odgovornost.

Fizička i informaciona imovina koja se koristi, u vlasništvu „FMS“ obrađuje se ili čuva na licu mesta, takođe u okviru delokruga organizacije i ocenjivaće se u odnosu na rizike po pitanju poverljivosti, integriteta i dostupnosti. Tamo gde je identifikovan visok stepen rizika, preduzimaće se postupci na smanjenju rizika, moraju se dokumentovati i istražiti. Van područja primene ISMS su informacione vrednosti koje se koriste isključivo od strane kupaca ili učesnika treće strane. Bilo kakve informacione vrednosti trećih lica koje se nalaze kod „FMS” smatraće se da su u sklopu ISMS sistema. „FMS” uspostavlja ISMS da bi se osigurao kontinuitet poslovanja, štiteći poverljivost, integritet i dostupnost informacija i poslovnih vrednosti i kako bi se smanjila šteta sprečavanjem i minimiziranjem uticaja incidentnih bezbednosnih događaja. Dužnost „FMS Beograd” je da obezbedi da sve informacije o narušavanju bezbednosti budu obrađene.

Rukovodstvo „FMS” je odgovorno za sveukupno upravljanje i opredeljenost za informacionu bezbednost. Menadžeri sektora su odgovorni za osiguravanje saopštavanja politike zaposlenima i trećim stranama, tako da je politika potpuno sprovedena unutar njihovih sektora. Menadžer bezbednosti informacija ima direktnu odgovornost za održavanje politike i pružanje smernica za njeno sprovođenje. Koordinacijom informacione bezbednosti rukovodi menadžer bezbednosti informacija (MSI). Jasan pravac i podrška bezbednosnim inicijativama, moraju se pokazati potpunim saopštavanjem takvih inicijativa i kontrolama od strane zaposlenih i trećih lica, kao i njihovo sveobuhvatno sprovođenje. Najviše rukovodstvo mora biti posvećeno načelima najbolje prakse informacione bezbednosti i standardima iz te oblasti i dokazati to uspostavljanjem i donošenjem bezbednosnih politike najopštijeg nivoa. Menadžer bezbednosti informacija je glavni koordinator za bezbednost i kontinuitet poslovanja. Najviše rukovodstvo će pružiti MSI ovlašćenje da dovede organizaciju do opšte bezbednosti i kontinuiteta poboljšanja i održavanja programa zaštite poslovanja.

Dugoročni cilj je smanjiti količinu vremena, novca i napora neophodnih za rešavanje narušavanja bezbednosti, pitanja kontinuiteta i incidenata, uvođenjem kontrola koje sprečavaju ili umanjuju verovatnoću njihovog pojavljivanja.

Menadžment će razmotriti, raspraviti i postaviti pravila o bezbednosnim pitanjima koja utiču na organizaciju i MSI će pratiti njihovu delotvornost.

9. POLITIKA KLASIFIKACIJE INFORMACIJA

Organizacija pruža efikasne i ekonomične elektronske usluge za razne klijente. Kao takva organizacija mora da uspostavi standarde i sredstva za efikasnu zaštitu podataka od neovlašćenog pristupa , zloupotrebe ili odavanja informacija. U skladu sa takvom politikom organizacije ustanovljeno je odgovarajuće pravilo za klasifikaciju informacija i zaštitu imovine i podataka kojima raspolaže. Svi delovi organizacije , saradnici i zaposleni moraju imati definisane odgovornosti i primenjivati odgovarajuća pravila za zaštitu informacija i u skladu s tim mora biti obavljena klasifikacija informacija u organizacij**i.**

10. IZVEŠTAJ O PROCENI RIZIKA

Organizacija „FMS“ d.o.o. Beograd kroz rad odbora za zaštitu informacija je analizirala procenu rizika u oblasti bezbednosti informacija sačinjava izveštaj. Izveštaj o proceni rizika uspostavlja metodologiju procene rizika i u skladu s tim, koristiće se kao procedura s kojom će se postupati, pri budućim procenama rizika. Opseg SMBI-a obuhvata ceo poslovni proces i IT usluge. U opseg je uključena sva informatička imovina, lokacije, tehnologija i zaposleni u „FMS“ d.o.o. koji aktivno učestvuju u radu sa imovinom i informacijama organizacije.

Procena rizika obuhvatila je poslovni prostor, tehnološku opremu i radne procese koji se koriste u radu organizacije „FMS“ d.o.o. Beograd i sve komunikacije koje organizacija obavlja sa spoljnim poslovnim okruženjem. Ovom analizom je obuhvaćen i sav softver i dokumenta sistema upravljanja kvalitetom. Na slici 1 dat je primer forme matrice sa svim elementima koji se unose i vrši procena rizika.

Glavna kategorija	Pod kategorija	Imovina	Kratak opis	Pretnja	Ranjivost	Primarna bezbednost	Verovatnoća	Uticaj	Rizik	Mogućnost ne otkrivanja	RPN	Kontrola	Tretman rizika

Slika 1: *Procena rizika*

11. IZJAVA O PRIMENJIVOSTI

Izjava daje popis svih kontrola kako je navedeno u Dodatku “A” SRPS ISO/IEC 27001. Kontrole će biti primenljive ili neprimenljive u organizaciji ili prenete na treća lica, koja učestvuju u realizaciji poslova “FMS”. Primenljive kontrole će imati sažet opis primenjene kontrole i tamo gde to može biti primenljivo, povezanost sa detaljima primene kontrole u politici bezbednosti. Neprimenljive kontrole će imati objašnjenje za njihovu neprimenljivost, dokumentovanu u Izjavi o primenljivosti i biće preispitivane od strane menadžera bezbednosti informacija.

Na slici 2, nalazi se forma matrice izjave o primenjivosti u koju se na osnovu zahteva standarda ISO/IEC 27001 primenjuju kontrole. Legenda (za izabrane kontrole i razloge za izbor kontrola) ZZ: Zakonski zahtevi, UO: Ugovorene obaveze, PZ/NP: poslovni zahtevi/usvojena najbolja praksa, RVR: rezultati vrednovanja rizika, AP: analiza pristupa

SRPS ISO/IEC 27001:2014 Kontrole				**Važeće kontrole**	**Primedbe**	**Izabrane kontrole**					**Primedbe**
						zz	**po**	**pz**	**pvr**	**ap**	
Tačka	**Podtačka**	**Oznaka kontrole**	**Cilj kontrole**								

Slika 2: *Izjava o primenjivosti*

12. ZAKLJUČCI

Kompanija„FMS“ je mlada kompanija koja teži da se što više usavrši, kako na polju primenete hnologije, tako i na polju primene ISOstandarda. Posebno ISO 9001 i ISO/IEC 27001. Kako bi oba standard u potpusnoti bili primenjeni u kompaniji, neophodna je detaljna analiza rizika, njihova procena i mogućnosti prihvatanja rizika kako kompanija ne bi pretrpela veliku štetu. Kroz analizu rizika predlažemo i akcije za smanjenje kako bi rizik bio u nominalnim granicama.

Veoma je bitna obuka zaposlenih i razvijanje njihove svesti o zaštiti informacija, kako bi uspešnije sprovodili bezbednosne politike i ukazivali na potencijalne probleme.

Pretnje po bezbednost informacija organizacije dolaze i spolja i iznutra. „Napade“ na informacije možemo podeliti u dve grupe: zlonamerne (osmišljene akcije spolja i iznutra, fokusirane na informacije kompanije) i slučajne (neplanirani upadi u sistem spolja i neadekvatno rukovanje informacijama od strane zaposlenih). Ponekadsu brzina i učestalost napada je toliki, da nije moguće u svakom trenutku efektivno i efikasno odgovoriti na njih. Evidentno je da samo planski i sistemski pristup bezbednosti informacija, zasnovan na po principu prevencije i/ili otklanjanja pretnji po bezbednost informacija, može pružiti organizaciji efikasnu zaštitu. Upravljanjem rizicima, upravljamo i bezbednošću informacija. Prvi korak ka tom cilju je razumevanje navedenih rizika i njihovog tretiranja.

13. LITERATURA

[1]SRPS ISO/IEC 27001:2014, Institut za standardizaciju Srbije, http://www.iss.rs, datum pristupa 1.09.2018.

[2] Definicjija Rizika, materijal sa predavanja Visoke poslovne škole Novi Sad, predmet-upravljanje rizicima, link:*www.vps.ns.ac.rs/Materijal/mat1318*, datum pristupa 18.02.2018.

[3] SRPS ISO 9001:2015, Sistem menadžmenta kvalitetom – zahtevi, Institut za standardizaciju Srbije

[4] Uvod u upravljanje rizicima, priručnik za obuku , Standcert doo 2014, autor Dr Nenad Injac.

Kratka biografija:

Siniša Maletić: Rodjen u Rumi 1986 godine. Osnovnu i srednju školu završava u rodnom gradu. Nakon završetka visoke poslovne škole, odsek za informatiku, upisuje Fakuktet tehničkih nauka u Novom Sadu 2012 godine. 2016 Upisuje master studije na katedri za kvalitet.