

IVAN BAŠIĆ, dr.sc.
DEAN VUKASOVIĆ, dipl.inž
GBS-IT d.o.o., Zagreb
ivan.basic@gbs-it.com
dean.vukasovic@gbs-it.com

IMPLEMENTACIJA ISMS-A - ISKUSTVO IZ PRVE RUKE

Sažetak

U radu će biti opisana iskustvo implementacije ISMS-a na cijelo poslovanje organizacije. Sagledati će se organizacija nakon implementacije sustava -što se promijenilo, koliko ljudi zna objasniti novom djelatniku kako ISMS utječe na svakodnevni rad, promjene u upravljanju projektima itd. Razmatrati će se kako se odražavaju na kupca i samu organizaciju temeljne postavke: dostupnost, cjelovitost i povjerljivost. Biti će opisan utjecaj na interne procesa: dokumentacijom praćeno stanje “na terenu”, sustav koji živi te se mehanizmom interne kontrole mijenja i unaprjeđuje. Promijenjen je i način edukacije djelatnika – provedena je edukacija svih djelatnika vezana uz sigurnost informacija, te usklađeno usvajanje dodatnih znanja na postojeća tehnička znanja. U konačnici dobili smo organizaciju koja upravlja investicijama na osnovu analize rizika, koja valorizira vrijednosti vlastitog znanja, koja prepoznaje kao svoju konkurentsku prednost svijest kupca da su njegove informacije cjelovite i dostupne te da je sačuvana njihova povjerljivost.

Ključne riječi: *implementacija ISMS-a, ISMS, sigurnost informacija*

1. UVOD:

Informacije organizaciji imaju veliku vrijednost, no mnoštvo prijetnji ugrožava tu vrijednost. Kako se najbolje zaštititi?

Tipična individualna rješenja se koriste kako bi se suprotstavilo specifičnim prijetnjama. Međutim prijetnji je svakim danom sve više. Da bi se organizacija othrvala, treba imati sistematičan pristup i sustav informacijske sigurnosti.

Ovakav sustav upravljanja sigurnošću informacija (*ISMS-Information Security Management System*) je propisan normama **ISO 27001** i **BS 7799-2**.

Implementacijom ovog sustava se integriraju pojedinačna rješenja gradeći ih na istom konceptu.

GBS-IT je implementirao ovu normu prvi u hrvatskoj za cijelo svoje poslovanje.

2. NORME ISO 27001 I ISO 17799 (BS 7799 PART I I PART II)

ISO 27001 i ISO 17799 su skup normi koje potiču od nekadašnjeg britanskog standarda BS 7799 (part I i part II).

ISO 17799 standard (ili BS 7799-1) je skup preporuka i smjernica izrađen prema najboljoj praksi za upravljanje sigurnošću informacija. On daje preporuke za postavljanje početnih uvjeta, uspostavu i održavanje sigurnosti. ISO 17799 nudi iscrpan skup kontrola

baziran na najboljoj praksi u informacijskoj sigurnosti. Taj skup kontrola je baza za razvoj standarda sigurnosti u organizaciji i uspostavu učinkovitog upravljanja sigurnošću.

Područja koja pokriva norma su:

- § Analiza i upravljanje rizikom
- § Politika sigurnosti
- § Organizacija sigurnosti
- § Klasifikacija i upravljanje imovinom
- § Sigurnost u upravljanju ljudskim resursima
- § Fizička sigurnost i sigurnost okoline
- § Upravljanje komunikacijama i operativom
- § Kontrola pristupa
- § Razvoj i održavanje
- § Upravljanje incidentima
- § Upravljanje kontinuitetom poslovanja
- § Sukladnost

ISO 27001 (ili BS 7799-2) je orijentiran na sustav upravljanja. Ova norma pokriva 4 glavna područja:

- Sustav upravljanja sigurnošću informacija (ISMS)
- Odgovornost posloводства
- Ocjena posloводства
- Unaprjeđenje ISMS-a

Koncept koji ovaj set normi uvodi je definicija samog pojma sigurnosti informacija u ovisnosti od tri parametra: povjerljivost, dostupnost i cjelovitost informacija.

Sigurnost informacija :Očuvanje povjerljivosti, integriteta i dostupnosti informacije.

- **Povjerljivost**: Informacija je dostupna samo osobama kojima je i namijenjena
- **Cjelovitost**: Točnost i sadržajnost informacije mora biti zaštićena
- **Dostupnost** Autorizirani korisnici moraju moći pristupiti informaciji kada im je potrebna

3. PREDUVJETI ZA USPJEŠNU IMPLEMENTACIJU

Prije samog kretanja u projekt implementacije ISMS-a treba se utvrditi stanje u organizaciji:

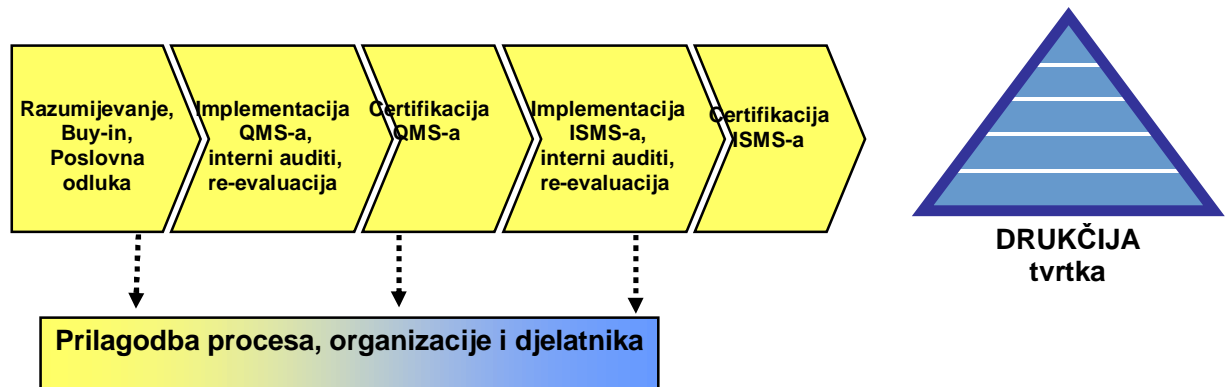
- § Da li vaši osnovni procesi kvalitetno funkcioniraju, te da li je implementiran sustav upravljanja kvalitetom?
- § Da li je sigurnost informacija relevantna za vaše poslovanje u dovoljnoj mjeri (*integrity, availability, confidentiality*), dokumentirano/iskustveno?
- § Da li management sudjeluje u projektu (*ROI*)?
- § Da li ste spremni učiti?
- § Da li imate formiran implementacijski tim koji može provesti promjene, određen budžet?
- § Da li imate dovoljno pametnih ljudi koji ne rade ništa, pa možete *sami* provesti implementaciju?

Nakon što su utvrđeni rizici neispunjenja ovih faktora kreće se na implementaciju

4. FAZE IMPLEMENTACIJE

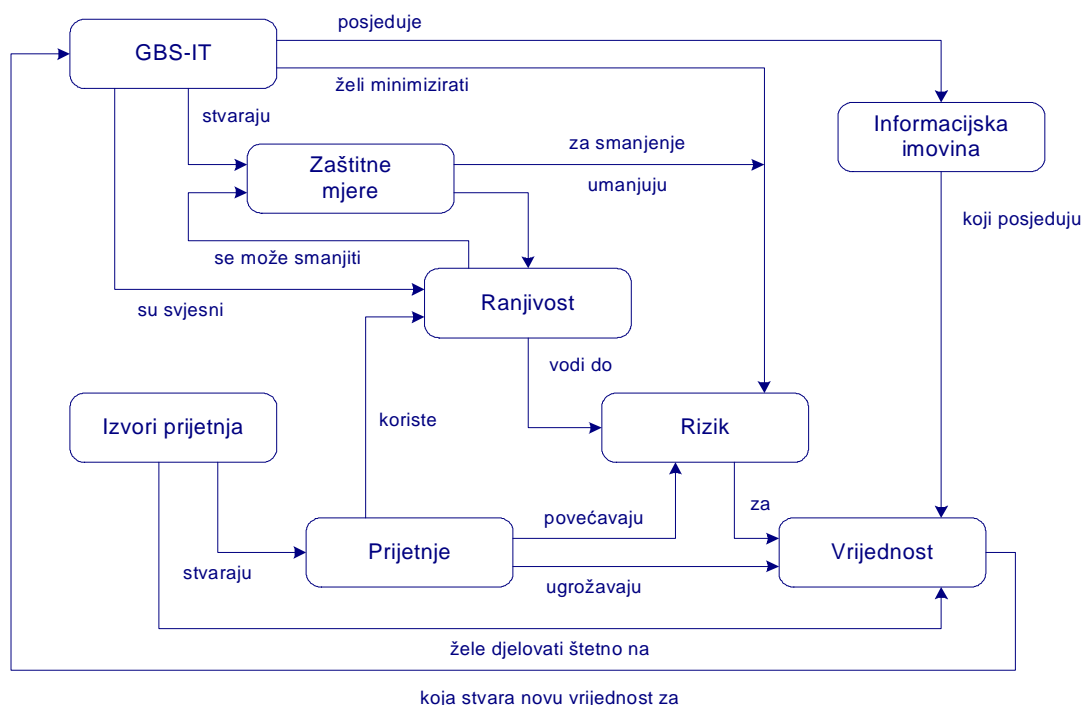
Kako bi se uspješno provela implementacija ISO 27001 potrebno je dobro poznavati svoje poslovanje i imati uređen sustav korektivnih i preventivnih radnji te upravljanja dokumentacijom. Kako bi to uspio GBS-IT je prvo implementirao sustav upravljanja kvalitetom po normi ISO 9001.

Slika1. Faze implementacije ISMS-a



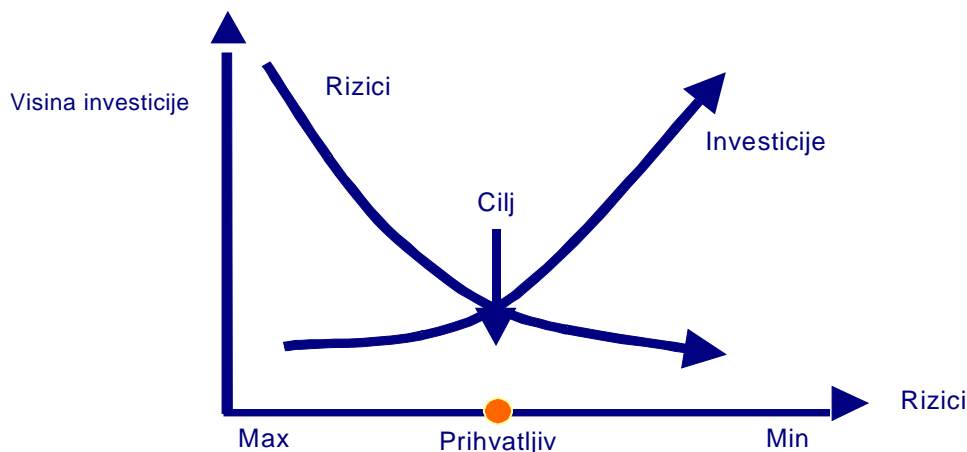
Prepoznavši vlastite procese krenulo se na analizu rizika i klasifikaciju imovine zahtijevane normom. Trebalo je prepoznati informacijsku imovinu, prijetnje na tu imovinu, izvore prijetnji te sukladno izračunatim rizicima definirati zaštitne mjere. Na slici 2 je prikazan međuodnos faktora potrebnih za kvalitetnu analizu rizika.

Slika 2. Osnovni model rizika



Kako bi se odredio prag na kojem se primjenjuju zaštitne mjere potrebno je napraviti *cost-benefit* analizu isplativosti primjene određene zaštitne mjere.

Slika 3. Utvrđivanje prihvatljivog rizika



Kada definiramo rizik u terminima vrijednosti za kompaniju – možemo definirati i cijenu nastupanja rizika u novčanim terminima. Usporedbom te vrijednosti i vrijednosti investicije u zaštitnu mjeru dolazimo do prihvatljive točke. Mora se imati na umu da investicija nije samo izračun uloga u hardware već i troškovi implementacije.

Primjena zaštitnih mjera je zadnji dio izgradnje ISMS sustava koji se svojim *Plan-Do-Check-Act* krugom nadopunjuje u krug postavljen implementacijom ISO 9001.

5. ORGANIZACIJSKE PROMJENE

Implementacija ISMS-a ima utjecaj na samu organizaciju. ISMS utječe na svakodnevni rad, promjene u upravljanju projektima itd. Odnos prema kupcu se promijenio jer je postojeći fokus na kupca dobio i posebne varijable - dostupnost usluge kupcu, cjelovitost informacijske imovine kako bi se osigurala kvalitetna usluga te povjerljivost. Promijenjen je i način edukacije djelatnika – provedena je edukacija svih djelatnika vezana uz sigurnost informacija, te usklađeno usvajanje dodatnih znanja na postojeća tehnička znanja.

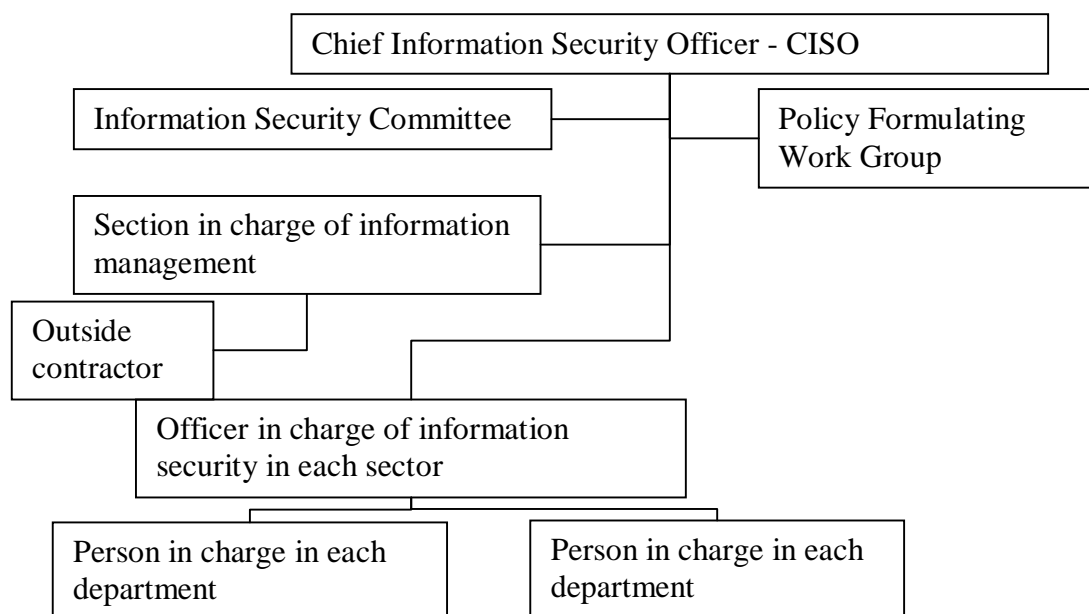
Međutim implementacija ISMS-a zahtjeva i neke formalne promjene. U samoj organizaciji moraju početi funkcionirati tijela koja će se baviti sigurnošću informacija.

Information Security Committee: odlučuje o postojećim sigurnosnim rizicima i njihovom tretmanu.

Chief Information Security Officer – CISO – uloga mu je slična ulozi QM za ISO 9001 samo za područje sigurnosti.

Policy Formulating Work Group – za svaku novu zaštitnu mjeru definira se skupina koja će kreirati primjenjivu politiku – ovo nije stalno tijelo – već se formira prema potrebi. U svakoj organizacijskoj jedinici mora postojati osoba zadužena za aspekte sigurnosti kako bi sustav zaživio.

Slika 4. Ključne uloge u ISMS-u



6. ZAKLJUČAK

Imperativi BS7799/ISO 27001

- § Ovo je standard menadžmenta
- § ISMS je samo dio internog sustava kontrola
- § Odabir internih kontrola je prvenstveno definiran analizom rizika
- § Sustav je baziran na stalnom unaprjeđenju – *Plan-Do-Check-Act* (Demingov krug)
- § Putovanje - a ne odredište – važan korolar PDCA kruga je da postoje korektivne/preventivne radnje i unaprjeđenja koja su identificirana, a nisu provedena.

U konačnici smo dobili organizaciju koja upravlja investicijama na osnovu analize rizika, koja valorizira vrijednosti vlastitog znanja, koja prepoznaje kao svoju konkurentsku prednost svijest kupca da su njegove informacije cjelovite i dostupne te da je sačuvana njihova povjerljivost.

LITERATURA

- [1] ISO 27001: Information Security Management - Specification With Guidance for Use
- [2] BS 7799-2:2000: Information Security Management Systems - Specification With Guidance for Use
- [3] ITIL Security Management, OGC - Office of Government Commerce
- [4] CISM Review Manual 2006, ISACA

IMPLEMENTATION OF ISMS – FIRST-HAND EXPERIENCE

Summary

In this paper will be described experience in implementation ISMS (Information Security Management Systems) on complete operations. Organization after implementation of ISMS will be observed: what is changed, how many people can explain ISMS in every day work to a new employee, changes in project management etc. Reflection of fundamental requirements: availability, integrity and confidentiality on customer will be described. Implementation of ISMS has influence on internal processes, it is a live system changing and improving thought internal controls. Education of employees is changed, too. Every employee must finish the course in information security based on his technical experience. Final result is organization which manages its investments trough risk analysis; valorise value of its own knowledge. This organization recognize customer knowledge that his information have integrity, are available, and confidential, as competitive advantage

Key words: *ISMS implementation, ISMS, information security*