ASOCIJACIJA ZA KVALITET I STANDARDIZACIJU SRBIJE

FESTIVAL KVALITETA 2007.
34. Nacionalna konferencija o kvalitetu
Kragujevac, 08. - 11. maj 2007.

ISO 27001 I ISO 20000 OSNOV ZA ORGANIZACIONE DOBITI

ISO 27001 AND ISO 20000, BASIS FOR ORGANIZATIONAL PROFIT

Mr Aleksandar Vujović, Prof. dr Zdravko Krivokapić

Rezime: *Rad je nastao kao težnja istraživača u Centru za kvalitet-Mašinski fakultet u Podgorici da prošire djelokrug rada i istraživanja i da se priključe savremenim trendovima u oblasti standarda i njihove implementacije. Kao novi i u našoj zemlji još uvijek nedovoljno primjenjivani standardi ISO 27001 i ISO 20000, predstavljaju izazov za istraživače. Cilj ovog rada je da se ukaže na naznačajnije i svakako ne i jedine dobiti koje organizacije ostvaruju kroz implementaciju, održavanje i unapređenje dva navedena modela. Time se želi ukazati na značaj njihove primjene i svakako dati doprinos u pravcu popularizaciji standarda ISO 27001 i ISO 20000 i dati podstrek istraživačima da daju doprinos u ovim oblastima.*
Ključne reči: *ISO 27001, ISO 20000*

1. UVOD

Svjedoci smo da je krajem dvadesetog vijeka na svjetsku poslovnu scenu poseban »ožiljak« ostavio nagli razvoj informacione tehnologije čime je industrijalistički period razvijanja mašina i tehnologija zamijenjen sa periodom informacija i sistema. Već početkom trećeg milenijuma informacione tehnologije imaju toliku rasprostranjenost da se u velikom dijelu ekonomski razvijenog svijeta savremena informaciona rešenja koriste na svakom koraku. To je dovelo do otvaranja novog perioda i to »vijeka znanja«. Znanje proizilazi iz informacije na što ukazuje i definicija znanja kao obim informacija, opažanja ili razumijevanja koje posjeduje neka ličnost. Takođe je prihvatljiva definicija znanja sa stanovišta obrade znanja i to je da je znanje formalizovana informacija na koju se poziva ili koja se koristi u procesu zaključivanja. Ili pak najprikladnija definicija znanja je »znanje su podaci plus »znanje« o značenju tih podataka, odnosno znanje je uvijek povezano sa procedurama korišćenja tog znanja. Sa druge strane u literaturi je najčešće isticana i sa stanovišta sistema najprihvatljivija i definicija informacije u kojoj se navodi da je informacija mjera organizacije isto kao što je entropija mjera dezorganizacije. Imajući ovo u vidu može se jasno istaći značaj bezbjednosti informacija jer je to bezbjednost odnosno čuvanje znanja kao suštinskog resursa za današnje poslovne sisteme. U uslovima visoke konkurentnosti, pravovremena i prava informacija je novac, opstanak i prestiž na tržištu. U pravcu obezbjeđenja odnosno ostvarenja bezbjednosti organizacionog znanja ili informacija usvojen je standard ISO 27001 u kojem su specificirani zahtjevi koje organizacija treba da poštuje da bi ostvarila sistem za zaštitu informacija.

U skladu sa navedenim rastućim trendovima u oblasti informacija i znanja, ostvaruje se i značajan razvoj organizacija koje se bave uslugama u oblasti informacionih tehnologija (IT). Da bi ove organizacije poslovale efktivno i efikasno i da bi ostvarivale proizvode u skladu sa zahtjevima korisnika ostvarujući njihovo zadovoljstvo, definisan je standard ISO 20000 kao model za menadžment u oblasti IT usluga. I jedan i drugi model predstavljaju osnovu za unapređenje poslovanja i kroz sledeće segmente rada će se pokušati da se ukaže na najznačajnije dobiti koje organizacije mogu da postignu kroz implementaciju, održavanje i unapređenje sistema koji se baziraju na ovim modelima.

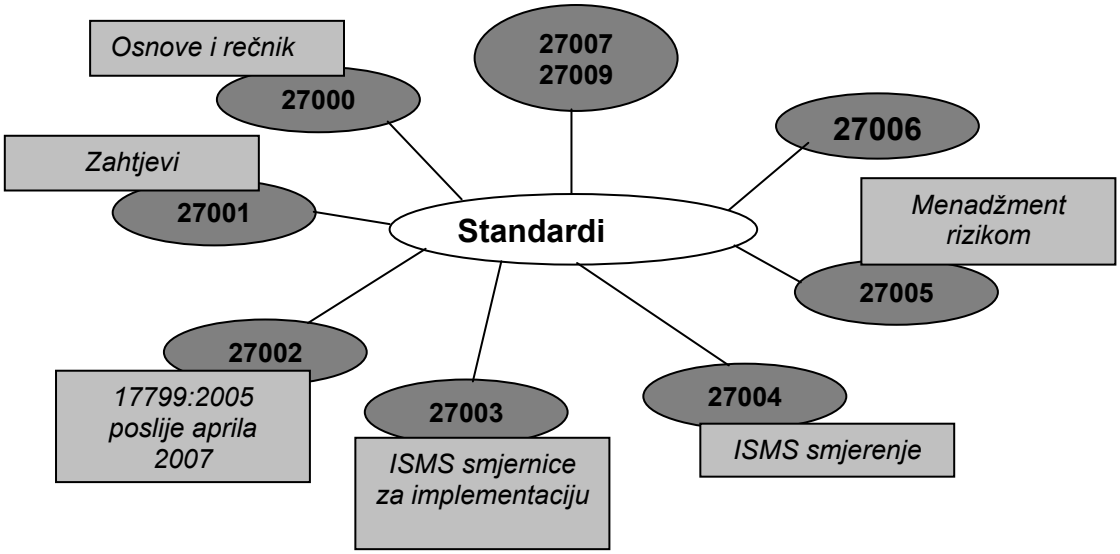
2. ISO 27001- SISTEMI UPRAVLJANJA BEZBJEDNOŠĆU INFORMACIJA-ZAHTJEVI

Početkom devedesetih godina Britanski institut za standardizaciju (BSI) je postavio osnove za razvoj standarda za zaštitu informacija podstaknut izrazitim zahtjevima organizacija u tom pravcu. 1995 godine, se usvaja prvi tekst standarda za sistem upravljanja bezbjednošću informacija BS 7799 koji je prvu reviziju doživio 1998. godine. Kasnije sa izrazitim razvojem Internet-a i brzih računarskih mreža objavljuje se i drugi dio standarda BS 7799. Ovi standardi se prihvataju od

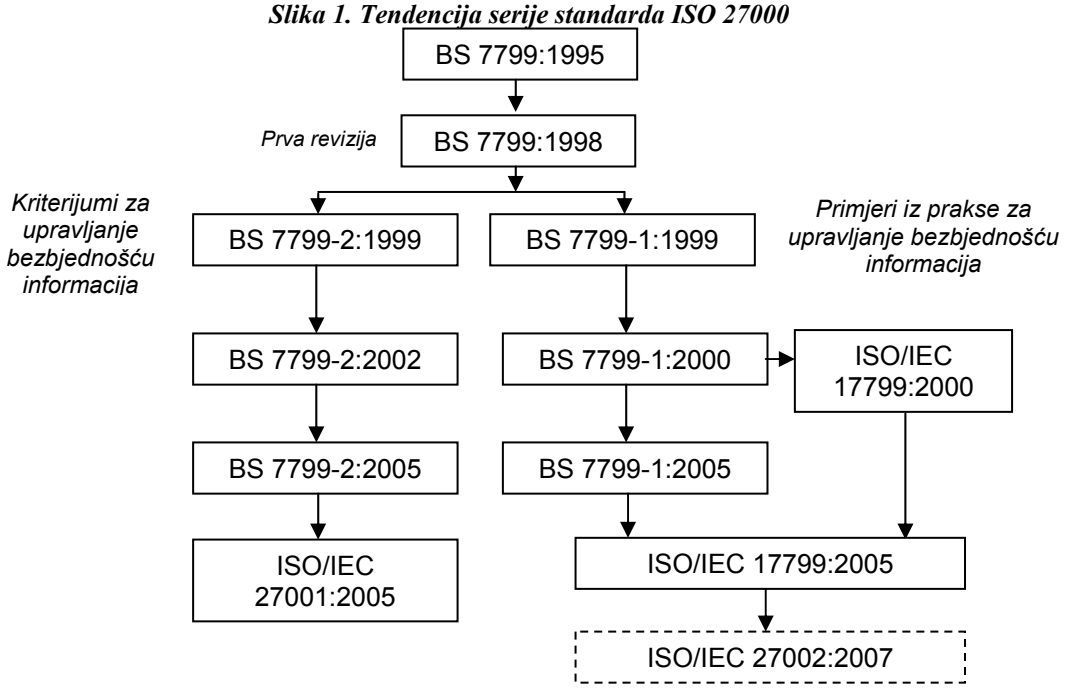
1) Mr Aleksandar Vujović, Mašinski fakultet u Podgorici-Centar za kvalitet
2) Prof. dr Zdravko Krivokapić, Mašinski fakultet u Podgorici-Centar za kvalitet

strane međunarodne organizacije za standardizaciju ISO i oni konačno u junu 2005. godine objavljuju drugu verziju standarda FISO 17799 pod nazivom Informacione tehnologije-bezbjednost tehnike-Načela upravljanja bezbjednošću informacija, a u oktobru 2005. godine objavljuju standard ISO 27001 pod nazivom Informacione tehnologije-Sistemi upravljanja bezbjednošću informacija-Zahtjevi. Dakle standard ISO 27001 je kompatibilan sa standardom ISO 9001 i po ovom modelu se poslije ispunjenja u njemu definisanih zahtjeva može sprovesti sertifikacija sistema od strane ovlašćenih sertifikacionih tijela. U dogledno vrjeme se očekuje da standard ISO 17799 preraste u standard ISO 27002, što će dovesti do ujednačavanja strukture serije standarda koji se odnose na bezbjednost informacija sa sturkturom ISO 9000. ISO 27001 će ostati standard koji definiše zahtjeve za ISMS (Sistem za upravljanje bezbjednošću informacija) i čini osnovu za sertifikaciju sistema, ISO 27002 (usvajanje se očekuje nakon aprila 2007) će preuzeti ulogu usmjeravanja korisnika pri primjeni ISO 27001 kao što je to slučaj sa serijom ISO 9000. Tendencija serije standarda ISO 27000 je prikazana na slici 1.

Na slici 2 je prikazana geneza standarda za Sisteme upravljanja bezbjednošću informacija ISMS (Information Security Management Systems).



Slika 1. Tendencija serije standarda ISO 27000



Slika 2. Geneza standarda ISMS

Standard ISO 27001 je koncipiran u pet poglavlja i to:

1. Poglavlje 4: Sistem za upravljanje bezbjednošću informacija (ISMS)
2. Poglavlje 5: Odgovornost rukovodstva
3. Poglavlje 6: Interna provjera ISMS
4. Poglavlje 7: Preispitivanje ISMS od strane rukovodstva i
5. Poglavlje 8: Unapređenje ISMS.

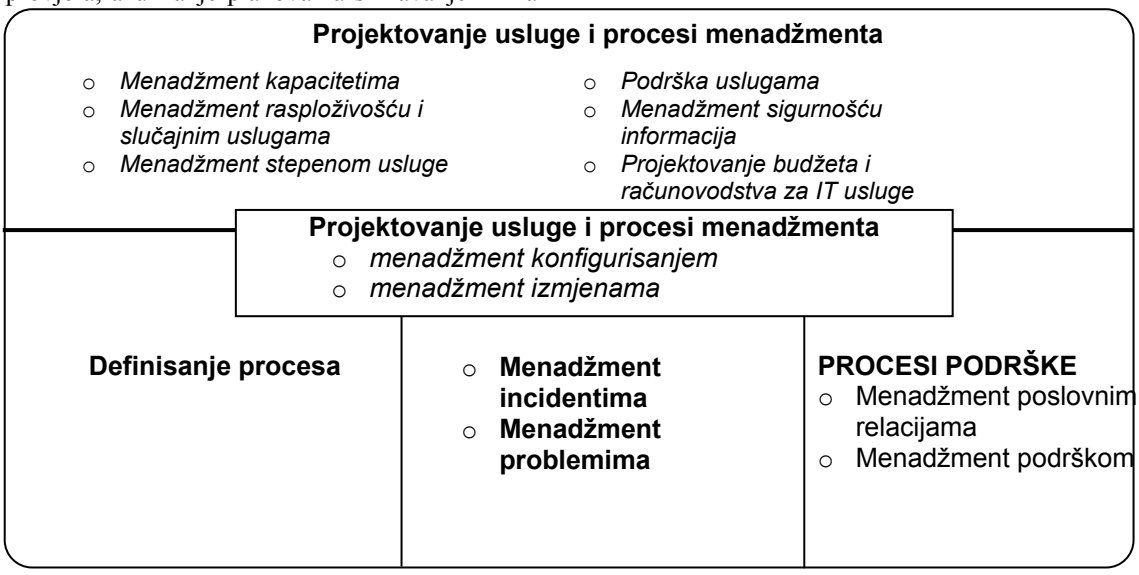
Osnovni pojmovi vezani za sistem bezbjednosti informacija dati su u tački 3 standarda. Dakle jasno je uočljiva kompatibilnost sa standardom ISO 9001. U tom pravcu u ovom standardu je jasno istaknut i model standarda kroz P-D-C-A ciklus stalnog unapređenja

Na osnovu zahtjeva korisnika I kroz uspostavljanje politike ISMS organizacija ulazi u fazu uspostavljanja odnosno planiranja sistema za upravljanje bezbjednošću informacija. U ovoj fazi se sprovode i aktivnosti na definisanju kriterijuma za ocjenu rizika, definiše se prilaz i metodologija za ocjenu rizika, definišu nivoi prihvatljivosti rizika i dr. Sledeća faza je sprovođenje planiranog odnosno 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. Treća faza je preispitivanja ISMS-a na osnovu definisanih procedura za preispitivanje, mjerenje efektivnosti upravljačkih mehanizama, sprovođenja internih provjera, ažuriranje planova za snižavanje rizika i dr. Kao završna faza u ovom kontinualnom ciklusu poboljšavanja egzistira faza održavanja i poboljšavanja ISMS-a koja se sprovodi kroz uvođenje poboljšavanja, preuzimanje korektivnih i definisanju preventivnih mjera, provjera dali su sprovedena poboljšavanja održiva i dr.

3. ISO 20000-MENADŽMENT IT USLUGAMA

Standard ISO 20000 je značajan standard za organizacije koje se bave uslugama Informacionih tehnologija i omogućava saradnju sa sličnim organizacijama širom svijeta koje posluju po ovom modelu. Ovim standardom, organizacije demonstriraju svojim korisnicima i ostalim zainteresovanim stranama da posluju sa posovnim procesima na bazi principa sigurnosti i cjelovitosti i da je poslovna politika usmjerena na stalna poboljšavanja u sistemu menadžmenta IT uslugama. Sertifikacija sistema koji ispunjava zahtjeve standarda obezbjeđuje konkurentnu prednost nad organizacijama koje nijesu prihvatile ovaj standard.

Ovim standardom se proklamuje prihvatanje jednog integralnog procesnog pristupa za potrebe efektivne isporuke usluga u oblasti informacione tehnologije i sadrži uputstva za kvalitet u menadžmentu IT uslugama (ITSM-Information Technology Management Systems) slika 3.



Slika 3. Procesi menadžmenta uslugama u ISO 20000

Standardom ISO 20000 koji kako je i ranije naglašeno zamjenjuje standard BS 15000 obezbjeđuje standardizovan put kojim se verifikuje da je jedna organizacija uspješno usvojila Menadžment IT uslugama i najbolju praksu iz ITI biblioteke koja je ustvari bila standard u ovoj oblasti skoro 20 godina. Ustvari, 2000-te godine je na bazi ITI biblioteke izašao prvi standard BS 15000. Ovaj standard se sastoji od dva dijela po strukturi slična seriji ISO 9000. U prvom dijelu su specificirani zahtjeva za sigurnost menadžmenta isporuke IT usluge, a u drugom dijelu se nalaze

primjeri iz najbolje prakse za menadžment uslugom. Pored BS 15000 standarda, ITI biblioteke i model COBIT je odigrao značajnu ulogu u formiranju ISO 20000. Britanski institut za upravljanje informacionim tehnologijama je izradio sistem za fokusiran na IT usluge koji se zove kontrolni ciljevi za informacione i srodne tehnologije ili skraćeno COBIT. Ovim modelom se obezbjeđuju specifične upravljačke smjernice za pomoć organizacijama u implementaciji mjera za upravljanje IT uslugama. COBIT posjeduje niz od 34 upravljačka cilja visokog nivoa od kojih se 13 oslanjaju na ITI biblioteku.

Konačno u maju 2005 godine ISO i IEC glasaju da se BS 15000 predstavi kao osnova ISO 20000 standarda. Osnovni ciljevi ISO 20000 su:

- smanjenje izlaganju rizicima,
- ispunjavanje ugovorenih zahtjeva i
- demonstriranje kvaliteta usluga.

Procesi sertifikacije po modelu ISO 20000 su počeli 2006 godine i prve organizacije koje su lako prihvatile ovaj model su bile one koje su sertifikovane po BS 15000 standardu. Aktuelna verzija standarda je bazirana na britanskom standardu BS 15000 i veoma blisko vezan sa Bibliotekom infrastukture informacionih tehnologija (ITIL). Ova biblioteka sadrži set od sedam povezanih knjiga od kojih svaka definiše smjernice odnosno uputstva za specifične oblasti, bazirana na najboljoj praksi. Ove smjernice se mogu primijeniti na sve organizacije i mogu ispuniti sve neophodne specifične zahtjeve. Ova biblioteka je vlasništvo Vladinog odjela za trgovinu Velike Britanije.

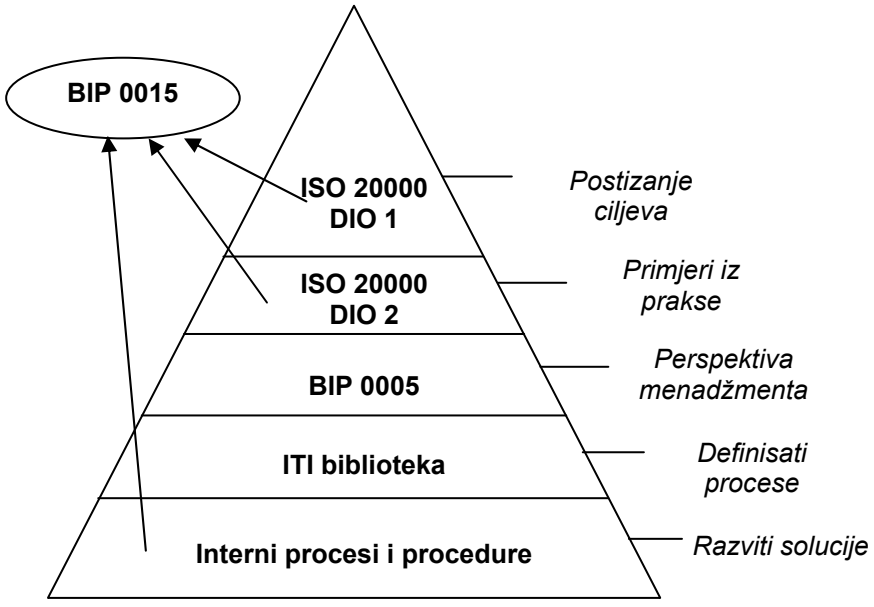
ISO 20000 sadrži:

- DIO 1 (ISO/IEC 20000-1:2005) - koji uključuje skup minimalnih zahtjeva i njime se promoviše usvajanje integralnog procesnog pristupa za uspješnu isporuku usluga i menadžment uslugama u cilju postizanja poslovnih i korisnikovih zahtjeva. Područje ovog standarda uključuje:
  - zahtjeve za sistem upravljanja,
  - planiranje i implementaciju menadžmenta uslugama,
  - planiranje i implementaciju novih ili izmijenjenih usluga,
  - procesi isporuke usluga,
  - procesi povezivanja,
  - procesi odlučivanja,
  - procesi kontrole i
  - procesi izdavanja usluge.

ISO 20000 sadrži:

- DIO 1 (ISO/IEC 20000-1:2005) - koji uključuje skup minimalnih zahtjeva i njime se promoviše usvajanje integralnog procesnog pristupa za uspješnu isporuku usluga i menadžment uslugama u cilju postizanja poslovnih i korisnikovih zahtjeva. Područje ovog standarda uključuje:
  - zahtjeve za sistem upravljanja,
  - planiranje i implementaciju menadžmenta uslugama,
  - planiranje i implementaciju novih ili izmijenjenih usluga,
  - procesi isporuke usluga,
  - procesi povezivanja,
  - procesi odlučivanja,
  - procesi kontrole i
  - procesi izdavanja usluge.

Na slici 4 prikazana je veza između ISO 20000 i ITI biblioteke i piramidalni tok implementacije modela ISO 20000.



Slika 4. Veza između ISO 20000 i ITI biblioteke

Primjenom standarda ISO 20000 obezbjeđuje put za uspješno sprovođenje kontinualnih unapređenja i načine za mjerenje poboljšavanja na svakom novom poboljšanom nivou.

Danas je posebno značajna i svrsishodna primjena savremenih hardverskih i softverskih rešenja u cilju automatizacije sistema baziranog na ISO 20000 standardu. Automatizacija u toj oblasti donosi značajne prednosti i to:

- pomoć u integraciji procesa,
- doslednost i ponovljivost procesa,
- omogućava bržu implementaciju ITI biblioteke i bržu sertifikaciju ISO 20000,
- pomaže u smanjenju troškova,
- pomaže u provjeravanju ostvarenih unapređenja i drugo.

Za potrebe uspostavljanja ISO 20000 modela neophodno je postaviti razne solucije internih procesa i procedura, zatim na bazi primjera iz prakse iz ITI biblioteke, definisati procese, korišćenjem Vodiča za menadžere za menadžment uslugama BIP 0005 uspostaviti pregled odnosno perspektivu ili gledište menadžmenta i sprovesti primjere iz prakse iz ISO 20000-2 i na kraju primijeniti model ISO 20000-1. Ove aktivnosti su praćene stalnim procesom samoocjenjivanja primjenom radne knjige za samoocjenjivanje u oblasti menadžmenta informacionim tehnologijama BIP 0015.

4. ORGANIZACIONE DOBITI OD IMPLEMENTACIJE ISO 27001 I ISO 20000

Kroz prethodne tačke ovoga rada mogu se naslutiti određeni doprinosi koje modeli ISO 27001 i ISO 20000 ostvaruju u smislu organizacionig performansi. Neosporno je da ova dva modela predstavljaju najbolj praksu u oblasti zaštite informacija i menadžmenta u oblasti IT usluga koja je pretočena u zahtjeve standarda. Implementacijom ISO 27001 standarda i sertifikacijom takvog sistema, organizacije ostvaruju brojne dobiti od kojih su neke:

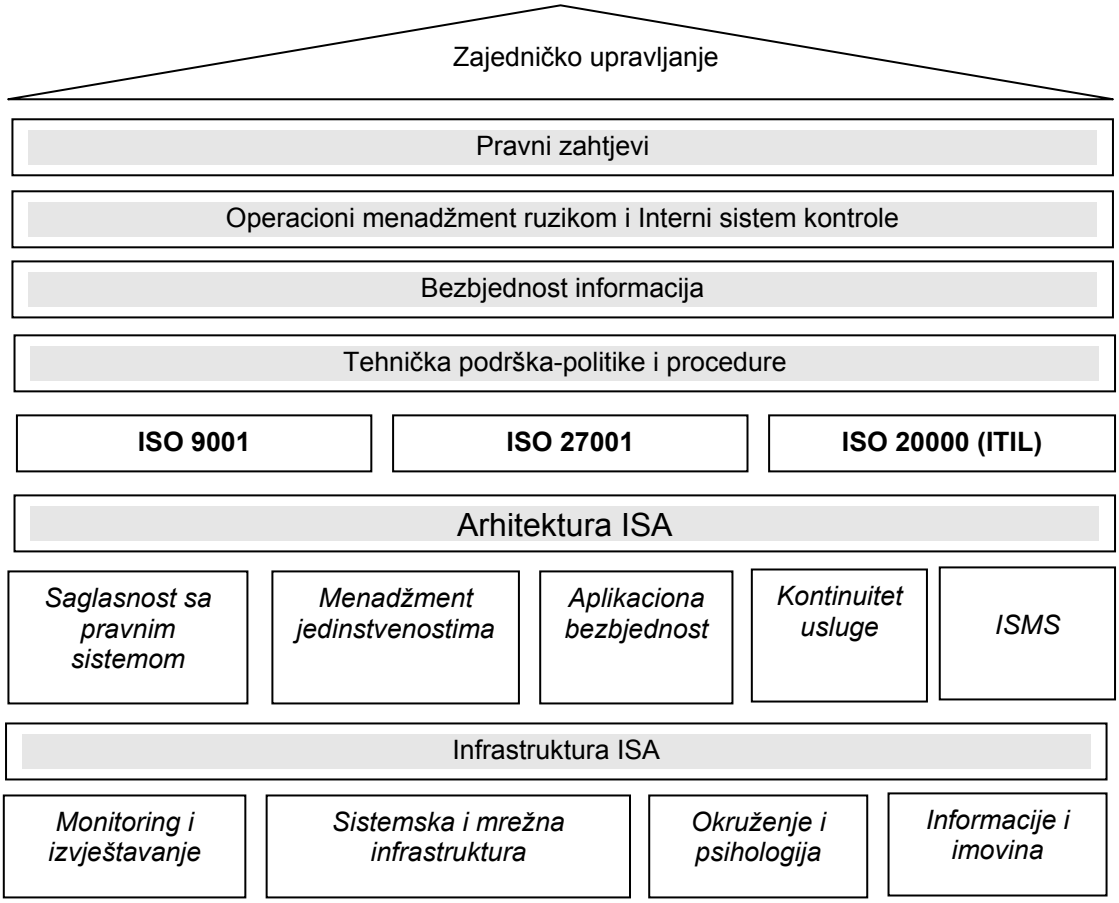
- kod potencijalnih ili postojećih korisnika se stvara povjerenje u informacioni sistem u organizaciji čime se sa korisnicima ostvaruju povjerljivije i čvršće relacije,
- obezbijeđuje se da organizacija ima potpuno komplementaran sistem sa pravnom regulativom koja je vezana za informacione tokove jer se radi o standardu koji ima jasnu fleksibilnost u tom pravcu,
- obezbjeđuje se sistem koji je usmjeren na jasna kontinualna poboljšavanja procesa kojima se obezbjeđuje informaciona sigurnost,
- ovim sistemom se ostvaruje transparentnost u pružanju usluga i menadžment na visokom nivou,
- obezbjeđuje se i sistem koji je posebno orijentisan na upravljanje rizikom i kroz upravljačke aktivnosti, smanjenje rizika na dozvoljenu i minimalnu mjeru,
- obezbjeđuje se naprednije razumijevanje informacionih tokova u organizaciji čime se ostvaruje značajna dobit i u dijelu razmijevanja i poboljšavanja poslovnih procesa,
- ostvaruje se mehanizam za jasno vidljive i opipljive dokaze o smanjenju troškova kroz bolji menadžment rizikom i smanjenje značaja uzročnika grešaka u organizaciji,
- ostvaruje se bolja analiza troškovi/dobiti,
- ostvaruje se lakši proces monitoringa kroz smanjenje radnih napora i primjenu recimo sistema samo provjere,
- moguće je povećati preventivno dejstvo kroz na primjer smanjenje »uskih grla« u mreži ili kroz analizu zaštićenih i sačuvanih ranijih podataka o procesima,
- smanjenje incidenata i bolje razumijevanje uzročnika,
- razvija se svijest zaposlenih u smislu značaja zaštite informacija,
- obezbjeđuje se jasan protok i raspoloživost informacija i dr.

Implementacijom standarda ISO 20000 organizacije stiču između ostalih sledeće dobiti:

- ostvaruje se sistem koji je apsolutno orijentisan na kontinualna poboljšavanja,
- ostvaruje se povjerenje kod korisnika da organizacija posluje u skladu sa principima apsolutne cjelovitosti i sigurnosti,
- ovim standardom se ostvaruje konkurentska prednost u odnosu na organizacije koje nemaju ovaj model u oblasti IT usluga,
- sistemom se obezbjeđuje isrvana, siguran i efektivan dokumentacioni tok što ostvaruje povjerenje kod korisnika i stvara preduslove za efektivno i efikasno korišćenje informacija koje sa sobom nose dokumenta,
- standardom se obezbjeđuje i primjena najbolje svjetske prakse iz oblasti IT usluga,
- obezbjeđuje sistem koji je fokusiran na kvalitet usluge nasuprot sistemu koji je fokusiran na kvalitet organizacijione strukture,
- obezbjeđuje da je sistem menadžmenta u oblasti IT usluga uravnotežen sa poslovnim potrebama organizacije,
- obezbjeđuje sistem pouzdanosti i raspoloživosti,
- obezbjeđuje sistem kojim se definiše nivo kvalitetne usluge i mogućnost da se jasno može mjeriti nivo postignutog kvaliteta,

- obezbjeđuje povećanje produktivnosti i omogućava najbolje iskorišćenje i upotrebu vještina,
- omogućava da organizacija prihvati odnosno da se prilagodi promjenama,
- zaposleni se upravljaju sa najboljom praksom u IT oblasti i dr.

Ova dva standarda zajedno sa modelom ISO 9001 obezbjeđuju jedan model za povjerenje u sigurnost informacija ili ISA (Information Security Assurance) model (slika 5).



Slika 5. Zajedničko djelovanje standarda ISO 9001, ISO 27001 i ISO 20000

Kroz ISA model se može sagledati mogućnost za zajedničko djelovanje standarda ISO 9001, ISO 27001 i ISO 20000 u cilju ostvarivanja sistema koji obezbjeđuje povjerenje u sigurnost informacija i efikasno upravljanje u oblasti IT tehnologija.

5. ZAKLJUČAK

Savremeni trendovi koji se ogledaju u globalizaciji tržišta i uniformnosti odnosno težnji za standardizacijom aktivnosti u oblasti sistema menadžmenta, nameće potrebu i obavezu da se i u našim uslovima i okruženjima sprovedu koraci u pravcu istraživanja, implementacije, održavanja i unapređenja sistema menadžmenta. Ovaj rad je nastao sa ciljem da popularište nedovoljno primjenjivane i oblasti koje su u povoju tj. oblasti menadžmenta u oblasti IT usluga i bezbjednosti informacija. U pravcu ostvarivanja efektivnih i efikasnih sistema za menadžment u oblastima IT usluga neophodno je koristiti model ISO 20000 i zahtjeve koje su u njemu specificirani. Time se ostvaruje konkurentska prednost u odnosu na organizacije koje ne primjenjuju ove norme. Pored ovih prednosti u radu je ukazano na mnoge druge koje organizacije izdižu na veće nivoe. U vremenu izrazitog rasta količine informacija i znanja u organizacijama i u njihovoj komunikaciji sa korisnicima, za potrebe bezbjednosti informacija i potrebe sticanja korisničkog povjerenja, neophodno je koristiti zahtjeve modela ISO 27001. Time se stvara sistem koji je fokusiran na kontinualna poboljšavanja i smanjenje troškova i eliminisanje uzročnika grešaka u sistemu. Zajedničkim djelovanjem ISO 20000 i ISO 27001 uz podršku modela ISO 9001 ostvaruje se sistem za bezbjednost informacija sa punim povjerenjem i usaglašenošću sa pravnim normama okruženja.

LITERATURA

[1] Savezni zavod za standardizaciju, »JUS ISO 9001:2001«, Savezni zavod za standardizaciju, izdanje 1, Beograd 2001.

[2] Krivokapić Z., Perović M., »Uvod u informatiku«, Unireks, Podgorica, 1995.

[3] Radlovački V., Beker I., »ISO 27001 I ISO 17799-Sistem upravljanja bezbjednošću informacija«, Istraživački tehnološki centar, Novi Sad, jun, 2006.

[4] JUS ISO/IEC 17799:2006, Savezni zavod za standardizaciju, nacrt standarda, Beograd 2005.

[5] ISO/IEC 27001:2005, Information technology-Security techniques-Information security management systems-Requirements, 15. 10. 2005, Geneva

[6] Hermann A., "Information Security Management for NSBs", Austrijski zavod za standardizaciju, Beč, 2006.

[7] Ćalić V., Petrović A., Ristanović D., „PC 98-Windows 98 i savremeni Internet", PC Press, Beograd, 1998.

[8] Petrović D., "Analiza standarda ISO 27001", seminarski rad na poslijediplomskim studijama na Ekonomskom fakultetu u Podgorici, Podgorica, 2007.

[9] Turbitt K., „ISO 20000: What's an Organization to Do?", BMC software, 2005

[10] Raup A., "ISO 20000&ITIL», Gartner Inc. G00t36652, January 5, 2006

[11] www.BSIstandards.co.uk

[12] Wright S., »Policy Monitor and its relationship with ISO 27001:2005«, Siemens Insight Consulting.

[13] BSI Management Systems, »Information security management based on ISO 27001"

[14] Pratt S., "ITIL and ISO/IEC 20000", www.afiniti.co.uk