SISTEM MENADŽMENTA BEZBEDNOŠĆU INFORMACIJA- ULOGA I ZNAČAJ SERTIFIKACIJE I AKREDITACIJE

mr Vida Živković, dr Dejan Krnjaić, Akreditaciono telo Srbije, Beograd

Abstrakt

Prethodnih godina sve više organizacija primenjuje sistem menadžmenta bezbednošću informacija (ISMS) kao deo svoje strategije upravljanja rizikom. Međunarodni standardi serije ISO/IEC 27000, primenjivi na organizacije svih vrsta i veličina (komercijalna preduzeća, državne agencije, neprofitne organizacije i sl.), pružaju pomoć u razumevanju principa, osnova i koncepta koji obezbeđuju zaštitu njihovih informacija.

U radu je dat pregled međunarodnih standarda serije ISO/IEC 27000, njihova svrha, oblast primene i značaj. Posebno su opisani postupak sertifikacije sistema menadžmenta bezbednošću informacija u skladu sa standardom ISO/IEC 27001:2005 i postupak akreditacije sertifikacionih tela, koji ove sisteme sertifikuju, u skladu sa standardima ISO/IEC 17021 i ISO/IEC 27006:2007. Opisani su glavni koraci pri sertifikovanju ISMS, opšta šema sertifikacije i uloge i veze različitih učesnika u njoj (sertifikovana organizacija, sertifikaciono telo, akreditaciono telo).

UVOD

Zaštita i bezbednost informacija za današnji svet biznisa je mnogo važniji nego ikada ranije. Danas, u velikoj meri, biznis zavisi od informacionih tehnologija, komunikacija putem mreža, kao i bežičnih i mobilnih komunikacija. Obavljanje poslova putem interneta i kompjutera, podugovaranje i korišćenje usluga treće strane postaju sve češći vidovi savremenog poslovanja. Lanac snabdevanja postaje sve složeniji i veći, a mogućnost kompjuterskih prevara dovodi do povećanja rizika u svim oblastima poslovanja.

Uspešan biznis i donošenje dobre odluke moguće je ostvariti samo uz pravovremeni pristup pravim i sigurnim informacijama koje su za to neophodne. Zaštita takvih informacija postaje preduslov za ostvarivanje prethodno pomenutog i zato joj treba prići sistemski. Međunarodni standardi serije ISO/IEC 27000, koji se odnose na informacione tehnologije, tehnike zaštite i sistem menadžmenta bezbednošću informacije, razvijeni su i doneti sa namerom da pomognu sistemski pristup u obezbeđenju ovog preduslova.

Da bi se steklo poverenje u tačnost i pouzdanost potrebnih informacija potrebno je imati poverenje u sistem menadžmenta njihovom bezbednošću.

Pouzdanost i poverenje u sistem menadžmenta bezbednošću informacija postiže se njegovom sertifikacijom od nezavisne i nepristrasne treće strane, odnosno sertifikacionog tela, kompetentnog za obavljanje tog posla i koje je svoju kompetentnost takođe dokazalo na adekvatan način. Najpodesniji način potvrđivanja kompetentnosti ovih sertifikacionih tela jeste akreditacija koju sprovodi nacionalno akreditaciono telo. Sertifikacijom se potvrđuje usaglašenost ISMS sa zahtevima definisanim u standardu ISO/IEC 27001:2005. Proces sertifikacije u odnosu na standard ISO/IEC 27001:2005 je u osnovi isti kao onaj koji se sprovodi pri sertifikaciji sistema menadžmenta kvalitetom prema ISO 9001 ili nekog drugog sistema menadžmenta. Standard ISO/IEC 17021 (SRPS ISO/IEC 17021) definiše kriterijume za sertifikaciona tela, koja sprovode proveru i sertifikaciju bilo kog sistema menadžmenta neke organizacije uključujući i sistem menadžmenta bezbednošću informacijama i on predstavlja osnov za akreditaciju. Ako pak sertifikaciono telo želi da se akredituje za sertifikaciju sistema menadžmenta bezbednošću informacijama u skladu sa ISO/IEC 27001:2005, tada je potrebno da zadovolji dodatne specifične zahteve u odnosu na zahteve ISO/IEC 17021 a koji su definisani u standardu ISO/IEC 27006:2007.

STANDARDI SERIJE ISO/IEC 27000

Svrha međunarodnih standarda serije ISO/IEC 27000 je da pruže pomoć organizacijama svih vrsta i veličina da razviju i primene sistem za upravljanje bezbednošću sopstvenih informacija i da se pripreme za nezavisno i nepristrasno ocenjivanje (sertifikaciju) tog sistema primenjenog na zaštitu informacija, kao što su, na primer finansijske informacije,

informacije o intelektualnoj svojini, podaci o osoblju ili informacije koje su im poverene od korisnika ili treće strane.
Ova serija obuhvata standarde koji: definišu zahteve za ISMS kao i zahteve za tela koja sertifikuju ISMS; obezbeđuju podršku, detaljna uputstva i instrukcije za celokupan proces planiraj-uradi-proveri-deluj (Plan-Do-Check-Act); daje specifična sektorska uputstva za ISMS i ocenjivanje usaglašenosti za ISMS.
Ovu seriju čine sledeći standardi koji su međusobno povezani:

- ISO/IEC 27000:2009, Information security management system - Overview and vocabulary koji daje opšti prikaz sistema menadžmenta bezbednošću informacija i definiše odgovarajuće termine,
- ISO/IEC 27001:2005, Information security management system – Requirements, naznačajniji standard ISMS serije koji definiše model za uspostavljanje, primenu, funkcionisanje, održavanje i poboljanje sistema menadžmenta bezbednošću informacija,
- ISO/IEC 27002: 2005 (prethodno BS 7799 -1 i ISO/IEC 17799), Code of practice for information security management, definiše pravila dobre prakse upravljanja bezbednošću informacija, odnosno obezbeđuje specifične savete i uputstva za kontrolisanje ISMS kao podršku ISO/IEC 27001,
- ISO/IEC 27003 (u izradi), Information security management system implementation guidance, obezbeđuje uputstvo za procesno orijentisani pristup i uspešnu primenu ISMS u skladu sa ISO/IEC 27001,
- ISO/IEC 27004 (u izradi), Information security management system – Measurement, koji daje uputsva i savete kako sprovesti merenja u cilju ocene efektivnosti ISMS,
- ISO/IEC 27005:2008, Information security risk management koji daje uputstva za ISMS metode i tehnike upravljanja rizikom kao podrška ISO/IEC 27001
- ISO/IEC 27006:2007, Requirement for bodies providing audit and certificatio of information security system koji daje zahteve za akreditaciju za sertifikaciona tela koja sertifikuju ISMS prema ISO/IEC 27001 zahtevima. On navodi specifične zahteve za sertifikaciju i zajedno sa ISO/IEC 17021 predstavlja osnovni standard za akreditaciju,
- ISO/IEC 27007 (u izradi), Guidelines for information security management systems auditing, obezbediće uputstva za interne i eksterne provere ISMS i program provera u skladu sa standardom ISO/IEC 27001.

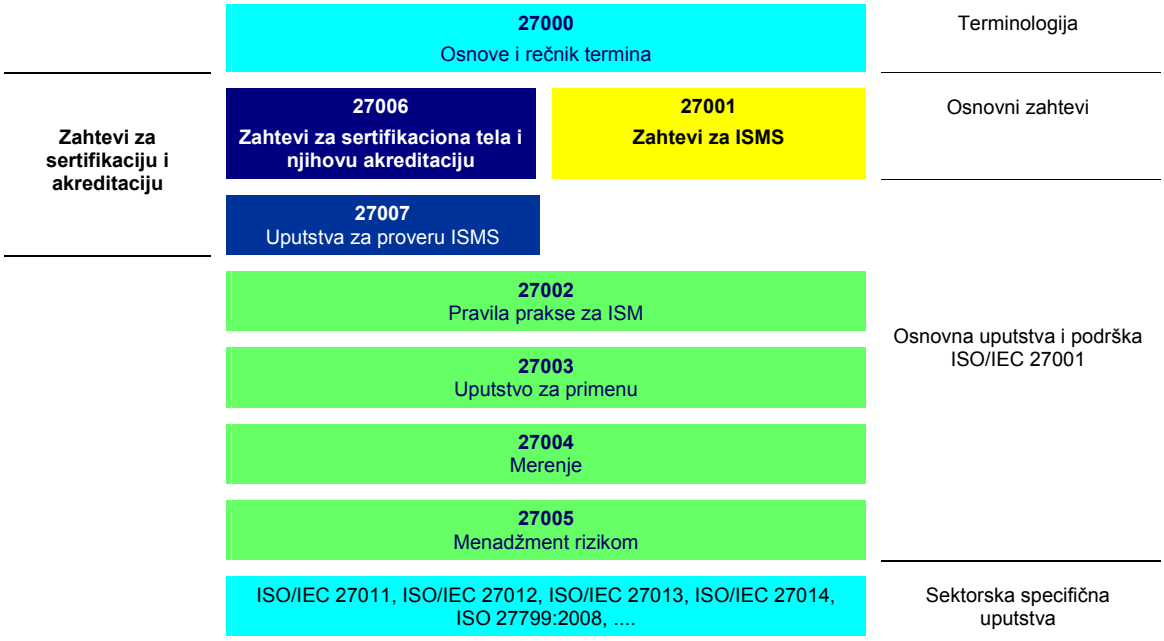
Pored navedenih osnovnih, postoji i određeni broj standarda koji se odnose na specifične sektore, i dopuna su seriji ISO/IEC 27000 standarda, kao:

- ISO/IEC 27011, zahtevi za sektor telekomunikacija
- ISO/IEC 27012, zahtevi za automobilsku industriju
- ISO/IEC 27013, svetska organizacija za loto
- ISO/IEC 27014, informacioni sistem u transportu

kao i standard

- ISO 27799:2008, Health informatics-Information security management in health using ISO/IEC 27002

Na slici 1. su prikazani struktura, međusobne veze i uloge standarda serije ISO/IEC 27000. Većina navedinih standarda je u primeni dok su ostali u postupku razvoja i donošenja. Može se reći da je glavni standard ISO/IEC 27001:2005, koji sa standardom ISO/IEC 27006:2007 definiše opšte zahteve za ISMS i njegovu sertifikaciju, dok ostali predstavljaju podršku i daju uputstva za interpretaciju celokupnog procesa planiraj-uradi-proveri-deluj i zahteva definisanih u ISO/IEC 27001.
Ova serija standarda je u vezi i sa mnogim drugim ISO i ISO/IEC standardima koji se odnose na oblast bezbednosti informacija i koji obezbeđuju specifične zahteve, uputstva i sl.
ISO/IEC 27001 ističe da nije moguće u potpunosti eliminisati celokupan rizik u vezi sa bezbednošću informacija i omogućava organizacijama da ustanove kriterijume koji će uravnotežiti mogućnosti poslovanja, zahteve definisane u propisima, ugovorne obaveze, cenu kontrolisanja bezbednosti informacija i rizik.



Slika 1. Međusobne veze standarda serije ISO/IEC 27000

AKREDITACIJA I PRIMENA STANDADRA ISO/IEC 27006:2007

Sistematskim pristupom i uspostavljanjem sistema menadžmenta bezbednošću informacija u skladu sa standardom ISO/IEC 27001:2005 ostvaruje se poverenje u sigurnost i pouzdanost potrebnih informacija. Pouzdanost i poverenje u sam sistem menadžmenta bezbednošću informacija, s druge strane, postiže se njegovom sertifikacijom.

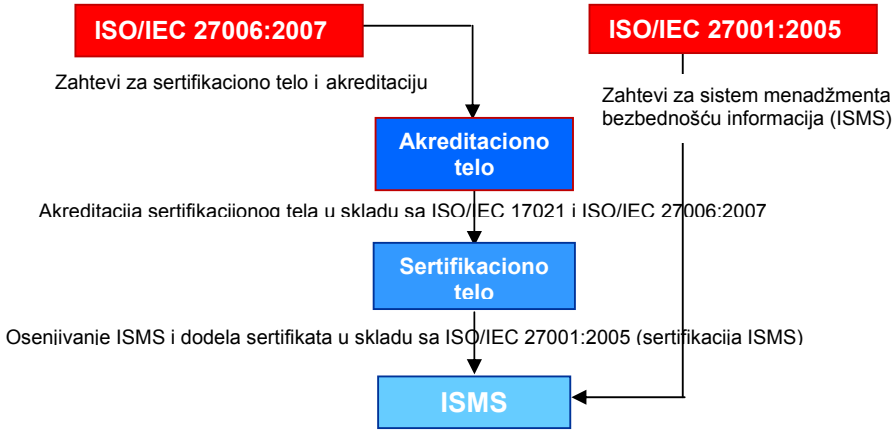
Tokom sertifikacije, kao postupka ocenjivanja usaglašenosti, različitim aktivnostima se potvrđuje ispunjenost zahteva koji se odnose na ISMS i koji su navedeni u ISO/IEC 27001:2005.

Kvalitetne i pouzdane rezultate sertifikacije mogu obezbediti samo sertifikaciona tela, čija je kompetentnost potvrđena u skladu sa harmonizovanim kriterijumima međunarodnih standarda (u slučaju ISMS to su međunarodni standardi ISO/IEC 17021 i ISO/IEC 27006), i uputstvima međunarodnih i regionalnih organizacija za akreditaciju. Akreditacija, kao harmonizovani postupak koji se sprovodi u skladu sa standardom ISO/IEC 17011, predstavlja efikasan način potvrđivanja i praćenja kompetentnosti tela za ocenjivanje usaglašenosti, pa i sertifikacionih tela, od strane nezavisne i nepristrasne institucije koju predstavlja nacionalno akreditaciono telo. U Republici Srbiji ta uloga je od strane države poverena Akreditacionom telu Srbije (ATS).

Ovakav način ocenjivanja, potvrđivanja i praćenja, odnosno sertifikacije ISMS koje je izvršila nepristrasna i nezavisna „treća strana“, koja i sama podleže ocenjivanju i praćenju od strane Akreditacionog tela, obezbeđuje veće poverenje u taj sistem, a samim ti i u bezbednost informacija koje su tim sistemom obuhvaćene. Primena usklađenih postupaka obezbeđuje slične nivoe kompetentnosti sertifikacionih tela, koja sertifikuju ISMS, što obezbeđuje ujednačen pristup i objektivnost, kao i visok nivo bezbednosti informacija.

U cilju harmonizacije, uspostavljen je i primenjuje se međunarodni standard ISO/IEC 27006:2007. On navodi specifične zahteve i obezbeđuje uputstva za tela koja sertifikuju ISMS prema ISO/IEC 27001 zahtevima. Ovaj standard zajedno sa ISO/IEC 17021, predstavlja osnovni standard za akreditaciju sertifikacionih tela koja sertifikuju ISMS. Namena ovog standarda je da obezbedi kredibilitet i kompetentnost za obavljanje provere i sertifikacije ISMS.

Standard ISO/IEC 17021 definiše opšte kriterijume na sertifikaciona tela koja sprovode ocenjivanje i sertifikaciju bilo kog sistema menadžmenta (sistem menadžmenta kvalitetom, sistem menadžmenta zaštitom životne sredine, sistem menadžmenta bezbednošću hrane, sistem menadžmenta bezbednošću informacija i dr.). Međutim, za tela koja žele da sertifikuju ISMS bilo je potrebno definisati dodatne specifične zahteve i oni su definisani u standardu ISO/IEC 27006. Ključni dodatni zahtevi, definisani u ovom standardu, se odnose na: sukob interesa, odnosno nepristrasnost I nezavisnost u postupku sertifikacije; kompetentnost i veština rukovodstva i zaposlenih u sertifikacionom telu; procedure za dodelu, održavanje, suspeziju i oduzimanje sertifikata; na ISMS dokumenta kojima se potvrđuje sertifikacija; kontrolisanje upotrebe sertifikacionog znaka; pristup zapisima; opšte kriterijume za provere i, u slučaju organizacija sa više lokacija, način izbora lokacija na kojima će se sprovoditi provera; metodologiju provere, postupak provere i izveštaj o proveri; kompetentnost tima za proveru; specifične elemente provere koji se odnose na ISMS; obim sertifikacije i odluku o sertifikaciji. Cilj ovog standarda je takođe da omogući akreditacionim telima da harmonizovano i efektivno ocene i potvrde kompetentnost ovih sertifikacionih tela u skladu sa navedenim zahtevima.
Na slici 2. su prikazane uloge i veze različitih učesnika u postupku sertifikacije ISMS i akreditacije sertifikacionih tela koja ga sertifikuju.



Slika 2. Uloge i veze učesnika u sertifikaciji i akreditaciji

ZAKLJUČAK

U zavisnosti od visine procenjenog rizika od pojave neusaglašenosti u oblasti bezbednosti informacija, a i u cilju snižavanja rizika na prihvatljiv nivo, država može propisati zakonsku regulativu sa obaveznom primenom ocenjivanja usaglašenosti, odnosno sertifikacije sistema menadžmenta bezbednošću informacija. Kao i proizvod ili proces i informacija može biti nebezbedna i može prouzrokovati razne štete, zato obezbeđenju sigurnosti informacija treba pristupiti sistemski i na nivou države proceniti za koje oblasti je neophodno da ovo pitanje bude uređeno odgovarajućim propisima. Uspostavljanje nacionalne strategije sigurnosti informacija u tom smislu postaje neminovnost i predstavlja prioritet kako za građane tako i za organizacije svih vrsta i veličina.

L i t e r a t u r a

1. ISO/IEC 17021:2006, Conformity assessment - Requirements for bodies providing audit and certification of management systems
2. Serija standarda ISO/IEC 27000, Information technology- Security techniques-Information security management systems,
3. D.Krnjaic, V. Živković, Potvrđivanje i praćenje kompetentnosti tela za ocenjivanje usaglašenosti u skladu sa novom EU legislativom i dokumentima IAF, ILAC i EA, Kvalitet br. 9-10, str 13-17, Poslovna politika 2008.