ISO 27001:2005 Potreba ili obaveza

Autor:

Dragan Marković
HDL Design House, Beograd
IRCA Sertified Auditor

Izvod:

U radu je prikazan kratak istorijat objavljivanja standarda vezanih za sigurnost informacija. Prikazan je trend sertifikacije ISMS-a. Navedeni su glavni elementi sistema i problemi u njegovom uvodjenju i primeni. U radu je dat pregled zakona koje je Skupština Republike Srbije donela, a koji se direktno odnose na sigurnosti informacija. U zaključku su prikazane glavne prednosti funkcionisanja ISMS-a u organiziciji i eventualni nedostaci koje mogu biti posledica usvojenih propisa u ovoj oblasti.

Ključne reči: ISO 27001:2005, sistem menadzmenta sigurnosti informacija, ISMS, IT

1. Uvod

Kada se oktobra 2005. godine pojavio standard ISO/IEC 27001:2005, za mnoge IT stručnjake je to bio samo jos jedan novi koncept koji organizacijama daje rešenje za sigurnost informacija u eksanzivnom razvoju IT sektora. No ubrzo su se stvari iskristalisale i prvo što su svi uočili je da ovo nije "samo" još jedan informatički standard već nešto mnogo šire. To nešto šire je pokušaj da se u centar stavi informacija, a ne informacioni sistem. Informacioni sistemi predstavljaju je mesto gde se većina informacija danas može naći, ali standard ISO 27001:2005 podrazumeva uvođenje jednog menađment sistema koji će upravljati svim informacijama od važnosti za jednu organizaciju, bez obzira gde se one i u kom obliku nalaze. Ovaj kvalitativni korak je uslovio da se vićana drugih standarda za sigurnost pojedinih delova ili celog informacionog sistema nadju kao deo ili neophodni alat za uspešno funkcionisanje sitema menadžmenta sigurnošću informacija.

2. Kako je sve počelo

Objavljivanju standarda ISO 27001:2005 od strane ISO-a je prethodilo više od pet godina rada, a sve je počelo devedesetih godina kada je počelo intentivnije da se govori o sigurnosti informacija. Kratki istorijat vezan za sisteme sigurnosti informacija moze se sažeti u nekoliko ključnih dogadjaja:

1992 – Ministarstvo trgovine i industrije Velike Britanije je objavilo "Kodeks prakse za Menadžment sigurnosti informacija"
1995 – Britanski institut za standarde (BSI) je ovaj dokument objavio pod oznakom BSI 7799 i nazivom "Sistem menadžmenta sigurnosti informacija - Specifikacija sa uputstvom za korišćenje"
1996 – Dejvid Votson postaje prvi kvalifikovani proverivač (Auditor) za standard BSI 7799

1999 – Izvršena je prva revizija BSI 7799. Akreditaciona i sertifikaciona šema je uspostavljena. LRQA i BSI postaju prva sertifikaciona tela.
2000 – Standard BS 7799 je ponovno objavljen ali formalno pod okriljem ISO-a kao ISO/IEC 17799 Informacione tehnologije – "Kodeks prakse za menadzment sigurnosti informacija"
2001 – Promovisan prvi 17799 alat (Toolkit 17799)
2002 – Objavljen je drugi deo standarda pod oznakom BS 7799-2. To je bila specifikacija, više nego kodeks prakse. Počinje proces usklađivanja sa drugim menadzment standardima, kao što su oni iz serije ISO 9000.
2005 – Objavljena je nova verzija ISO 17799. Ovo uključuje dva nova poglavlja i veće usklađivanje sa BS 7799-2.
2005 – ISO 27001 je objavljen zamenjujući BS 7799-2 koji je povučen. Standard je specifikacija za sistem menadzmenta sigurnosti informacija, koji je usaglašen sa ISO 17799 i spojiv sa ISO 9001.

Poslednjih 6 godina objavljen je veći broj standarda iz serije 27000 koji se odnose na specifične segmente poslovanja organizacija ili bliže definišu pojedine zahteve standarda ISO/IEC 27001:2005.
Pregled objavljenih stanarda serije ISO 27000 (zaključno sa oktobrom 2011)

ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security managemen
ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance
ISO/IEC 27004:2009 Information technology — Security techniques — Information security management - Measurement
ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)
ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for the accreditation of bodies providing audit and certification of information security management systems
ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity
ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management
ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002

3. Sigurnost informacija – problem savremenog društva

Informacije mogu postojati u mnogo oblika i formi. One mogu biti štampane na papiru, uskladištene u elektronskom obliku, mogu se slati poštom ili elektronskim putem, prikazati na filmu ili izreći u razgovoru. Informacije u bilo kom obliku ili sredstvo preko kojeg se one zajednički koriste ili na kojem se čuvaju, one uvek treba da budu odgovarajuće zaštićene. (1)

Pod današnjim pojmom sigurnosti informacija se uobičajeno misli na očuvanje integriteta, raspoloživosti i poverljivosti informacija. Glavni pokretači savremenog poslovanja su:

- Profitabilnost,
- Povratak investicija,

- Ostvarivanje konkurentnosti,
- Usaglašenost sa zakonskim i drugim propisima i standardima,
- Reputacija

Za ostvarivanje poslovnih ciljeva potrebni su različiti resursi koji u svim slučajevima trebaju da budu zaštićeni, a danas ponajviše od konkurencije. Za državne organe, problem predstavlja sigurnost informacija koje su od vitalnog značaja za bezbednost.

Na sigurnost informacija utiču tri glavna faktora:

- Ljudi,
- Sistem,
- Okruženje

U savremenom poslovanju ljudski resursi i ponajviše njihovo znanje (odnosno tehnološka, informaciona i svaka druga veština) je od suštinskog značaja, ne samo u smislu razvoja već i za sam opstanak poslovnih aktivnosti organizacije. Sistemi se, sami po sebi, međusobno razlikuju (jer njihovi elementi nisu identični). Od okruženja će zavisiti sa jedne strane postavka sistema, a sa druge strane okruženje u najvećem delu određuje vrstu rizika po sigurnost informacija.

Kada se govori o sigurnosti informacija kao problemu savremenog društva, poseban pažnju treba staviti na sigurnost informacija različitih državnih organa i institucija, koje mogu imati dalekosežne posledice po funkcionisanje i bezbednost država.

Danas, u velikoj meri, poslovanje zavisi od informacionih tehnologija, komunikacija putem mreža, kao i bežičnih i mobilnih komunikacija. Obim i brzina razmene informacija umnogome doprinose ranjivosti današnjih sistema za procesuiranje informacija. Podatak da je, prema nekim istraživanjima, ljudski faktor u 85% slučajeva uzrok pojave incidenata vezanih za sigurnost informacija, navodi na to da se akcenat treba staviti na organizaciona i sistemska rešenja.

4. Uspostavljanje ISMS-a – izazov za organizaciju

Proces uspostavljanja sistema menadžmenta sigurnosti informacija je odnosu na druge menadžment sisteme nešto komplikovaniji i vreme za njegovo uspostavljanje je duže. Ovo je posledica nekoliko ključnih elemenata:

- Sveobuhvatna procena rizika koju zahteva sam standard
- Mnogobrojni tehničkih uslovi koji moraju biti ispunjeni u savremenim IT sistemima
- Vrsta i učestalost mogućih pretnji po sistem
- 133 kontrolne mere koje trebate primeniti u sistemu (uz uz ograničeni broj mogućih isključenja)

Ovakav pristup koji je standard postavio je za rezultat imao to da je godišnji rast broja sertifikovanih organizacija bio mali. Prema zvanicnim podacima ISO-a na kraju 2009. godine bilo je sertifikovano 12 934 organizacije. Na Slici 1. je prikazan trend rasta broja ISMS sertifikata.

ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements

Overview				
Year	**2006**	**2007**	**2008**	**2009**
TOTAL	**5797**	**7732**	**9246**	**12934**
Africa / West Asia	426	600	983	1554
Central / South America	18	38	72	99
North America	79	112	212	322
Europe	1064	1432	2172	3564
Far East	4150	5494	5740	7335
Australia / New Zealand	60	56	67	60

Regional share - in %				
Year	**2006**	**2007**	**2008**	**2009**
TOTAL	**100%**	**100%**	**100%**	**100%**
Africa / West Asia	7.3%	7.8%	10.6%	12.0%
Central / South America	0.3%	0.5%	0.8%	0.8%
North America	1.4%	1.4%	2.3%	2.5%
Europe	18.4%	18.5%	23.5%	27.6%
Far East	71.6%	71.1%	62.1%	56.7%
Australia / New Zealand	1.0%	0.7%	0.7%	0.5%

Annual growth - absolute numbers				
Year		**2007**	**2008**	**2009**
TOTAL		**1935**	**1514**	**3688**
Africa / West Asia		174	383	571
Central / South America		20	34	27
North America		33	100	110
Europe		368	740	1392
Far East		1344	246	1595
Australia / New Zealand		-4	11	-7

Annual growth - in %				
Year		**2007**	**2008**	**2009**
TOTAL		**33%**	**20%**	**40%**
Africa / West Asia		41%	64%	58%
Central / South America		111%	89%	38%
North America		42%	89%	52%
Europe		35%	52%	64%
Far East		32%	4%	28%
Australia / New Zealand		-7%	20%	-10%

Slika 1. Trend rasta broja ISMS sertifikata

Prvih nekoliko meseci od zvaničnog objavljivanja standarda, koji je tako dugo pripreman nije bilo ni jedne sertifikovane organizacije, ali stvari su se vrlo brzo počele da menjaju, ipak sporije u odnosu na primenu drugih standarda. Upoređujući ove podatke sa podacima o sertifikaciji prema drugim standardima, na primer ISO 22000:2005, možemo uočiti, da je u periodu 2006 – 2009 godina, broj sertifikata ISMS-a rastao po stopi koja je za 30 % bila niža od broja izdatih sertifikata za ISO 22000, bez obzira na veliku ekspanziju i razvoj IT sektora u celom svetu.

Jedan od velikih pomaka u pristupu ISMS u odnosu na standarde koji su se primenjivani, najčešće od strane proizvođača specifične informatičke opreme, softvera ili velikih multinacionalnih kompanija, je u sveobuhvatnom pristupu sistema menadzmenta sigurnošću informacija. Mora se naglasiti da iako je standard ISO/IEC 27001:2005 izdat pod segmentom informacionih tehnologija, on ne predstavlja “samo” informatički standard, jer obuhvata i fizičko – tehničku zaštitu, upravljanje ljudskim resursima, usklađenost sa zakonskim, tehničkim i drugim propisima i sveobuhvatno planiranje i vrednovanje aktivnosti u sistemu menadžmenta sigurnosti informacija.

Velika konkurencija na tržištu, nedostatak finansijskih sredstava i borba za sve veću profitabilnost podstakla je i najveće svetske kompanije da posle nekog vremena prihvate ovaj standard kao najbolji za ispunjenje njihovih ciljeva u odnosu na sigurnost informacija. Najveci pomak u tom smislu je sertifikovanje glavne kancelarije Majkrsofta (Microsoft Global Foundation Services Division)

i pojedinih njegovih ogranaka u Americi i Evropi, prema standardu ISO/IEC 27001:2005 od strane BSI početkom 2011 god. Ovo je uticalo snažno na konkurenciju koja je odgovorila sa najavom sertifikacije pojedinh delova ili čak citavih kompanija. Mora se uzeti u obzir da usled obimnih zahteva standarda pojedine multinacinalne kompanije odustaju od sertifikacije, jer već imaju svoje sisteme koji su razvijani u dužem vremenskom periodu. Procena kompanije Teksas Instrument (Texas Instruments), odnosno njenog IT Security Department-a je da bi sertifikacija prema zahtevima ovog standarda koštala između 8 i 10 miliona $, uključujući i neophodne infrastrukturne, organizacione i tehničke izmene u kompaniji.

5. ISMS za mnoge u Srbiji postaje obaveza

Skupština Republike Srbije je, uskladjujući zakonodavstvo Srbije sa zakonodavstvom evropske unije, donela set zakona koji se odnose na sigurnost informacija (direktno iliindirektno). U roku od dve godine doneti su sledeći zakoni koji se odnose na sigurnost podataka:

1. Zakon o zaštiti podataka o ličnosti
2. Zakon o tajnosti podataka
3. Zakon o čuvanju poslovne tajne

U skladu sa Zakonom o tajnosti podataka Vlada Republike Srbije donela je Uredbu o posebnim merama zaštite tajnih podataka u informaciono – telekomunikacionim sistemima. U članu 10 ove Uredbe eksplicitno je napisano da radi održavanja bezbednosti sistema u toku njegovog korišćenja, organ javne vlasti, odnosno pravno lice sprovodi “primenjivanje novih tehničkih i programskih sredstava u sistemu u skladu sa odgovarajućim tehničkim standardima SRPS ISO/IEC 27001 i SRPS ISO/IEC 17799”(2).

Ova Uredba je obavezala sve državne organe i organizacije koje rade sa njima i za njih, a imaju pristup tajnim podacima, da praktično uspostave sistem menadzmenta sigurnosti informacija (mada formalno ne moraju biti sertifikovani). Uredba je tako koncipirana da se u njenih 27 članova mogu prepoznati glavni ciljevi grupa kontrola Aneksa A standarda ISO/IEC 27001:2005.

Postavlja se pitanje kako će Vlada Republike Srbije, koja je donela Uredbu, vršiti kontrolu njenog sprovođenja jer se organi javne vlasti, odnosno organizacije ne obavezuju na sertifikaciju, pa ostaje nejasno ko će i sa kakvim kompetencijama vršiti proveru usklađenosti sistema sa zahtevima standarda ISO 27001:2005.

6. Zaključak

Imajući u vidu stalnu ekspanziju IT industrije i sve izazove koje stoju pred savremena drštva potreba za uvođenjem sistema menadžmenta sigurnosti informacija je veća nego ikada. Na potrebu impleplementacije zahteva standarda ISO/IEC 27001:2005 pre svega utiču brojni rizici po sigurnost informacija. Zakonski propisi koji su doneseni u Republici Srbiji, stvaraju samo predpostavsku za bržu implementaciju i stvaranje neophodnih uslova da se problematika sigurnosti informacija postavi na jedan kvalitativno viši nivo.

Litratura:

(1) ISO/IEC 17799:2004
(2) Uredba o posebnim merama zaštite podataka u informaciono-telekomunikacionim sistemima
(3) ISO web site – www.iso.org