ASOCIJACIJA ZA KVALITET I STANDARDIZACIJU SRBIJE

FESTIVAL KVALITETA 2008.
35. Nacionalna konferencija o kvalitetu
Kragujevac, 13. - 15. maj 2008.

PRIPREMA ZA CERTIFIKACIJU ISO 27001 POMOĆU PROGRAMA HESTIA ISMS*

Mr Zdenko Adelsberger[1)]

Rezime: *U radu se nalazi prikazan način pripreme kompletnog postupka za certifikaciju organizacije prema standardu ISO 27001:2005. Uz prikaz postupka dat je i pregled kako se taj postupak može bitno pojednostaviti i skratiti upotrebom softwera HESTIA ISMS.*
Ključne reči: *informacijska sigurnost, sigurnost, informacioni sistem, ISMS*

Abstract: *The article describes complete procedure of preparing organization for certification based on standard ISO 27001:2005. Together with procedure it is also shown how the procedure can be simplified by using software HESIA ISMS.*
Key words: *Information Security, Security, Information System, ISMS*

1. UVOD

Postojanje informacionih sistema (IS) ni u kom slučaju nije započelo kompjuterskim dobom. IS postoje praktički od kada su poznate djelatnosti i rad ljudi, od najstarijih vremena pa do danas. U općem smislu, pod IS se smatra skup resursa, pravila i organizacija provođenja aktivnosti vezanih za generiranje, obradu, prijenos, arhiviranje i upotrebu informacija. Kao što se može zaključiti, glavni objekt oko kojega se sve vrti u IS je **informacija**. No, šta se može reći o definiciji pojma informacije. Postoji niz raznih definicija koje su manje ili više slične, ali za potrebe ovog teksta može se pojednostavljeno reći da informacija predstavlja svaki podatak koji ima neku vrijednost za korisnika. Čim se radi o vrijednosti onda se u prvom redu smatra da je moguće svaku informaciju valorizirati i izraziti neku mjeru kroz odgovarajuću novčanu vrijednost. To ponekad nije jednostavno, odnosno, ponekad oni koji su "zaduženi" za valorizaciju informacija nemaju dovoljno iskustva ili nemaju dobro razrađena mjerila kojima bi mjerili vrijednost informacije. To ovog trenutka nije od značaja, osim konstatacije da je informacija ima neku vrijednost. Automatski se nameće zaključak da nešto što ima neku vrijednost predstavlja imovinu za vlasnika. U tom smislu i standard ISO 27001:2005 kaže da je informacija imovina prema kojoj se u organizaciji treba odgovarajuće odnositi, kao i prema bilo kojoj drugoj imovini.

Kada je riječ o materijalnoj imovini problem očuvanja vrijednosti iste je u biti dosta jednostavno definirati (onemogućiti krađu, onemogućiti oštećenja, osigurati pravilnu upotrebu, itd). S druge strane, materijalna imovina je opipljiva i relativno jednostavno za shvatiti njeno očuvanje. Međutim, informacija je apstraktan pojam, ne može se dotaknuti itd. Problem očuvanja informacije unutar IS zbog toga je malo teže prikazati. Tu značajnu ulogu igra standard ISO 27001:2005 u kojem se kaže da se očuvanje informacija – njene vrijednosti može ostvariti u okviru IS tako da se osigura zadovoljavanje osnovna tri zahtjeva:

- *Tajnost* - Informacija mora biti dostupna samo ovlašenim korisnicima
- *Integritet* – sadržaj informacije se ne smije promijeniti bez dozvole vlasnika, te
- *Dostupnost* – do informacije se može doći od strane ovlaštenog korisnika kada i gdje je to potrebno.

Za IS koji osigurava ova tri aspekta sigurnosti u kontekstu standarda ISO 27001:2005 se kaže da je siguran, te da se u njemu čuva informaciona vrijednost. No, ISO 27001:2005 pored toga zatjeva da se način uspostave ova tri aspekta informacijske sigurnosti ostvaruje kroz organizirani sistem i da se stanje sigurnosti stalno unapređuje. To se **mora** ostvarivati procesnim pristupom, a da se do unapređenja dolazi tzv. PDCA krugom. Poštivanjem tih zahtjeva, ali i nekih drugih koji nisu tu spomenuti kaže se da organizacija ima sistem za upravljanje informacijskom sigurnošću, poznat po akronimu ISMS (Information Security

1) Mr Zdenko Adelsberger, EOQ ISMSM, QA, QSM, OHSSM, Bluefield doo, Zagreb, HR, mail: zadelsbe@zg.t-com.hr
*) Ovaj rad je nastao kao rezultat praktične primjene samostalno razvijenog programa Hestia ISMS

Management System). Upravo je standard ISO 27001:2005 skup zahtjeva koje se mora ispuniti ako se želi certficirati uspostavljeni ISMS.

1. PROJEKT IMPLEMENTACIJE ISMS

Uspostavljanje ISMS u organizaciju je izuzetno složen i ozbiljan posao u kojega se mora uključiti niz raznih specijalista. Uz to, vremeski dosta traje zbog obima posla i teškoća koje se pojavljuju. To znači, u koliko se želi implementirati ISMS u organizaciju, u pravilu se treba pokrenuti projekt s identificiranim voditeljem i sva tri parametra projekta: ciljem (kvaliteta realizacije), budžetom i vremenskim planom realizacije. Nakon završetka projekta implementacije ISMS u organizaciju, te dobijanja certifikata prema standardu ISO 27001, sam projekt automatski prelazi u proces upravljanja i unapređenja ISMS, s time što se funkcija voditelja projekta zamjenjuje s funkcijom menadžera informacijske sigurnosti (ISMSM).

	Faze PDCA modela	Aktivnosti
Projekt implementacije	**Plan** (uspostaviti ISMS)	Uspostaviti ISMS politiku, ciljeve, procese i procedure važne za upravljanje rizikom i poboljšanje informacijske sigurnosti kako bi dali rezultate u skladu s ukupnom politikom i ciljevima organizacije.
	Do (implementirati i izvršavati ISMS)	Implementirati i izvršavati ISMS politiku, kontrole, procese i procedure.
Početak upotrebe nakon certifikacije	**Check** (nadgledati i provjeravati ISMS)	Procijeniti i gdje je primjenjivo, mjeriti izvršavanje procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo te izvještavati upravu o rezultatima radi provjere.
	Act (održavati i poboljšavati ISMS)	Poduzeti korektivne i preventivne akcije zasnivane na rezultatima interne ISMS prosudbe (audita) i provjere uprave ili ostalim bitnim informacijama, kako bi se postiglo stalno poboljšanje ISMS-a.

Tabla 1- PDCA model ISMS prema ISO 27001:2005

U tabeli 1. su prikazane faze PDCA modela za uspostavu i održavanje - unapređenje ISMS prema ISO 27001:2005. Početak implementacije (faze P i D) se definiraju kao projekt implementacije. Nakon uspješno završenog projekta implementacije ISMS normalno bi se trebalo pozvati akreditacijsko tijelo koje bi certificiralo ISMS u organizaciji. Nakon toga nastavlja se životni ciklus ISMS prema PDCA krugu (faze C i A), te ponovno na početak u fazu P. Međutim ta faza više ne predstavlja dio nekog projekta, već uspostavljenog procesa sveukupnog upravljanja i poboljšanja ISMS.

Važno je naglasiti da je standard ISO 27001:2005 u potpunosti usaglašen sa temeljnim standardom ISO 9001:2000, ali i sa ISO 14001:2004. To znači da se tamo definirani zahtjevi u pogledu uspostavljanja sistema upravljanja u okviru ISMS moraju apsolutno poštivati. To dovodi do nužne integracije QMS i ISMS. Ta se integracija prvenstveno ogleda kroz jedinstveno i zajedničko rješavanje pitanja kao što su:

- upravljanje dokumentima i zapisima,
- upravljanje auditom,
- korektivne i preventivne akcije,
- upravljanje imovinom, te
- analiza.

Realizacija pojedinih faza projekta implementacije ISMS u organizaciju, a kasnije i poboljšanje sistema je vrlo kompleksno, prvenstveno zbog potrebe stalne procjene rizika kao osnovnog pokazatelja šta i koliko treba poduzimati da bi se postigao odgovarajući stupanj sigurnosti, ali i redovne pojave da je IS vrlo dinamičan i podložan stalnim promjenama kako po volumenu, tako i po sadržaju elemenata koji ga određuju. Za imalo veće organizacije, praktički je nemoguće provesti upravljanje sa ISMS bez odgovarajućeg skupa softverskih alata kojima se bitno poboljšava mogućnost upravljanja i dokazivanja da je sistem pod kontrolom (presudno za certificiranje i recertificiranje).

Na tržištu postoji relativno veliki broj alata kojima se može pomoći u većoj ili manjoj mjeri kod implementacije i unapređenja ISMS. Analizom većeg broja tih alata zaključili smo da je najbolje razviti vlastiti alat koji je funkcionalno potpuno usmjeren na zadani posao implementacije ISMS i kojim se mogu zadovoljiti svi zahtjevi koje definira standard ISO 27001:2005.

U tabeli 2 su prikazani neki od značajnijih parametara s posebnim naglaskom na razlike i prednosti rješenja softvera HESTIA ISMS.

Na slici 1. je prikazana blok shema programa HESTIA ISMS. Na njoj se vide samo najvažniji

moduli koji su uključeni u sve faze implementacije ISMS u organizaciju.

Parametar	HESTIA ISMS	Vs Risk™	RA2	CRAMM
Usklađeno sa 27001	**DA**	**DA**	**DA**	**DA**
Usklađeno sa BS7799-3	**DA**	**DA**	NE	NE
Vizard za procjenu rizika	**DA**	**DA**	NE	NE
Slobodna definicija skala za procjenu rizika	**DA**	NE	NE	NE
Risk metoda	Kvant.	Kvant	Kvant.	Kvant.
Upravljanje dokumentac.	**DA**	NE	NE	NE
Podržava 4 nivoa dokum.	**DA**	NE	NE	NE
Licenc.	**Single / multy use**	Single use	Single use	**Single / multy use**
Višejezika	**DA**	NE	NE	NE
Ugrađena relacija prijetnja – ranjivost – kontola	**DA**	NE	NE	NE
Generira SoA	**DA**	DA	DA	DA
Visual Query	**DA**	NE	NE	NE
Potpuna administarcija prava	**DA**	NE	NE	NE
Cijena € (po korisniku)	**999**	1.400	1.600	3.500

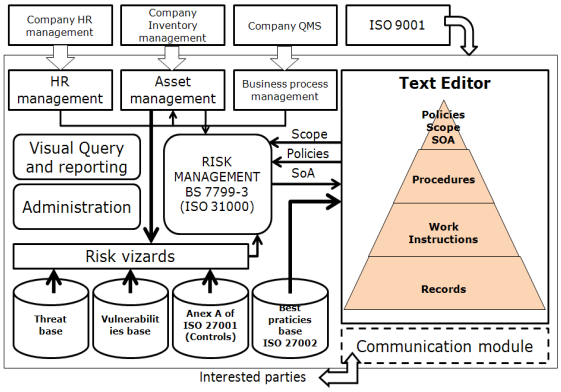
Tabla 2- Usporedba nekih softvera za ISMS

U svakom slučaju program HESTIA ISMS uvažava postojeće sisteme u organizaciji, kao što su npr. eventualno uspostavljeni QMS, postojeća kadrovska evidencija (upravljanje ljudskim potencijalom), osnovna sredstva, sisteme zaštite ljudi i prostora, itd. Iz tih sistema je moguće importirati razne postojeće podatke, što je naročito značajno za velike organizacije da bi se izbjeglo masovno prekucavanje podataka.

Glavni moduli programa Hestia ISMS su:

- Modul za definiranje opcija programa i pravila kojima se izvršava program kod korisnika;
- Modul za administraciju (održavanje baze podataka, arhiviranje baze, evidencija i prava korisnika, itd);
- Modul matičnih podataka (evidencije osoblja, organizacija, partnera, poslovnih procesa, itd.) relevantnih za IS organizacije;
- Modul za upravljanje informacionom imovinom;
- Modul za definiranje pravila procjene rizika (ranjivosti, prijetnje, sigurnosne mjere);
- Modul za optimalnu selekciju kontrola za prijetnje i ranjivosti prema klasifikaciji informacijske imovine;
- Modul upravljanja rizicima (procjena rizika, obrada rizika)
- Modul za automatsko generiranje dokumenta "Izjava o primjenjvosti" (SoA);
- Modul za izvještavanje i komunikaciju sa zainteresiranim stranama;
- Modul za upravljanje dokumentacijom;
- Modul za izradu predložaka (Template) za politike, procedure, upute i zapise;
- Ugrađen potpuni WYSIWYG tekst procesor za obradu dokumenata (kompatibilan s MS Wordom)
- Ugrađen grafički program za crtanje dijagrama toka (Flow Chart)
- Modul za import baza "najbolje prakse" za politike i procedure, ali i ostale tipove dokumenata.

Svi ugrađeni moduli u funkcionalnom smislu u potpunosti zadovoljavaju prvenstveno sve zahtjeve koji za te poslove traže standardi (ISO 27001, ISO 27002, BS 7799-3, ISO 9001, itd).

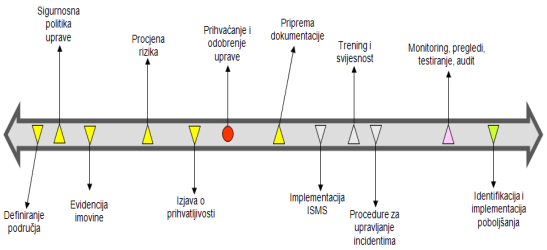


Slika 1 – Blok shema programa Hestia ISMS

Posebna pažnja je poklonjena jednostavnosti rada primjenom najnovijih programskih tehnika što je dovelo do intuitivnog rješenja koje korisnici vrlo lako prihvaćaju.

Zbog svoje konfiguracije i tehnike realizacije, program HESTIA ISMS se može koristiti i za obuku ili treninge tima koji vrši implementaciju. Platforma na kojoj program radi su od MS XP do WIN 2K servera kao dijeljena aplikacija ili u modu client/server, pa se može pogoniti i preko intraneta / interneta.

Sama tehnika primjene programa Hestia ISMS u prvom redu se svodi na poštivanje procedure implementacije kajo je manje više zadana i zahtjevana u standardu ISO 27001:2005. Na temelju tih zahtjeva proces implementacije – uvođenja ISMS u organizaciju se može prikazati kao što je prikazano na slici 2.



Slika 2 – Blok shema implementacije ISMS

Praktično, pomoću programa Hestia ISMS treba proći te korake od početka do kraja. Nakon što se implementira ISMS i certificira pomoću programa Hestia ISMS se nastavlja proces upravljanja i poboljšanja.

ZAKLJUČAK

Programom Hestia ISMS se omogućava kvalitetna implementacija ISMS prema zahtjevima standarda ISO 27001:2005 u svim fazama od planiranja do certifikacije, a i u kasnije u toku održavanja i unapređenja. Primjenom prgrama Hestia ISMS korisnik ima sve potrebne alate za uspješno i optimalno uvođenje ISMS i kasnije upravljanje.

LITERATURA

[1] ISO 27001:2005 “Information technology — Security techniques — Information security”

[2] ISO 17799:2005 “Information technology -- Security techniques -- Code of practice for information security management”

[3] BS 7799-2:2006 “Information security management systems. Guidelines for information security risk management