ASOCIJACIJA ZA KVALITET I STANDARDIZACIJU SRBIJE

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

UPRAVLJANJE RIZICIMA ZA ISO 27001 POMOĆU PROGRAMA HESTIA ISMS*

Dejan Adelsberger[1)]

Rezime: *Prikazan je proces upravljanja rizicima prema zahtjevima standarda ISO 27001, te način praktičnog provođenja pomoću softvera HESTIA ISMS.*
Ključne reči: *sigurnost informacija, ISMS, procjena rizika, upravljanje rizicima*

Abstract: *This article displays the process of risk management according to standard ISO 27001, and the practical way of implementing it using software HESTIA ISMS.*
Key words: *information security, ISMS, risk assessment, risk management*

1. UVOD

Implementacija ISMS prema zahtjevima standarda ISO 27001:2005 je relativno vrlo složen postupak koji je manje više definiran kroz sami standard. U svakom slučaju, problem implementacije ISMS u organizaciju treba shvatiti kao projekt koji mora imati sve opće karakteristike projekta (cilj, rok i budžet), ali i neke specifične, kao npr: neki od učesnika moraju za određene aktivnosti imati dobro obrazovanje i vrlo veliko iskustvo, primjerene baze znanja najboljih praksi u raznim područjima, itd. Kada se govori o potrebama velikog znanja i iskustva, onda na prvom mjestu se misli na stručnjake koji treba da procijene rizike na informacijskoj imovini u cilju očuvanja i unapređenja glavna tri aspekta informacijske sigurnosti: tajnosti, integriteta i dostupnosti (CIA). Naime, ukupne aktivnosti vezane za implementaciju ISMS na temelju standarda ISO 27001:2005 direktno zavise od procjene rizika. Kako ozbiljnost poduzimanja bilo kakve aktivnosti nosi u sebi i financijske zahtjeve, može se zaključiti da nekvalitetna procjena rizika ima najčešće dva efekta:

- Slaba procjena (**preoštra**) izaziva ogromne nepotrebne troškove koji mogu dovesti u pitanje i odobrenje uprave za konačnu implementaciju i certifikaciju a s druge strane ne dovodi se objektivno do značajno višeg stupnja sigurnosti, te ;
- Slaba procjena (**preblaga**) izaziva male troškove implementacije, ali praktički nedovoljnu sigurnost informacijskog sistema, pa troškovi posljedica mogu biti tako veliki da su u stanju ugroziti i egzistenciju organizacije.

Zbog toga se kod odabira tima koji će napraviti dio projekta pripreme i procjene rizika mora pristupiti ozbiljno. Amaterima i pripravnicima tu nije mjesto.

2. IMPLEMENTACIJA ISMS

Projekt implementacije ISMS ima dvije faze: priprema i planiranje, te provođenje i realizacija plana implementacije. U okviru ovog rada je od interesa samo prva faza koja završava donošenjem i prihvaćanjem dokumenta "Izjava o primjenljivosti" (SoA) od strane rukovodstva firme. Koraci implementacije početne faze su prikazani u tabeli 1. Ta početna faza ima praktički 3 podfaze koje u su tabeli prikazane kao posebne faze 1,2 i 3. U drugoj koloni su navedeni koraci koje predlaže i prepoznaje standard ISO 27001:2005. U trećoj koloni su navedeni opisi koraka koji treba napraviti s referencom na točku standarda ISO 27001:2005, te u zadnjoj koloni prijedlog dokumenta koji bi trebalo generirati da bi se mogao u pravilu provesti slijedeći korak.

Od slučaja do slučaja ovi koraci se mogu manje ili više modificirati, ali u konačnici sve se svodi na varijacije onoga što je u standardu ISO 27001:2005 navedeno, a prikazano u navedenoj tabeli.

1) Dejan Adelsberger, EOQ ISMSM, QMSM, dejan@inter-soft.hr
*) Ovaj rad je nastao kao rezultat praktične primjene softwera HESTIA ISMS u procesu implementacije ISMS za organizacije.

Faza	Korak	Opis	Dokument
1	1	Definicija područja (obuhvata) ISMS (4.2.1.a.)	Područje ISMS
	2	Definicija sigurnosne politike ISMS (4.2.1.b.)	Sigurnosna politika
2	3	Definicija metode procjene rizika (4.2.1.c.)	Standardi za implementaciju upravljanja rizicima (prisup organizacije, metode i analize za postizanja zahtjevanog nivoa sigurnosti): • Lista potencijalnih ciljeva i sigurnosnih mjera (kontrola) • Lista dodatnih kontrola koje nisu definirane u ISMS certifikac
	4	Identifikacija rizika (4.2.1.d.)	Lista rizika i popisa imovine
	5	Analiza i procjena rizika (4.2.1.e.)	Izvještaj o rezultatima procjene rizika
	6	Obrada rizika (4.2.1.f.)	Izvještaj o rezultatima obrade rizika
	7	Izbor ciljeva kontrola i kontrola - sigurnosnih mjera (4.2.1.g.)	Standardi mjerenja rizika
3	8	Osiguranje uprave za odobrenje i prihvaćanje preostalog rizika (4.2.1.h.)	Pisano odobrenje za preostali tizik
	9	Osiguranje autorizacije uprave za implementaciju ISMS (4.2.1.i.)	
	10	Priprema dokumenta: Izjava o primjenljivosti (4.2.1.j.)	Izjava o primjenljivosti (SoA)

Tabla 1- Koraci implementacije ISMS – prva faza

Realizacija navedenih koraka je praktički nemoguća bez podrške odgovarajućih softverskih alata. Ručni rad – provođenje pojedinih koraka za male organizacije se može kako – tako provesti i poću nekog tekst procesora, tabličnog kalkulatora i nekog programa za crtanje, ali vrlo teško. U trenutku kada se uspostavi sistem ISMS i dalje treba unapređivati procese upravljanja s njime, tada prestaje mogućnost prihvatljive kvalitete provođenja tih zahtjeva koji su definirani u ISO 27001:2005, ISO 9001:2000, odnosno ISO 9004:2000. Zbog toga je praktički nužno od početka primjeniti odgovarajuće softversko rješenje kojim se mogu postići svi ti ciljevi.

U tu svrhu razvijen je poseban program pod imenom HESTIA ISMS kojim je moguće provesti sve faze implementacije ISMS u organizaciju. Zbog nedostatka prostora da bi se prikazale sve mogućnosti programa na ovom mjestu će se ilustrirati samo dio koji se odnosi na aktivnosti i korake vezane za pripremu i procjenu rizika kao i generaciju dokumenta SoA.

3. PRIMJENA PROGRAMA HESTIA ISMS ZA PROCJENU RIZIKA

Od niza aktivnosti koje su važne za procjenu rizika u procesu implementacije ISMS bit će prikazani slijedeće:

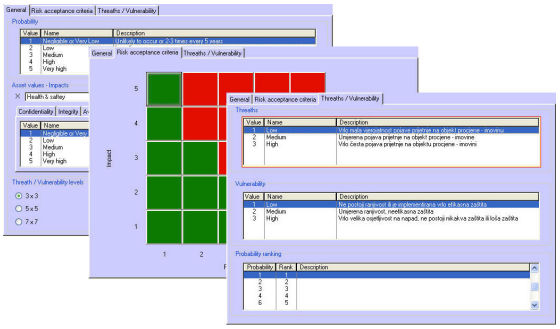
a) Definiranje parametara za rad aplikacije
b) Unos/import podataka potrebnih za obradu imovine (korisnici, organizacijske jedinice, odjeli, tipovi imovine ...)
c) Obrada imovine (unos/import)
d) Unos/import podataka o ranjivostima, prijetnjama te njihovo povezivanje i grupiranje
e) Povezivanje imovine s ranjivostima i prijetnjama
f) Procjena rizika
g) Obrada rizika
h) Izrada dokumenta SoA.

U nastavku će biti prikazane neke značajke najvažnijih gore pomenutih funkcija za upotrebu programa Hestia ISMS.

Definiranje parametara za procjenu rizika odnosi se na izbor matrica – odnosno skala koje će se koristiti za procjene rizika za parametre ranjivost i prijetnje. Program dozvoljava odabir matrica 3x3, 5x5 ili 7x7. Taj je korak izuzetno važan jer kada se odabere određena finoća skale, tada promjena predstavlja poništenje svih do tada napravljenih procjena i ponovni rad.

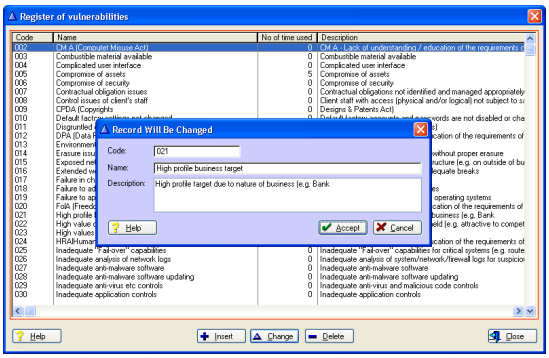
U okviru te aktivnosti se pored obaveznih posljedica (CIA) mogu definirati u do tri aspekta posljedica koja su interesantna za organizaciju. Npr. Aspekt uticaja informacijske sigurnosti na profit, image u javnosti, okoliš itd.

Prikaz izgleda ekrana za podešavanje parametara prikazan je na slici 1.



Slika 1 – Podešavanje parametara aplikacije

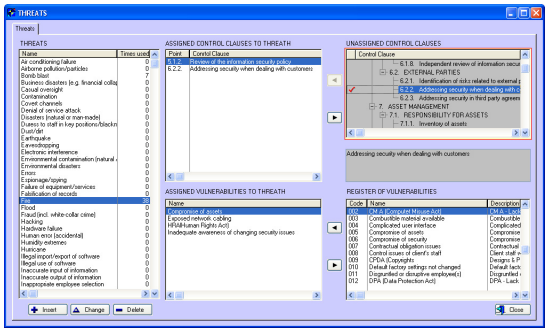
Kako bi se mogla raditi automatska procjena rizika potrebno je nakon popunjavanja registra imovine definirati ranjivosti (Slika 2.) i prijetnje, te ih međusodbno povezati (Slika 3.) te ih grupirati u grupe rizika kako bi se procjena rizika mogla obaviti na automatizirani način.



Slika 2 – Registar ranjivosti

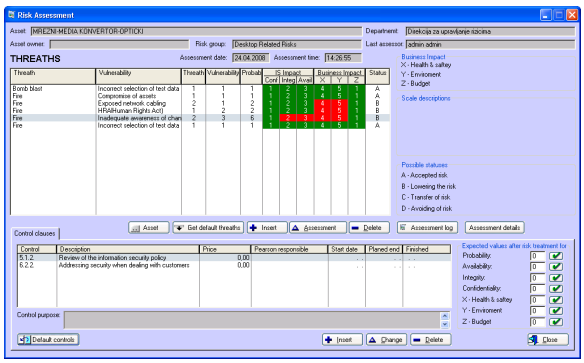
U registrima ranjivosti i prijetnji se kod nabavke programa nalazi veliki broj, više stotina, već poznatih i očekujućih podataka koji se trenutno nalaze evidentirani u svjetskim bazama podataka što korisniku omogućava da praktički za većinu slučajeva ima sve potrebne podatke.

Da bi se što više mogao automatizirati postupak procjene rizika, a kojih u i malo većim organizacijama može biti više hiljada, program Hestia ISMS omogućava tehnikom vizarda povezivanje prijetnji, ranjivosti i sigurnosnih mjera (kontrola) koje su date u aneksu A standarda ISO 27001:2005. Način kako se to može povezati u programu prikazan je na slici 3. To je izuzetno interesantna mogućnost koja uz neke druge primjenjene tehnike automatizacije procjene rizika primjenjene u programu skraćuje višestruko operativno vrijeme. Uz to, mogućnost grešaka se smanjuje i omogućava ujednačenost kvalitete procjene rizika kroz cjelokupni opseg – područje definiranosti ISMS.



Slika 3 – Povezivanje prijetnji, ranjivosti i sigurnosnih mjera (kontrola)

Sama procjena rizika koja se radi na cjelokupnoj imovini uključenoj u opseg IS je najkritičnija u cjelokupnom postupku implementacije. Već je napomenuto da se u programu Hestia ISMS primjenila jedinstvena tehnika operativnog pristupa procjeni rizika, koja uz fleksibilnost ispunjava apsolutno sve zahtjeve koje postavljaju standardi ISO 27001:2005 i BS 7799-3:2006, ali i neki drugi iz serije ISO, BS, NIST itd. Primjer kako se u programu Hestia ISMS vrši procjena rizika prikazano je na slici 4.

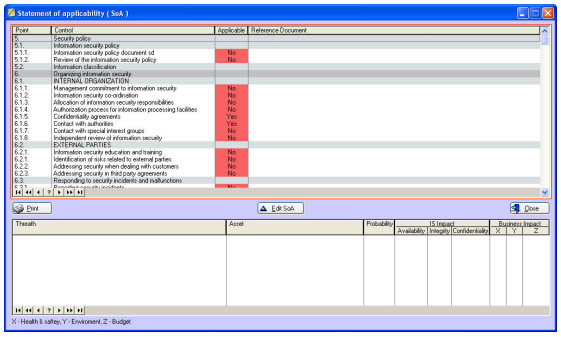


Slika 4 – Procjena i obrada rizika

U okviru procjene rizika, odmah se forsira i obrada rizika, te Cost-benefit analiza opravdanosti planirane zaštite.

Kao rezultat cjelokupne procjene rizika, obrade rizika i suglasnosti uprave u pogledu troškova daljnje implementacije ISMS prema zahtjevima standarda ISO 27001:2005 nužno je donijeti dokument "Izjava o primjenljivosti" (SoA). Ovaj presudni dokument za daljnji nastavak implementacije mora odobriti uprava, a kasnije u fazi certificiranja ju auditor koristi kao polazno objašnjenje zašto se nešto uradili (ili niste) u fazi implementacije ISMS.

Na slici 5. je prikazan ekran programa kojim se automatski generira dokument SoA. Treba ga samo odštampati i potpisati od strane uprave.



Slika 5 – Automatska izrada dokumenta SoA

Svi gore navedeni postupci primjenjeni u programu Hestia ISMS nastali su kao rezultat mogih provedenih ručnih implementacija i istraživanja u smjeru optimizacije provođenja aktivnosti uz maksimalno poštivanje zahtjeva svih relevantnih standarda u tom području. Gore navedene funkcije su samo manji dio cjelokupnih ugrađenih u program Hestia ISMS koji zamišljen kao integralni alat za planiranje, pripremu i provođenje implementacije ISMS, ali i kasnije za njegovo unapređenje.

ZAKLJUČAK

Umjesto zaključka evo neki karakteristika programa Hestia ISMS:

- Mogućnost rada jednog / više korisnika
- Mogućnost rada na jednoj radnoj stanici, mreži ili Internetu / Intranetu
- Višejezičnost
- Svi podaci se nalaze u baze stroge enkripcije
- Potpuna kontrola rada na aplikaciji s vođenjem log lista
- Potpuna usaglašenost s standardom ISO 27001
- Izlazni podaci u formatima .PDF, .DOC, .XLS, .XML, ...
- Uključena baza znanja najbolje svjetske prakse s mogućnošću obnavljanja.
- Minimalni zahtjevi za aplikaciju HESTIA ISMS:
  - Samostalni PC ili radna stanica koja podržava WIN XP
  - Server WIN 2003, Linux
  - Internet -> Windows server

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”