Zdenko Adelsberger, EOQ manager i auditor, Bluefield d.o.o. Zagreb, zadelsbe@zg.htnet.hr
Nenad Injac, EOQ manager i auditor, Oskar Edukos Zagreb, Quality Austria Beč, nenad.injac@qualityaustria.com
Dejan Adelsberger, EOQ manager, inter-SOFT d.o.o. Zagreb, dejan@inter-soft.hr

Implementacija standarda za informacijsku sigurnost ISO17799 i ISO27001

Sažetak:
Potreba za upravljanjem informacijskom sigurnošću je postala ne samo dijelom i zakonska obaveza poslovnih subjekata, već i pitanje opće dugotrajne i stabilne funkcionalnosti svake organizacije. Kako je u zadnjih 20-tak godina informacija postala jedna od najkuretnijih „roba" na tržištu, posebno zbog dominantnog elektronskog oblika obrade, prijenosa i pohranjivanja, nužno je došlo na svjetskoj i nacionalnoj razini do normativne regulacije pitanja vezanih za informacijsku sigurnost. U radu se prikazuje metodologija pristupa i provođenja implementacije preporuka standarda ISO17799:2005 u organizaciju, te zahtjevi prema standardu ISO27001:2005 koji moraju biti ispunjeni da se dobije certifikat za sistem upravljanja informacijskom sigurnošću (ISMS).

Uvod

Kao početak problema borbe za informacijsku sigurnost treba odmah razjasniti šta se podrazumjeva pod pojmom informacija. U raznoj literaturi se sreće niz definicija koje su manje ili više slične, ali za ove potrebe može se pojednostavljeno reći da je „informacija svaki podatak koji ima neku vrijednost za onoga tko ga zna".

Kako je fizički sama informacija „apstraktna stvar", teško se može usporediti sa klasičnim materijalnim sredstvima za koja je relativno jednostavno organizirati čuvanje i zaštitu. No svaka informacija se:

- čuva u nekom obliku (zapis na papiru, na CD/DVD medijima, tvrdim diskovima, u glavama – pamćenju zaposlenika i partnera, itd);
- prenosi (telefoni, telefaksi, kompjuterske mreže, pisma, itd);
- obrađuje (kompjuteru, kod partnera, ručnim manipulacijam zaposlenika, itd), te
- daje na upotrebu raznim korisnicima.

To upućuje na činjenicu, da ako se uvedu određene kontrole na oblike prijenosa, čuvanja, obrade i distribucije informacija, posredno će biti i informacija zaštićena.

U standardu ISO 17799:2005 se kaže da je "Informacija imovina koja kao i ostala važna imovina u poslovanju ima vrijednost za organizaciju i mora biti stalno odgovarajuće štićena."

Upravo taj standard ISO17799 definira šta bi sve organizacija trebala da poduzme da bi se osiguralo štićenje, odnosno zaštita informacija. U samom standardu ISO17799:2005 ima 11 klauzula, odnosno poglavlja, te 132 kontrole čime se sveobuhvatno, na današnjem stupnju saznanja i tehnologije predlaže šta bi se sve trebalo poduzimati u cilju zaštite informacija.

Ako se želi certfificirati ISMS koristi se standard ISO 27001:2005 koji kaže šta organizacija mora provesti da bi se javno priznao organizirani i upravljani sistem zaštite

informacija. Standard ISO27001:2005 je skup zahtjeva koje organizacija mora ispuniti da bi se priznao certifikat za informacijsku sigurnost.

Standard ISO27001:2005 razlikuje dvije vrste zahtjeva za upravljanje informacijskom sigurnošću:
- Metodološki zahtjevi (Poglavlja 4 – 8), i
- Zahtjevi za sigurnosne kontrole (Anex A standarda)

Poglavlja 4-8 standarda ISO27001 sadrže metodološke zahtjeve jer ona kažu *kako* razviti i upravljati s informacijskom sigurnošću. U njima se nigdje ne spominje koje kontrole treba implementirati.

ISO27001:2005 u aneksu A sadrži 2 vrste zahtjeva za sigurnosnim kontrolama:
- Kontrolni ciljevi (Control Objectives)
- Sigurnosne kontrole (Security control)
-

Ovi kontrolni zahtjevi su direktno kopirani iz standarda ISO17799:2005 (poglavlja 5-15). Na njih se referira kao na sigurnosne kontrolne zahtjeve jer čine polazište za ISMS.

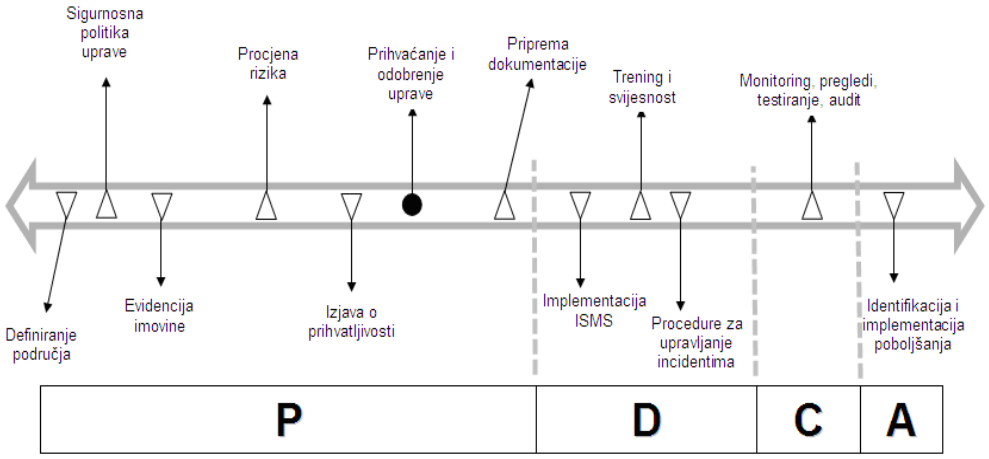
Iz gore navedenoga proizilazi da se za uspostavu i certificiranje sistema za upravljanje s informacijskom sigurnosću (ISMS - Information Security Management Systems) koristi standard ISO27001:2005. U nastavku rada će se prikazati u općim crtama postupak implementacije standarda ISO27001:2005 s naglaskom na najkritičnije korake implementacije.

Projekt implementacije ISMS u organizaciju

Implementacija standarda ISO27001:2005 u organizaciju ima dvije faze. U prvoj fazi koja ovog trenutka nije od posebnog značaja, magemant donosi stratešku odluku da se ide u taj projekt, odnosno osigurava punu podršku za implementaciju.

Druga faza implementacije ima nekoliko koraka. Ti koraci su: određivanje opsega i granice ISMS, definiranje politike ISMS, evidencija imovine (za čuvanje, prijenos i obradu informacija), procjena rizika, donošenje dokumenta „Izjava o prihvatljivosti" (SoA), prihvaćanje i odobrenje uprave, priprema dokumentacije, implementacija ISMS, planiranje i provođenje treninga i podizanja svjesnosti, izrada procedura za upravljanje incidentima i kontinuitetom poslovanja, provođenje monitoringa (pregleda i testiranja), audit, te identifikacija i implementacija poboljšanja.

Treba odmah reći da je standard ISO27001:2005 harmoniziran sa standardom ISO9001:2000, što omogućava integraciju, ali implicira da sve što se nalazi u nekim poglavljiva ISO9001:2000 mora se isto primjeniti i u implementaciji standarda ISO27001:2005. To su npr. procesni pristup, PDCA krug, osnovnih 6 managerskih postupaka za upravljanje, itd. Kada se ti zahtjevi primjene na projekt implementacije ISMS može se pokazati da vremenski dijagram realizacije ima oblik kao na slici 1.



Slika 1. Vremenski dijagram implementacije projekta ISMS s koracima PDCA kruga

Ključni dokument koji se u cijelom projektu implementacije koristi kao temelj za donošenje odluke uprave o konačnom prihvaćanju strukture ISMS je „Izjava o prihvatljivosti" (SoA - Statement of Applicatibility). Kroz taj dokument se točno definira šta sve treba od kontrola primjeniti u organizaciji da bi se uspostavio željeni ISMS. U koliko se kontrola ne primjenjuje tada se mora u dokumentu SoA detaljno navesti razlog zašto se ta kontrola ne koristiu okviru konkretnog ISMS.

Osnov za definiranje dokumenta SoA su sigurnosna politika organizacije, definirana na početku, te u skladu s njom izvršena procjena rizika. To drugim riječima znači, da rezultati procjene rizika na imovini određuju sve kriterije za bilo kakve potrebne kontrole i aktivnosti vezane za uspostavu ISMS.

Procjena rizika za ISMS

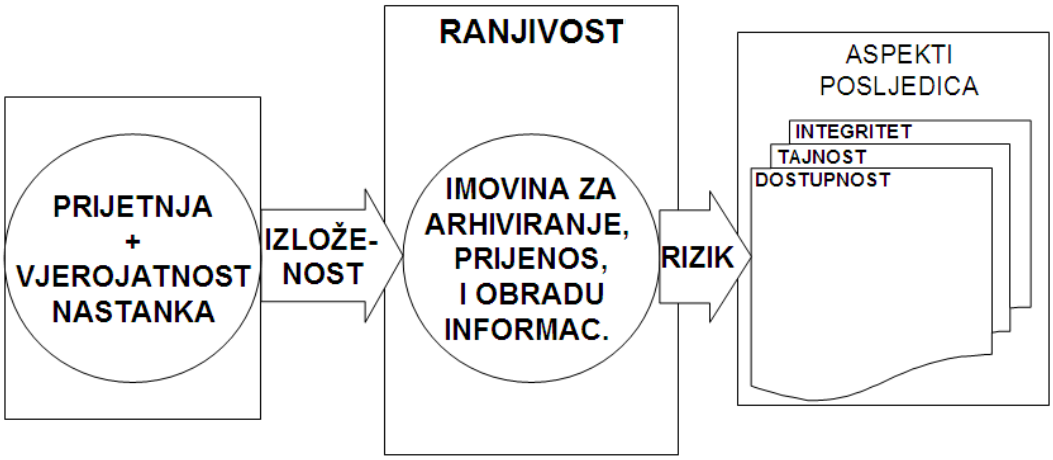
Procjena rizika je jedan od najkritičnijih koraka implementacije ISMS, ne samo zato što je rezultat procjene rizika temelj za planiranje i provođenje potrebnih kontrola, već i zbog samog postupka i metodologije provođenja procjene. Zbog toga je BS (British Standards) izdao uputu BS7799-3:2006 (Guidelines for information security risk management) za provođenje procjene rizika na imovini za potrebe ISMS.

Prema ISO17799:2005 glavni aspekti informacijske sigurnosti su očuvanje raspoloživosti, tajnosti i integriteta informacije. Prema standardu ISO17799:2005, i uputi BS7799-3:2006 nužno je vršiti procjenu rizika ugrožavanja ova tri aspekta informacijske sigurnosti.

Da bi se moglo pristupiti procjeni rizika nužno je da procjenitelj ili njegov tim dobro znaju mehanizme i relacije ugrožavanja informacijske sigurnosti. Na slici 2. je prikazan mehanizam djelovanja rizika na ISMS. Može se pokazati da su ključni parametri koji određuju rizik postojanje prijetnje i ranjivosti ISMS na tu prijetnju.

Prema definiciji **prijetnja** može uzrokovati neželjeni događaj koji može imati štetne posljedice za aspekte informacijske sigurnosti (Dostupnost, Integritet, Tajnost), a **ranjivost** su sigurnosne slabosti povezane s imovinom organizacije, odnosno slabo ili nikako prvedena zaštita od konkretne prijetnje.

U uputi BS7799:2006 se daje nekoliko prijedloga metodologije procjene rizika za informacijsku sigurnost. Pored tih metoda u praksi se sreće još niz drugih varijanti, ali svima je zajedničko da se u pravilu oslanjaju na kvalitativnu procjenu.



Slika 2. Mehanizam pojave rizika u ISMS

Cjelokupni postupak procjene rizika se provodi u nekoliko koraka: definiranje opsega procjene, izbor tima, definiranje metodologije za procjenu, definiranje kriterija za prihvaćanje, definiranje pravila obrade rizika, identifikacija ranjivosti i prijetnji, identifikacija i popis imovine, izrada procjene na imovini, odabir kontrola, te kao konačan dokument izrada SoA.

Ovaj vrlo složen i važan postupak procjene praktički se ne može koliko toliko kvalitetno napraviti ručnim postupkom, već se mora koristiti neko programsko rješenje. U tom smislu će se prikazati postupak procjene rizika pomoću vlastitog kpompjuterskog programa Hestia17799.

Procjena rizika pomoću programa Hestia17799

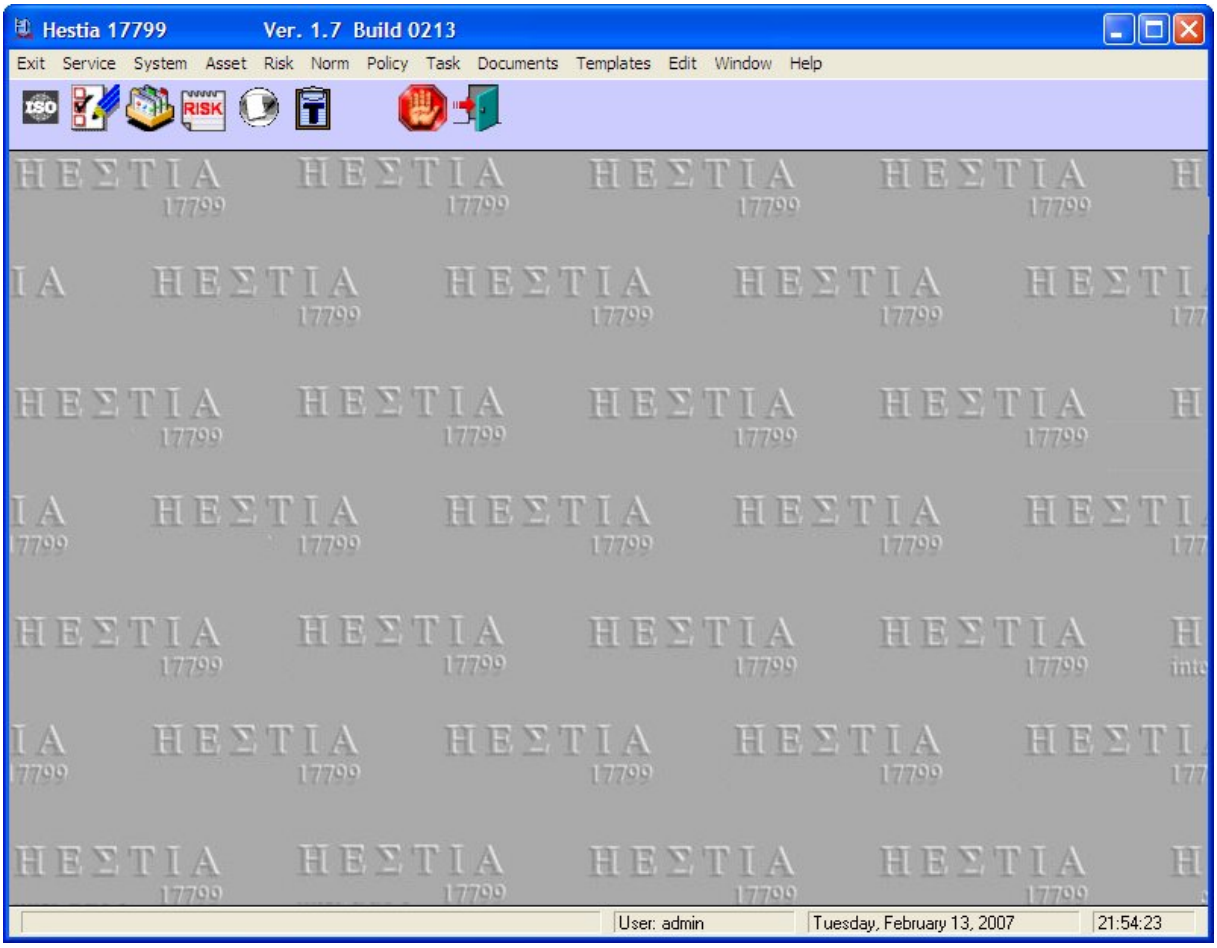
Hestia17799 je programski alat za implementaciju ISMS u organizaciju bazirano na standardima ISO17799 i ISO27001. Osnovne funkcije programa su:

- Edukacija za implementaciju sigurnosti IS
- Planiranje, priprema i implementacija norme ISO 17799
- Provođenje Consultinga za partnerske firme
- Provođenje audita
- Mjerenje nadgradnje sustava sigurnosti IS
- Planiranje aktivnosti u slučajevima katastrofa

Struktura programa je tako podešena da zadovolji zahtjeve metodologije implementacije ISMS. Postoje dvije verzije programa: standard i profesionalna. Standardna verzija programa ima sve potrebne funkcije koje završavaju s dokumentom SoA, a profesionalna dodatno ima mogućnosti izrade dokumentacije, procedura, uputa, te mogućnost implementacije baze znanja s politikama. Za sve dokumente u profesionalnoj verziji postoji mogućnost definiranja predložaka – templatea. Zbog obima ovdje će biti prikazan dio standardne verzija programa Hestia17799.

Za obadvije verzije programa značajno je da su višejezične, višekorisničke, omogućen timski rada, itd.

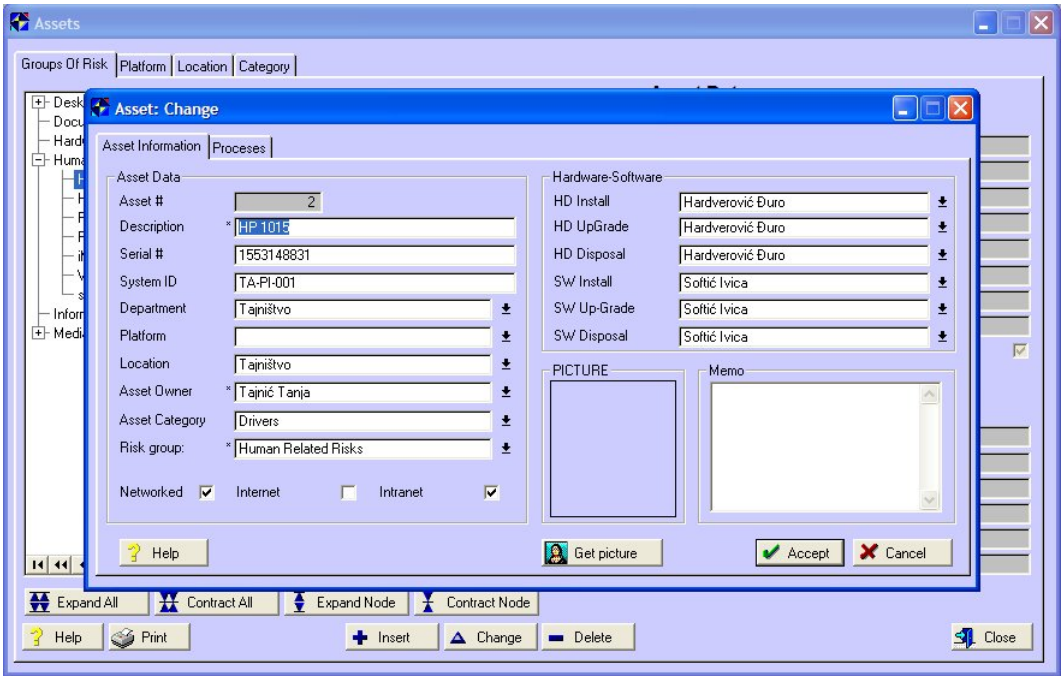
Na slici 3. prikazan je galvni ekran programa Hestia17799.



Slika 3. Glavni ekran programa Hestia17799

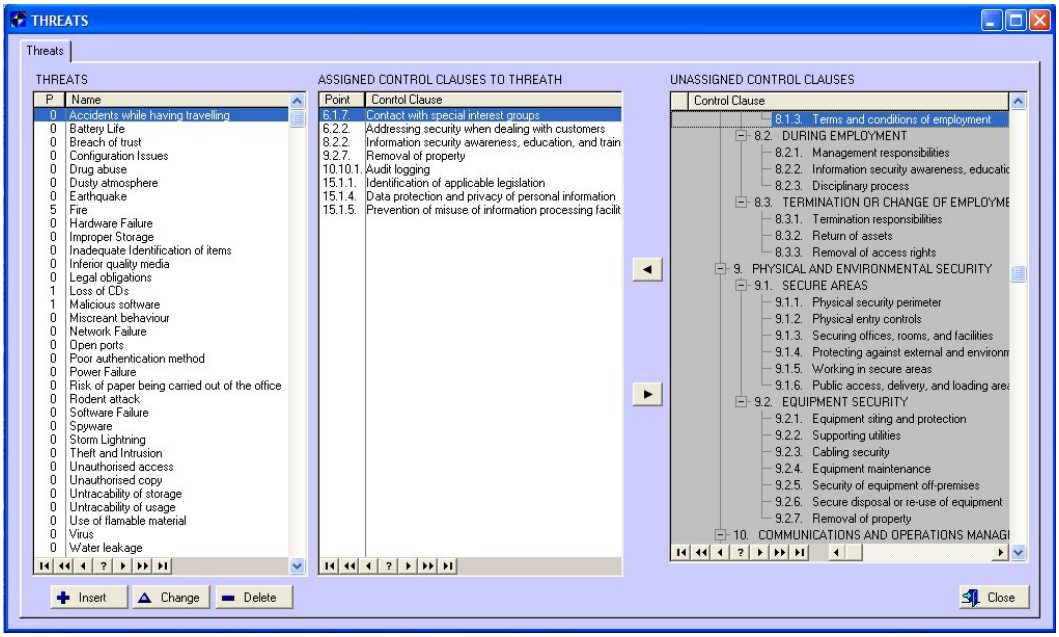
Do pojedinih funkcija se pristupa preko padajućih menia, što omogućava korisnicima jednostavnost u radu. Kao primjer poslužit će ilustracija postupka pripreme i procne rizika, te izrada dokumenta SoA.

Određivanje popisa sve imovine relevantne za procjenu informacijske sigurnosti je jedan od početnih koraka, kako je to gore i navedeno. Na slici 4. je ilustracija kako se može definirati svaka imovina, kategorizirana prema raznim kriterijima kojima se omogućaca veća fleksibilnost u radu. Program kontrolira i dopušta definirati samo određene osobe za određene akcije vezane za funkcioniranje konkretne imovine. Kriterij za to je unaprijed definirana kompetentnost pojedinaca za određene aktivnosti, kao npr, održavanje, reinstalacije programa, itd.



Slika 4. Obrada imovine za informacijsku sigurnost

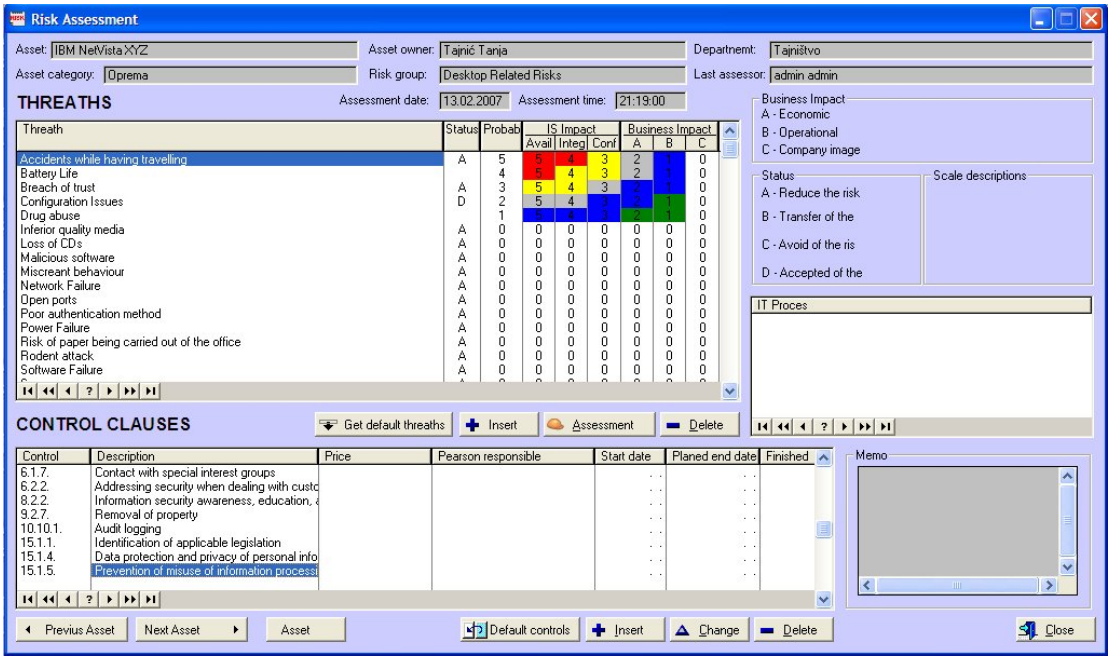
Definiranje prijetnji i dovođenje svake prijetnje s kontrolama standarda ISO17799 je slijedeći korak, koji je izuzetno važan, Za taj korak je nužno imati suradnju vrlo iskusnog stručnjaka za rizike u području informacijskih sistema. mogućnost kako se to može uraditi u programu Kestia17799 prikazan je na slici 5.



Slika 5. Identifikacija prijetnji i povezivanje s kontrolama standarda ISO17799

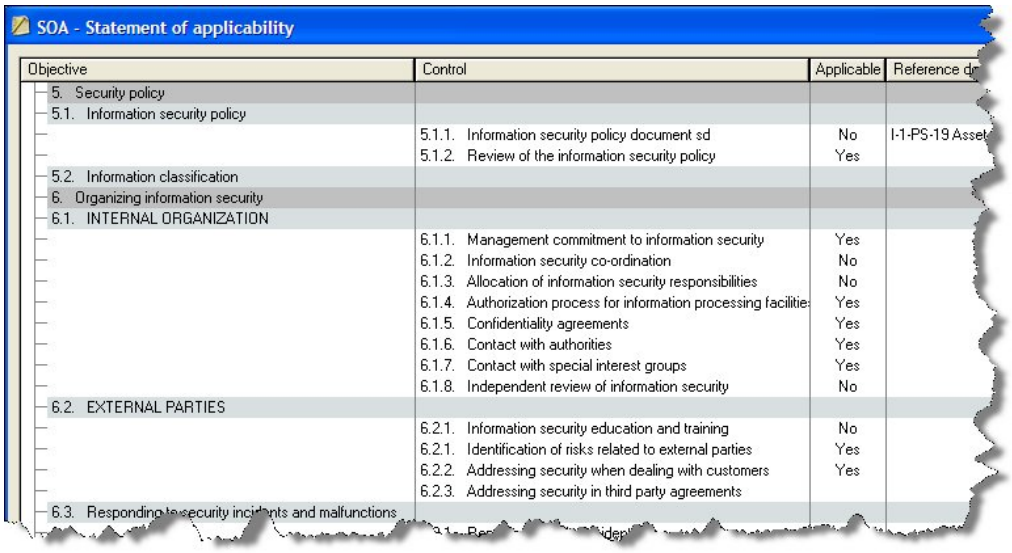
Uz neke dodatne radnje svakako je slijedeći vazan korak sama procjena rizika. Ekran preko kojega se vrši procjena rizika na imovini prikazan je na slici 6. Ekran je dosta složen na prvi pogled, ali korisniku omogućava na jednom mjestu odraditi sve potrebne korake u procjeni rizika. Za ovaj korak se također traži dovoljan nivo iskustva za rad na samoj procjeni. No, ako je priprema bila dobro napravljena u smislu selekcije prijetnji i

ostaliz releventnih veza podataka, korisnik ima relativno malo mogućnosti da napravi značajne greške u procjeni.



Slika 6. Ekran za procjenu rizika na odabranoj imovini

Po završetku rada na procjeni svakako dolazi slijedeći korak, definiranje dokumenta o primjenljivosti (SoA). Na slici 7. prikazan je primjer rada s dokumentom SoA.



Slika 7. Dokument Soa

Kako je rečeno, dokument SoA je konačni dokument nastao kao rezultat procjene rizika i podloga za odluku uprave o metodologiji i obimu implementacije ISMS u organizaciju.

Slijedeći procesni koraci nakon prihvaćanja uprave su rad na dokumentaciji, implementaciji i obuci. Na kraju cijelog projekta je certifikacijski audit. treba reći da mnoge organizacije ne idu do kraja s certifikatom, jer procjenjuju da im je dovoljan neki zamišljen nivo uspostave informacijske sigurnosti.

Sv te slijedeće korake je relativno jednostavnije uraditi, posebno se se osnovna ideja uspostave informacijske sigurnosti temelji na najboljoj praksi, a ne na izmišljanju originalnih riješenja. Npr. zna se šta je najbolja praksa npr. za zaštitu e-mail servisa u organizaciji. Pitanje je samo s kojom tehnologijom organizacija raspolaže za takav posao i koliko je sprema investirati poboljšanje ako je potrebno.

Naravno da sam prigram Hestia17799 pruža mogućnosti i te obrade te povezivanje sa svjetskim bazama znanja u području informacijske sigurnosti za preuzimanje najbolje prakse.

Zaključak

Svi koji su barem jednom radili na implementaciji ISMS prema normi ISO17799 svjesni su činjenice o izuzetnoj složenosti postupka, potrebi velikog znanja i iskustva u definiranju optimalnih politika i specifičnih procedura, kao i cjelokupnoj organizaciji uspostave, te kontroli konzistentnosti propisanih postupaka i zadanih podataka. Program Hestia17799 predstavlja kvalitetno rješenje koje na stol korisniku donosi alat kojim se poslovi implementacije ISMS bitno pojednostavljuju. Program je riješen tako da omogućava timski rad i stalno obogaćivanje baze znanja novim iskustvima i saznanjima koja su dokazana u svjetskoj praksi rada ISMS.

Literatura:

1. ISO/IEC 17799:2005, Information technology - Security techniques - Code of practice for information security management
2. ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems – Requirements
3. ISO/IEC 13335-1:2004, Information technology . Security techniques . Management of information and communications technology security . Part 1: Concepts and models for information and communications technology security management
4. ISO/IEC TR 13335-3:1998, Information technology . Guidelines Part 3: Techniques for the management of IT security
5. ISO/IEC TR 13335-4:2000, Information technology . Guidelines for the management of IT Security. Part 4: Selection of safeguards
6. ISO/IEC TR 18044:2004, Information technology . Security techniques . Information security incident management
7. Alan Calder and Steve Watkins: IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799 - 3rd Edition, ISBN: 0749444142, Publisher: Kogan Page
8. Alan Calder: Nine Steps to Success An ISO 27001 Implementation Overview, ISBN 1-905356-10-2, IT Governance Publishing
9. Robert Buchanan: Disaster Proofing Information Systems, ISBN: 007140922X, McGraw-Hill (November 2002)
10. Erik Thomsen: OLAP Solutions: Building Multidimensional Information Systems, ISBN: 0471400300, Publisher: John Wiley & Sons, Inc.
11. Warren G. Kruse II, Jay G. Heiser: Computer Forensics : Incident Response Essentials, ISBN: 0201707195, Publisher: Addison-Wesley Professional
12. Chris Prosise, Kevin Mandia: Incident Response: Investigating Computer Crime, ISBN: 0072131829, Publisher: McGraw-Hill Companies
13. Gerald L. Kovacich: The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, ISBN: 0750698969, Publisher: Butterworth-Heinemann
14. Charles Sennewald: Security Consulting, ISBN: 0750696435, Publisher: Butterworth-Heinemann, 2 edition

Objavljeno: „KVALITET" – Poslovna politika, Broj 1-2, 2007. ISSN 0354-2408