OCJENA RAZINE USKLAĐENOSTI SIGURNOSTI POSLOVNOG SUSTAVA SA NORMOM ISO 27001/2
EVALUATION OF INFORMATION SECURITY MANAGEMENT SYSTEM CONFORMITY WITH AN ISO 27001/2

Zoran Ćosić, *Statheros d.o.o. Kaštel Stari, Hrvatska*
Marija Boban, *Sveučilište u Splitu*, *Pravni Fakultet, Split, Hrvatska*

Sadržaj - *U modernom poslovnom okruženju, zahtjevi i očekivanja kupaca i zainteresiranih strana za boljim i kvalitetnijim proizvodima i uslugama se neprestano povisuju. S tim rastu očekivanja i potrebe za informacijama kao pokretačkim snagama svake organizacije. Kod korisnika se povećava potreba za osiguravanjem raspoloživosti, povjerljivosti i cjelovitosti informacija, koje se pojavljuju u najrazličitijim oblicima. S ovisnošću o informacijskim tehnologijama povećavaju se i prijetnje i ranjivosti, kojima su izloženi informacijski izvori, što neupitno utječe ne povećanje informacijskih rizika. Značajka sustava upravljanja sigurnošću informacija je u upravljanju rizicima. Sama provedba ocjenjivanja rizika organizaciji omogućuje prepoznavanje rizika s kojima se susreće. Upravljanje rizicima označava odabir i uvođenje primjerenih sigurnosnih kontrola i mjera kojima se rizici smanjuju na prihvatljivu razinu.*

Abstract -*In the modern business environment, requirements and expectations of customers and stakeholders for quality concerning products and services are constantly growing. Accordingly, need for information as a driving force of any organization are also increasing. This policy is leading to the new point of view on the need for ensuring the availability, confidentiality and integrity of information that appears in various forms. Modern information technologies and their introduction into business processes present „the main source" of threats and vulnerabilities which undoubtedly have affect in high level of information risks. The authors see the feature of information security management is risk management. The implementation of risk assessment in the organization helps to identify the risks they face. Risk management denotes the selection and implementation of appropriate security controls and measures to reduce risks to an acceptable level in order to prevent security risks and security threats.*

Ključne riječi: business environment, information security, ISO 27001, ISO 27002, availability, confidentiality, integrity, information technologies, threats, vulnerabilities, information risks, security controls

1. UVOD

U modernom poslovnom okruženju[1], zahtjevi i očekivanja kupaca i zainteresiranih strana za boljim i kvalitetnijim proizvodima i uslugama neprestano rastu. Samim tim rastu očekivanja i potrebe za informacijama kao pokretačkim snagama svake organizacije. Kod korisnika se povećava potreba za osiguravanjem raspoloživosti, povjerljivosti i cjelovitosti informacija, koje se pojavljuju u najrazličitijim oblicima. S ovisnošću o informacijskim tehnologijama povećavaju se i prijetnje i ranjivosti, kojima su izloženi informacijski izvori, što neupitno utječe ne povećanje informacijskih rizika.

Značajka sustava upravljanja sigurnošću informacija je u upravljanju rizicima. Sama provedba ocjenjivanja rizika organizaciji omogućuje prepoznavanje rizika s kojima se susreće. Upravljanje rizicima označava odabir i uvođenje primjerenih sigurnosnih kontrola i mjera kojima se rizici smanjuju na prihvatljivu razinu.

Eksplozivni razvoj informacijskih sustava[2] tijekom zadnjih nekoliko desetljeća doveo je posredno i/ili neposredno i do snažnog razvoja ostalih područja ljudske djelatnosti , kao što su tehnika, medicina, izdavaštvo, baze podataka, a naročito komunikacije. Primjena informacijskih sustava u ostalim ljudskim djelatnostima toliko je snažna da je praktički danas nezamislivo njihovo postajanje bez rada informacijskog sustava. Niz prednosti primjene informacijskih sustava u životu ljudi ogleda se u neslućenim mogućnostima obrade i proračuna podataka, pretraživanja, arhiviranja te komuniciranja. To je naravno imalo za posljedicu bitno povećavanje složenosti informacijskih sustava, koncepcijskih i tehničkih rješenja te ogromnog uvećanja broja ljudi koji rade neposredno s informacijskom tehnologijom. Svaki takav složeni sistem podložan je značajno propustima, i greškama u implementaciji, radu kao posljedica nedovoljne obučenosti korisnika, nekvalitetne izrade informacijskih sustava, ili neodgovornog rada tijekom uporabe od strane korisnika. No, pored tih problema u radu, evidentni su i problemi zlonamjernih napada od vanjskih

[1] Sigurnost informacija po normi ISO/IEC 27001 – Jože Knez, Goran Budiselić

[2] http://www.kvalis.com/index.php?option=com_content&view=article&id=162:sigurnost-informacija-imperativ-opstanka&catid=86:isms-informacijska-sigurnost&Itemid=476

faktora, koji imaju za cilj unijeti zbrku u rad informacijskog sustava, neovlašteno prikupljanje podataka, te u krajnjoj mjeri i funkcionalno uništenje informacijskog sustava
Sustav upravljanja sigurnošću informacija po zahtjevima norme ISO/IEC 27001/27002 sadrži glavne elemente odnosno zahtjeve kao i ostali sustavi upravljanja kvalitetom, okolišem i sigurnošću na radu. Zahtjevi najvažnijih elemenata, kao što su: upravljanje dokumentima i zapisima, odgovornost uprave, unutrašnje prosudbe, upravina ocjena i neprekidno poboljšavanje, uključujući preventivne i korektivne radnje, nema smisla (unutar iste organizacije) voditi odvojeno jer se međusobno dopunjuju i tvore jedinstven sustav upravljanja.
Zbog svoje univerzalne primjenljivosti i sveobuhvatnosti isti je standard opće prihvaćena u svijetu, a ISO organizacija ju je također prihvatila kao svoj standard, pod oznakon ISO27002. Prva verzija norme ISO27002 objavljena u prosincu 2000. god. Slijedeći značajan događaj u daljnjem razvoju norme za upravljanje sa sigurnošću informacija je bio koncem 2005. god. Kada je organizacija ISO donijela najnoviju reviziju norme 27002:2005, te usvojila novi norma 27001:2005, koji je u stvari potekao os norme BS7799-2.

2. PRISTUP OCJENAMA USKLAĐENOSTI

Ocjena sukladnosti ISMS[3] predstavlja proces prikupljanja dokaza i procjene usklađenosti sa zahtjevima standarda na temelju kojih se može procijeniti uspješnost informacijskog sustava. Ocjena sukladnosti informacijskih sustava, na mnogim tržištima vrlo mlada struka, nastala isprva kao potpora reviziji financijskih izvještaja, , osim egzaktne, analitičke, danas predstavlja i modernu savjetodavnu funkciju, desnu ruku koja menadžmentu pomaže pri korporativnom upravljanju. Ocjena sukladnosti informacijskih sustava predstavlja stoga sustavan postupak kojim se ocjenjuje djeluje li informacijski sustav u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama. Objekt[4] ocjene sukladnosti informacijskih sustava jest sustavna, temeljita kontrola svih dijelova informacijskog sustava, a osnovni zadatak je procijena njegovog trenutnog stanja, zrelosti, razine uspješnosti, otkrivanje rizičnih područja, razine rizika te davanje preporuke menadžmentu za poboljšanje prakse njegova upravljanja Ocjena sukladnosti informacijskih sustava je upravljačka organizacijska funkcija koja omogućuje njegovu neovisnu i objektivnu provjeru uspješnosti (zrelosti), odnosno analizu i provjeru funkcija, ciljeva i dijelova informacijskog sustava kako bi se prikupili dokazi koji se mogu neovisno razmatrati ili biti dobrom podlogom za ostale vrste ocjene sukladnosti.

2.1 GAP analiza

GAP analiza predstavlja alat za procjenu poslovnih resursa kako bi se usporedila njihova trenutačna iskorištenost ili angažiranost u odnosu prema planiranom potencijalu. Prema tome, odgovorom na pitanja gdje se trenutačno nalazi stanje informacijske sigurnosti tvrtke te koji nivo sigurnosti se želi postići moguće je dobiti u potpunosti ili djelomično odgovor na pitanje da li se isplati investirati u određeni segment informacijske sigurnosti. U poslovnom kontekstu, GAP analiza se koristi i u klasifikaciji funkcionalnosti određenih kontrola koje se koriste u informacijskoj znanosti, te se one klasificiraju kao odgovarajuće, prosječne ili neodgovarajuće . Cilj GAP analize je identifikacija raspona neusklađenosti ili jaza između trenutnog stanja sustava i optimalnog stanja sustava u kojem sustav ima najbolje performanse.

2.2. CobiT

CobiT[5] (engl. CobiT – Control Objectives for Information and Related Technologies) je svjetski prihvaćen okvir unutar kojega se propisuju područja i pojedinačne kontrole za upravljanje informacijskim sustavima i pripadajućim informatičkim procesima.
Autor CobiT okvira je ISACA (Information System Audit and Control Association, www.isaca.org) i ITGI (IT Governance Institute, www.itgi.org).
Izvorno (CobiT v1 iz 1996.) nastao kao alat za podršku provedbe ocjene sukladnosti financijskih izvještaja, CobiT se vrlo brzo razvijao i pratio razvoj uloge informatike u poslovanju (CobiT v2 iz 2000. već je u svjetskim razmjerima postao najkorišteniji okvir kontrole informacijskih sustava, verzija 3 iz 2004. godine je predstavljala integralni okvir upravljanja informatikom, a trenutno važeća verzija – CobiT 4.1 predstavlja najvažniji okvir provedbe koncepta korporativnog upravljanja informatikom). CobiT sadrži 4 područja, 34 ključna informatička procesa (cilja kontrole), preko 300 detaljnih informatičkih kontrola, 18 aplikacijskih i 6 procesnih kontrola.

2.3. Auditing

Opća definicija audita[6] jeste da je audit sistematičan, neovisan, dokumentiran, planiran i svrsishodan proces prikupljanja objektivnih dokaza o sukladnosti sustava te evaluacija osoba, organizacije, procesa, poduzeća, projekta ili proizvoda. Auditi se provode radi osiguranja vrijednosti i pouzdanosti informacija i dokumenata koji svjedoče o postojanju nekog sustava.
Cilj audita je utvrđivanje sukladnosti sa propozicijama nekog zahtjeva, standarda itd. Proces auditiranja provodi se po zahtjevima norme ISO 19011 koja daje smjernice o metodologiji provedbe auditinga i kompetencijama auditora. Auditor je osoba kompetentna za provođenje audita koja bi trebala imati sljedeće osobine:

- ✓ Etičnost
- ✓ Istinoljublje
- ✓ Profesionalnost
- ✓ Neovisnost
- ✓ Pristup zasnovan na dokazima

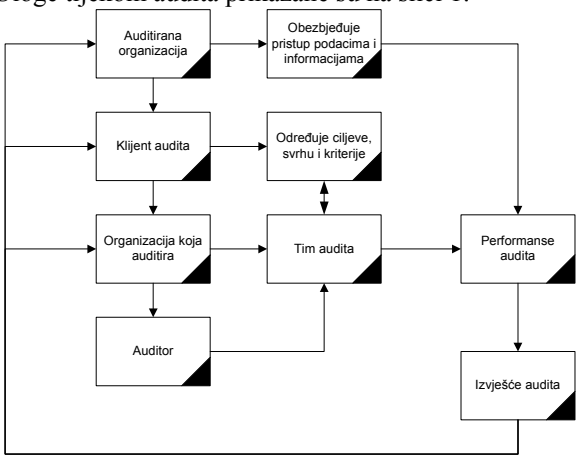
[3] Informational Management system; ISO 27001/2
[4] Prof.dr.sc Mario Spremić – Metode provedbe ocjene sukladnosti informacijskih sustava , prethodno priopćenje UDK 007:65.012.16
[5] Prof.dr.sc Mario Spremić – Metode provedbe ocjene sukladnosti informacijskih sustava , prethodno priopćenje UDK 007:65.012.16
[6] Audire- lat. slušati

3. AUDITING[7] ISMS PO NORMI 19011:2002[8]

Proces provedbe audita definiran opsegom ISMS-a po normama ISO 27001/2[9], tehnika auditiranja je sistematično traženje dokaza o sukladnosti. Audit ima svoju definiranu strukturu, zaduženja i raspored zadataka. Nemoguće bi bilo auditirati svaku pojedinu aktivnost, odluku, dokument, proces i sl. te se istražuju samo odabrani aspekti, najčešće metodom slučajnog uzorka odabrani u toku samog audita. Ipak, i pored toga, potrebno je obuhvatiti sva područja koja zahtijeva norma.

U mnogim područjima stvari će funkcionirati vrlo dobro i efikasno, ali u procesu audita bitno je ono suprotno: dokazi o nesukladnostima prema normi. Zato vrijedi pravilo da je sustav u skladu s normom sve dok se ne pronađe ono što je u nesukladnosti. U slučaju nedostatka informacija, odluka o tome da li je sustav sukladan ili ne, pada na leđa auditora.

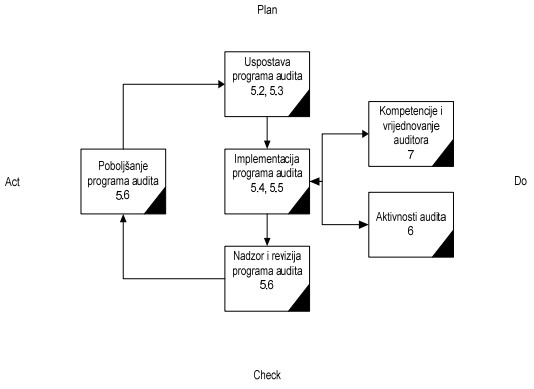
Uloge tijekom audita prikazane su na slici 1:



Slika 1

3.1 Planiranje audita

Prije same ocjene sukladnosti voditelju audita se predaje dokumentacija o samom ISMS-u, najšešće Poslovnik ISMS i dokument Izjava o primjenjivosti[10]. Na slici 2 dan je grafički prikaz uloga tijekom procesa auditinga.



Slika 2

Planiranje audita provodi se sukladno PDCA[11] ciklusu koji predviđa:

- ✓ -Izradu plana kroz planiranje aktivnosti i organizacijskih cjelina koje su predmet audita
- ✓ -Implementacija plana kroz odabir auditora i verifikaciju kompetencija
- ✓ -eventiualna revizija plana i njegovo poboljšanje.

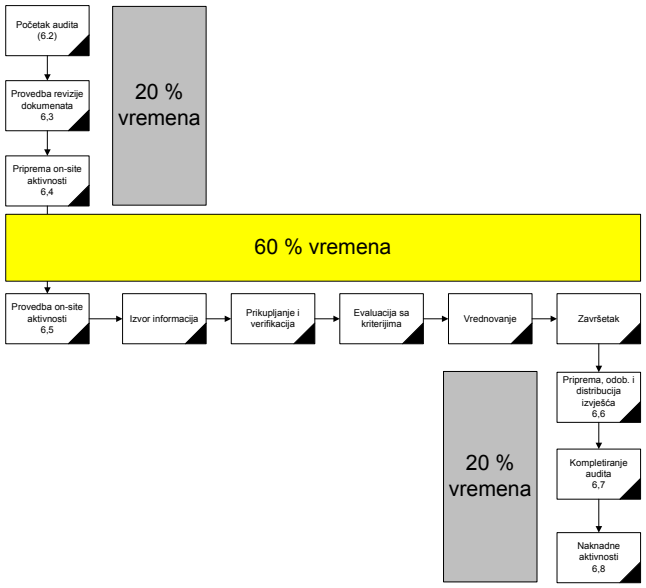
3.2 Provedba

U svakom trenutku, voditelj ocjene sukladnosti mora voditi računa o tome da li se ocjena sukladnosti odvija u skladu s programom ocjene sukladnosti. Jedna od najbitnijih osobina auditora je da mora znati dobro upravljati vremenom. Izvođenje ocjene sukladnosti traži puno vremena, ne samo intervjuiranje osoba, već i vrijeme potrebno da se do njih dođe i da se zabilježe pozitivni i negativni nalazi. Često sugovornici mogu biti raspoloženi za priču te, svjesno ili nesvjesno, odvesti intervju u sasvim drugom pravcu i time potrošiti vrijeme da se prođe kompletna kontrolna lista pitanja.

Osim toga, intervjuirane osobe često ne mogu odmah odgovoriti na sva postavljana pitanja pa ili traže odgovore od drugih osoba ili pretražuju svoje dokumente. U procesu intervjuiranja, auditoru će puno pomoći iskustvo pri procjeni koliko dugo može trajati pojedini intervju. Isto se odnosi i na pregled lokacije ili dokumentacije.

Uspoređujući zapaženo sa zahtjevima norme ISO 27001, moguće je naći nesukladnosti koje, objektivno, mogu biti manje ili veće. Ukoliko se pronađu takve nesukladnosti, potrebno ih je raspraviti s intervjuiranom osobom, kako bi se izbjeglo moguće krivo subjektivno tumačenje auditora. Auditor obično ukazuje na pojavu nesukladnosti, ali nije nužno dati odmah preporuku za njeno otklanjanje.

Slika 3 prikazuje provedbu audita:



Slika 3

[7] Procjena razine usklađenosti sigurnosti poslovnog sustava sa ISO 27002 normom - Seminarski rad, Zoran Ćosić, doktorski studij FOI Varaždin, 2009

[8] http://www.iso.staratel.com/ISO19011/Doc/ISO190112002/ISO19011_eng.pdf

[9] http://www.27000.org/iso-27001.htm; http://www.27000.org/iso-27002.htm

[10] Statement of applicability- ISO/IEC 27001

[11] Plan, do, check, act

3.3 Rezultat audita i izvješćivanje

Završno izvješće audita treba predstavljati sistematičan zapis ocjene sukladnosti, opsega, nalaza i zaključaka. Ovo izvješće je namjenjeno Upravi organizacije koja ne mora nužno biti detaljno upoznata s aktivnostima na području informacijske sigurnosti. Radi toga je bitno da izvješće bude uravnotežena slika kompletnog procesa ocjene sukladnosti, a ne samo popis nesukladnosti.
U izvješću se svakako treba nalaziti popis osoba koje su bile intervjuirane, ali zavisno o zahtjevima organizacije, na popisu ne moraju biti svi s kojima su auditori razgovarali ili ih anketirali. Pored popisa osoba, izvješće sadrži i program ocjene sukladnosti koji je usuglašen na početnom sastanku. Središnji dio izvješća svakako sadrži nalaze ocjene sukladnosti – popis nesukladnosti.

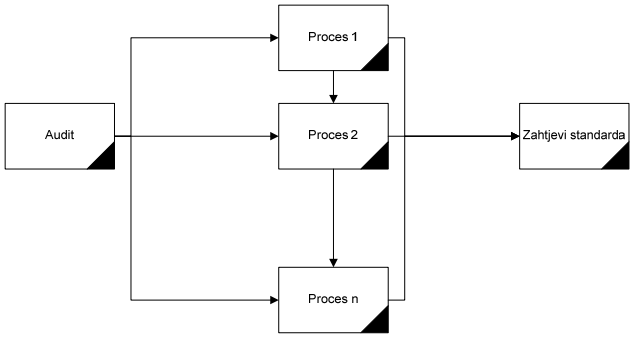
4. OCJENA RAZINE USKLAĐENOSTI

Ocjena razine sukladnosti metodologijom auditinga provodi sukladno sljedećim pristupima:

- ✓ Procesno orjentirani pristup
- ✓ Normativno orjentirani pristup

4.1 Procesno orjentirani pristup

Polazi od zakonitosti i logike poslovnih procesa organizacije i traži sukladnost sa zahtjevima standarda ISO 27001/27002. Slika 4 prikazuje procesni pristup auditinga.



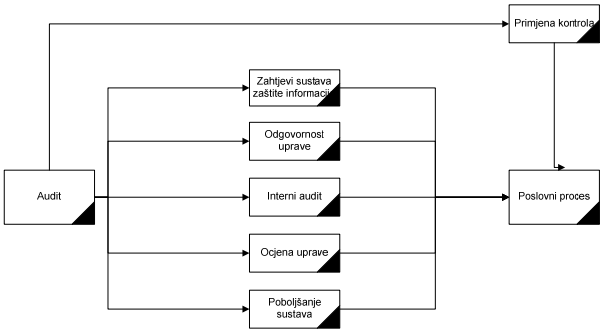
Slika 4

U procesno orjentiranom pristupu audita polazi se od identificirani poslovnih procesa korz čiji se tijek verificira usklađenost sa zahtjevima norme. Procesno orjentirani pristup se najviše koristi prilikom izvedbe audita.

4.2 Normativno orjentirani pristup

Za ovakav pristup karakteristično je da se polazi od pojedinih zahtjeva standarda koji se verificiraju kroz različite poslovne procese. Kod ovakvog pristupa nije moguće obezbjediti obuhvat i kontrolu svih procesa u organizaciji.
Prilikom audita moguće je koristiti pripremljene check-liste koje olakšavaju provedbu audita i usmjeravaju auditora.

Slika 5 prikazuje normativni pristup auditinga.



Slika 5

5. ZAKLJUČAK

Ocjena usklađenosti ISMS sa normom ISO 27001/2 predstavlja neminovnost za organizacije koje žele biti pouzdan partner svojim kupcima i dobavljačima. Zakonodavstvo RH reguliralo je primjenu ISO 27001 Zakonom o informacijskoj sigurnosti (2007) te Uredbom o mjerama informacijske sigurnosti (2008). Ona se, naime, odnosi na obvezne mjere identifikacije opasnosti, klasifikacije informacije te na sustavan postupak kojim se ocjenjuje djeluje li informacijski sustav u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama. Konačan rezultat tih postupaka jest izvještaj auditora informacijskog sustava koji se, prema područjima analize (temeljene na CobiT ili ITIL okviru ili ISO 27001 normi), sastoji od sljedećih koraka:

- ✓ analiza stanja (zrelosti) primjene informacijskih sustava u poslovanju prema promatranim područjima
- ✓ procjena poslovnih rizika koji proizlaze iz zatečenog stanja i
- ✓ preporuke menadžmentu za poboljšanjem toga stanja.

6. LITERATURA

[1] Sigurnost informacija po normi ISO/IEC 27001 – Jože Knez, Goran Budiselić
[2] Prof.dr.sc Mario Spremić – Metode provedbe ocjene sukladnosti informacijskih sustava , prethodno priopćenje UDK 007:65.012.16
[3] Procjena razine usklađenosti sigurnosti poslovnog sustava sa ISO 27002 normom - Seminarski rad, Zoran Ćosić, doktorski studij FOI Varaždin, 2009
[4] Zakon o informacijskoj sigurnosti RH 2007
[5] Uredba o mjerama informacijske sigurnosti RH 2008
[6] ISO IEC 27001:2005 Informational security management system
[7] http://www.kvalis.com/index.php?option=com_content&view=article&id=162:sigurnost-informacija-imperativ-opstanka&catid=86:isms-informacijska-sigurnost&Itemid=476
[8] http://www.27000.org/iso-27001.htm
[9] http://www.27000.org/iso-27002.htm