Upravljanje informacijskom sigurnošću u zdravstvu

Velibor Božić
OB „Dr. Tomislav Bardek“, Koprivnica

SAŽETAK U današnjem društvu organizacije svih profila (proizvodne, neproizvodne, javne, privatne) sve su više ovisne o informacijsko–komunikacijskoj tehnologiji (IKT). IKT je u tolikoj mjeri prisutan da ga korisnici često nisu niti svjesni – podrazumijeva se. Upravo takva ovisnost o IKT–u predstavlja potencijalnu opasnost za očuvanje funkcionalnosti organizacija. Postavlja se pitanje je li menadžment svjestan opasnosti od mogućih incidenata i problema u radu IKT–a. Postoji li svijest o opasnosti od nedostupnosti IKT–a (kultura rizika) ili nastanka neželjenih događaja vezanih uz IKT. Postoji li sustavan pristup identifikaciji prijetnji, otkrivanju ranjivosti, procjenjuje li se važnost ostvarenih prijetnji na poslovanje. Postoji li svijest da IKT ima određenu vrijednost koja utječe na učinkovitost i djelotvornost poslovanja. IKT–imovina bi se, naime, trebala tretirati kao i sva ostala imovina, te je potrebno poduzimati preventivne i korektivne radnje (sustav kontrole) kako bi se smanjila opasnost od uništenja ili zloporabe IKT–a.

KLJUČNE RIJEČI informacijski sustavi; rizik; upravljanje rizicima; zdravstveni sektor

Živimo u 21. stoljeću u kojem je organiziranje u najširem smislu, tj. organizacija kao nositelj zajedničkog djelovanja niza subjekata usmjerenih zajedničkom cilju (proizvodne, neproizvodne, uslužne…) u potpunosti ovisna o komunikacijsko-informacijskoj tehnologiji (IKT), htjeli to priznati ili ne. Njezina opstojnost u potpunosti ovisi o učinkovitom i djelotvornom IKT-u. Potpuna ovisnost veže uz sebe i rizike poslovanja. Rizici promatrani kao kombinacija vjerojatnosti pojave nekog događaja i utjecaja tog događaja na poslovanje mogu biti pozitivni i negativni. Primjera za takvu tvrdnju kroz povijest ima nebrojeno mnogo. Zadržimo se samo na području IKT-a. Može se postaviti pitanje bi li Bill Gates uspio da nije prihvatio rizik? S druge strane, sigurnosni propusti vezani uz Sonyjeve igraće konzole uzrokovale su velike financijske gubitke kompaniji, ali što je gore i gubitak ugleda kod korisnika. Ovo su samo dva izdvojena primjera koji potvrđuju činjenicu da rizik može imati pozitivne i negativne posljedice.

Rizik može istovremeno biti pokretač i kočničar poslovanja. On je neodvojivi dio poslovanja neke organizacije i na neki način mora se staviti pod kontrolu kako bi se mogli ostvariti poslovni ciljevi. Bilo da je riječ o proizvodnim ili neproizvodnim (uslužnim) djelatnostima, primjena komunikacijsko-informacijske tehnologije postaje kritičnim faktorom o kojem ovisi ispunjavanje strategije poslovanja, djelotvornost i učinkovitost, kao i opstojnost organizacije. Ovisnost organizacije o dobrom funkcioniranju informacijske tehnologije jest rizik sam po sebi na najvišoj razini poslovanja. Kako se suočiti s tim rizikom? Treba li ga prihvatiti, boriti se s njim ili ga ignorirati? Kakav je odnos uprave prema IT-rizicima? Jesu li vlasnici i menadžeri svjesni IT-rizika ili ne? Je li upravu moguće podučiti o načinima suočavanja s IT-rizicima?[1,2]

Postavlja se pitanje: je li moguće upravljati rizicima općenito, pa onda i u području informacijske tehnologije? Kako bi organizacija bila sposobna maksimalno iskoristiti pozitivne rizike i kvalitetno se suočiti s negativnim rizicima, neophodno je da ima znanje o upravljanju rizicima. Kvalitetno upravljanje rizicima u području informacijske tehnologije itekako je moguće. Upravljanje rizicima u području informacijske tehnologije doprinosi učinkovitosti i djelotvornosti poslovanja i ostvarivanju vizije organizacije.[1]

ZAŠTITA INFORMACIJSKIH SUSTAVA ZDRAVSTVENIH USTANOVA

Temeljni je cilj zaštite informacijskih sustava u zdravstvu zaštiti povjerljivost, dostupnost i integritet informacija o pacijentu.[3,4]

U zaštiti informacija potrebno je voditi računa o svim elementima sustava – pacijentima, javnosti, zaposlenicima, poštivanju zakona i propisa, upravi, nadzoru (upravnom vijeću). Svi sudionici sustava moraju biti na neki način zadovoljeni u kontekstu zaštite integriteta, te zaštite i dostupnosti informacija. Prilikom zaštite podataka potrebno je voditi računa o riziku.

Rizici sigurnosti podataka. Na povjerljivost, dostupnost i integritet informacija mogu utjecati mnogi faktori koji proizlaze iz ranjivosti sustava. Rizik nastaje zbog prijetnje sigurnosti koja proizlazi iz ranjivosti sustava i zbog razmjera posljedica po sustav koju ta prijetnja može prouzročiti.[5] Zaštitom informacijskih sustava rizik se mora smanjiti na prihvatljivu mjeru.

Bit upravljanja zaštitom informacijskih sustava (o čemu se tu radi?) Povjerljivost, dostupnost i integritet informacija izloženi su riziku. Na povećanje rizika izravno utječu prijetnje po sigurnost sustava. Prijetnje se temelje na ranjivosti sustava. Ranjivost sustava omogućuje izloženost imovine sustava riziku (informacija, u ovom kontekstu). Imovina sustava ima određenu vrijednost koja utječe na cjelokupnu organizaciju.

Rizik izravno utječe na vrijednost imovine tako što je umanjuje. Organizacija (u ovom slučaju bolnica, odnosno zdravstvena ustanova) ima određene sigurnosne zahtjeve. Ti sigurnosni zahtjevi se ispunjavaju kroz određene kontrole. Kontrole su ključne u smanjivanju rizika (zadovoljavanje zahtjeva za povjerljivošću, dostupnošću i integritetom informacija). Kontrole pomažu zaštiti protiv prijetnji po sustav. Time je krug zaštite sustava zatvoren.

Faktori rizika u medicinskim ustanovama uključuju medicinske faktore (npr. liječničke pogreške, bolničke infekcije…), financijske faktore (nekontrolirana zaduživanja/plaćanja, pogrešno upravljanje troškovima, loš financijski menadžment…), regulatorne faktore (nepoštovanje zakona, propisa, direktiva…). U medicinskim ustanovama postoji veliki rizik od nedostupnosti podataka, neovlaštenog pristupa podacima, neovlaštenog mijenjanja podataka. Kako bi se svi ti rizici sveli na prihvatljivu razinu, potrebno je upravljati rizicima. Tri su osnovna mehanizma za upravljanje rizicima:

- BSC (*Balanced Scorecard*) – strateška razina (BSC/4A matrica)[6,7]
- COBIT 4.1 + IT Risk (COBIT 5.0) – taktička razina (kontrolni ciljevi grupiraju se u jedan od A (*access, availability, accuracy, agility*) u tzv. 4A pristupu)
- ISO 27799:2008 – operativna razina – konkretne aktivnosti.[8,9]

ULOGE KOD UPRAVLJANJA RIZICIMA

Uloga uprave (ravnateljstva u bolnici) kod upravljanja rizikom:[10-12]

- procjena prirode rizika i definiranje razine do koje se razina rizika mora smanjiti kako bi bio prihvatljiv za poslovanje
- procjena vjerojatnosti pojave rizika
- određivanje načina upravljanja s neprihvatljivim rizicima
- definiranje sposobnosti poduzeća da minimalizira vjerojatnost pojave prijetnji i njihovog utjecaja na poslovanje
- identificiranje troškova i koristi od rizika te određivanje kontrolnih aktivnosti
- definiranje kriterija za mjerenje učinkovitosti borbe protiv rizika
- razmatranje utjecaja rizika na odluke uprave.

Uloge izvršnih direktora (članovi stručnog vijeća u bolnici):

- odgovornost za dnevno provođenje upravljanja rizikom
- širenje svjesnosti o riziku unutar područja kojim rukovode
- upoznavanje zaposlenika s ciljevima upravljanja rizicima
- osiguravanje modela da upravljanje rizikom postane jednakopravna tema sa svim ostalim temama na sastancima menadžmenta
- uključivanje upravljanja rizikom u bilo koji od projekata kao jedne od njegovih faza bez koje ne može biti uspješno realiziran.

Osim navedenih uloga, uprava i izvršni direktori zajednički imaju ulogu osigurati djelotvorno i učinkovito upravljanje rizikom:

- usvojiti politiku i strategiju upravljanja rizikom
- definirati upravljanje rizikom na strateškoj i operativnoj razini
- stvoriti kulturu svjesnosti postojanja rizika u poduzeću
- osigurati procese nadgledanja rizika
- koordinirati aktivnosti u poduzeću koje su povezane s upravljanjem rizikom
- razvijati odgovore na rizik (što napraviti ukoliko se rizik ostvari – programi kontinuiteta poslovanja)
- pripremiti izvješća o rizicima prema vlasnicima i svima ostalima koji su zainteresirani za poslovanje.

Za učinkovito upravljanje rizicima u poduzeću potrebno je osigurati internu kontrolu. Uloge interne kontrole:

- kontroliranje upravljanja kritičnim rizicima (koje identificira menadžment)
- ukazivanje na eventualne propuste u procesu upravljanja
- pomoć kod identifikacije rizika
- koordiniranje izvješća o riziku prema upravi i vlasnicima

BALANCED SCORECARD (URAVNOTEŽENA KARTA REZULTATA)

Kaplan i Norton predstavili su ideju BSC-a (*Balanced Scorecard*) u siječnju/veljači 1992. godine.[13] Potreba za takvim alatom značila je priznanje da mjerenje samo financijskih rezultata nije dovoljno za upravljanje modernom organizacijom. Većina posla koji se danas radi u organizacijama ne bi se trebala odnositi samo na obradu financijskih rezultata – puno više pažnje trebalo bi usmjeriti na ostvarenje unapređenja procesa, trening zaposlenih, iznalaženje novih načina povezivanja s kupcima. Može se reći da su te aktivnosti kamen temeljac uspješne organizacije. One omogućavaju efikasnije upravljanje tako što pomažu ostvarenju strategije poslovanja. Izostanak sustava mjerenja koji reflektira uravnoteženi pogled na organizacijske ciljeve mogao bi se usporediti s vožnjom automobila gledajući u stražnje ogledalo ili s upravljanjem avionom gledajući samo na mjerni uređaj za mjerenje visine.[13]

U osnovnoj verziji BSC uključuje četiri vrste pogleda na organizaciju (perspektive): financije, kupci, interni poslovni procesi te učenje i razvoj. Neke organizacije dodaju još i peto područje ili zamjenjuju sve perspektive s jednom jedinom koja je jedinstveni odraz njihove misije i strategije. Naprimjer, neke organizacije dodaju dimenziju okruženja njihovoj karti rezultata. Ipak, četiri perspektive koje su definirali Kaplan i Norton općenito su primjenjive u različitim organizacijama.

Primjer primjene BSC-a na bolničko okruženje:

- P acijenti
  - Povećanje zadovoljstva pacijenata – brža reakcija, skraćivanje tretmana, izbor medicinskih metoda liječenja, postojanje informiranih pristanaka, bolja zaštita informacija
- Financije
  - Rast – pravovremenost financiranja (dotok sredstava potrebnih za funkcioniranje zdravstvenih ustanova)
  - Profitabilnost – učinkovite i troškovno isplative aktivnosti
  - Likvidnost – analiza faktora koji određuju tijek novca, bolja kontrola opreme i usluga koje utječu na fiksnu imovinu
  - Stabilnost – bolja kontrola troškova rada
- Interni procesi
  - Povećanje kvalitete medicinskih usluga – stvaranje standardiziranih medicinskih postupaka, istraživanja i analize problema
  - Upravljanje medicinskim rizicima – praćenje medicinske prakse, postojanje slijedivosti (od nabave materijala i lijekova pa sve do administracije), minimiziranje medicinskih pogrešaka
  - Unapređenje poslovnih procesa – pojednostavljivanje i ubrzavanje procesa te odvajanje profesionalnih i standardiziranih procesa
  - Upotreba informacija – dijeljenje informacija po principu „neophodan dio informacije, onomu kome zaista treba“
- Učenje i razvoj – Što učiti da bi se postigao razvoj?
  - Unapređenje profesionalnosti osoblja
  - Optimizacija uloga i odgovornosti
  - Kontinuirana edukacija

BSC predstavlja opširan pregled funkcioniranja poslovnog sustava koji nije temeljen samo na tradicionalnim financijskim mjerama. To je samo dio novosti u BSC-pristupu. Stvarna korist BSC-pristupa je da se stvori tabela rezultata koja otkriva pretpostavke za dobro poslovanje. Strategija će pokazati da akcije u području učenja i rasta utječu na unapređenje internih poslovnih procesa koji će ispuniti posebne ciljeve kupaca i time utjecati na financijski rezultat. BSC afirmira uravnoteženi pristup u analizi poslovanja što znači da se pokušavaju sagledavati kritični faktori uspjeha u međusobnoj uzročno-posljedičnoj vezi.

Uprava definira misiju (zašto postojimo) i viziju (gdje želimo doći). Na osnovi misije i vizije definira se strategija (način kako postići viziju). Za provedbu strategije potrebno je definirati strateške ciljeve. Do njih se može doći različitim tehnikama (npr. SWOT-analiza).

Strateški ciljevi za medicinske ustanove:

- Postizanje i održavanje visoke razine sigurnosti i zaštite osobnih podataka pacijenata
- Uspostava i održavanje visoke razine medicinskih usluga
- Minimiziranje medicinskih pogrešaka
- Najbrži mogući odgovor na medicinske potrebe zajednice
- Poboljšavanje razmjene informacija između medicinskih ustanova i zajednice
- Povećanje vještina i znanja osoblja
- Identifikacija i adresiranje novih izazova
- Implementacija suradnje između elemenata zdravstvenog sustava
- Postavljanje sustava potpune podrške zdravstvenom sustavu
- Uspostavljanje bolje okoline za istraživački rad liječnika i unapređenje medicinske skrbi

Kod definiranja strateških ciljeva treba voditi računa o tome da su oni postavljeni u skladu s misijom i vizijom te da su ostvarivi, mjerljivi, realni i vremenski definirani. Za svaki strateški cilj potrebno je odrediti niz aktivnosti, tj. proces kojim se taj strateški cilj može postići. Neispunjavanje, tj. loša provedba svakog od navedenih strateških ciljeva, predstavlja strateški rizik.

Kao pregledna metoda koja upravi poduzeća (bolnice) može pomoći u definiranju i praćenju odnosa poslovnih ciljeva, rizika i utjecaja na poslovanje formulirana može se uzeti tzv. BSC/4A matrica. Popis strateških rizika poslovanja organizacije prema 4A-matrici prikazan je u tablici 1.[6,7,9,10,14]

COBIT – TAKTIČKA RAZINA

COBIT je akronim od *Control Objective for Information and related Technolgy*. Nastao je 1992. godine pod okriljem dvije organizacije: *Information Systems Audit and Control Association* (ISACA) i *IT Goverment Institute* (IGI). COBIT osigurava menadžerima, nadzornicima i IT-korisnicima skup mjera, indikatora, procesa i primjera (najbolja praksa) za maksimalno korištenje prednosti informacijske tehnologije te razvoj adekvatnog upravljanja i kontrole nad poslovnim procesima u organizacijama.

Upravo na taktičkoj razini (razina izvršnih direktora) koristi od COBIT-a su velike jer on osigurava kvalitetnu implementaciju bolničkog informacijskog sustava te upravljanje operativnim rizicima.[1,10,15]

COBIT omogućuje da IT ne bude samo donositelj IT-usluga već strateški partner u poslovanju. Njegova ključna uloga je omogućiti kontrolu svih IT-procesa, usmjeravati ih prema stalnoj provjeri i sigurnosti izvedbe. Cilj COBIT-a je upravljanje poslovnim uslugama i trebao bi riješiti tzv. IT-suficit, tj. nedovoljno iskorištavanje IT-a, a s druge strane trebao bi osigurati da IT može podržati zahtjeve poslovnog sustava (treba onemogućiti IT-deficit).

TABLICA 1. Strateški rizici poslovanja (BSC/4A-matrica)

Poslovni ciljevi	Utjecaj na posao (rizici)	4A-utjecaj na poslovanje			
		agilnost	točnost	pristup	dostupnost
Financije					
Osiguranje povrata investicija u IT	Neadekvatan financijski povrat od IT-investicija	P			
Upravljanje IT-rizicima	IT-rizicima se ne upravlja, kompanija je nesigurna	P	P	P	P
Unapređenje korporativnog upravljanja i transparentnosti	Nedovoljna transparentnost prema zainteresiranim stranama, nesukladnost s pravnom regulativom	P			
Kupci (korisnici)					
Unapređenje usmjerenosti na korisnike i usluge	Loša ili nedovoljna usluga korisnicima, gubitak klijenata		S	P	P
Ponuda konkurentnih proizvoda i usluga	Neadekvatni proizvodi i usluge ne ispunjavaju potrebe kupaca; gubitak dohotka	P	S	P	S
Postavljanje kontinuiteta i dostupnosti usluga	Nedovoljna razina usluga rezultira nezadovoljstvom kupaca i gubitkom dohotka		S	P	P
Stvaranje agilnosti u skladu s novim poslovnim zahtjevima	Nemogućnost pravovremene reakcije na promjene tržišta ili na zahtjeve kupaca donosi gubitak	P		S	
Troškovno optimiziranje isporuke usluga	Proizvodi ili usluge koji su preskupi uzrokuju nekonkurentnost i gubitak kupaca	P			
Realno i učinkovito izvješćivanje bitno je za donošenje odluka	Loše odluke na strateškoj razini rezultiraju gubitkom klijenata; gubici i pad vrijednosti organizacije	P			
Interni procesi					
Unapređenje i održavanje funkcionalnosti internih procesa	Neefikasni i nedovoljno optimizirani procesi u organizaciji		P	P	
Niži troškovi procesa	Niža profitabilnost	S			
Uskladivost sa zakonima, regulativom i ugovorima izvan organizacije	Kršenje istih rezultira krivičnom odgovornošću uprave i odgovornih		P	P	
Uskladivost s internim politikama	Neučinkoviti i neadekvatni procesi		P	S	S
Upravljanje poslovnim promjenama	Nedovoljno dobri procesi dovode do nekonkurentnosti	P			
Unapređenje i održavanje produktivnosti osoblja	Smanjenje produktivnosti i učinkovitosti	P	P		
Učenje i razvoj					
Unapređenje proizvoda i poslova	Gubitak šansi, mali rast, gubitak tržišnog udjela	P			
Pribavljanje i zadržavanje vještih i motiviranih ljudi	Nemogućnost napretka (rasta organizacije i rasta trenutnih operacija)	P	S		

P – primarni utjecaj; S – sekundarni utjecaj

COBIT podržava korporacijski IT, tj. upravljanje poslovnim procesima (eng. *IT governance*) tako što donosi okvir unutar kojeg prezentira domene, procese, aktivnosti na upotrebljiv i logičan način. Sastoji se od četiri osnovne domene i 34 procesa unutar domena. Domene su:

Planiranje i organiziranje. Ova domena odnosi se na strategiju i taktiku; tu se definira najbolji način na koji IT može doprinositi ostvarenju poslovnih ciljeva.

Akvizicije i implementiranje. Ovdje je predmet interesa realizacija strategije. Definiraju se IT-rješenja, razvijaju se i obogaćuju, implementiraju se i integriraju u poslovni proces.

Isporučivanje i podrška. Ova domena odnosi se na isporuku traženih usluga, što uključuje isporuku, upravljanje sigurnošću (rizik) i kontinuitetom isporuke,

TABLICA 2. COBIT – struktura prikaza IT-procesa

Prvi dio:
- Informacijski kriteriji (kakve informacije moraju biti)
- Koji poslovni zahtjev IT-proces zadovoljava
- Kroz ostvarenje kojih ciljeva IT-proces zadovoljava poslovni zahtjev
- Koje aktivnosti IT-proces poduzima za ostvarenje cilja
- Kako se mjeri ostvarenje cilja
- Koje poslovno područje unutar upravljanja poslovanjem IT-proces primarno obrađuje, a koje sekundarno podržava
- Koje IT-resurse proces koristi za ostvarenje cilja

Drugi dio:
- Sadrži kontrolne ciljeve za ostvarenje svrhe IT-procesa

Treći dio:
- Sadrži ulaze i izlaze iz procesa (to su aktivnosti iz različitih domena)
- Tzv. RACI-matrica koja pokazuje od kojih se aktivnosti sastoji IT-proces te tko je odgovoran za pojedinu aktivnost, na koga se računa, tko se konzultira, a tko informira; *Responsible, Accountable, Consulted, Informed*
- U RACI-matrici vide se i funkcije koje su potrebne za ispunjenje svrhe IT-procesa (uprava, šef informatike, izvršni direktor, poslovođa, djelatnik, voditelj projekta...)
- Ciljevi u hijerarhijskom odnosu i metrike za mjerenje ostvarenja

Četvrti dio:
- Model zrelosti IT-procesa prema CMM-modelu

TABLICA 3. Procesi unutar COBIT-a koji se koriste kod upravljanja rizicima

Planiranje i organizacija
- komuniciranje upravljačkih ciljeva i direktiva kroz organizaciju
- upravljanje ljudskim resursima
- procjena i upravljanje IT-rizicima
- upravljanje projektima

Nabava i implementacija
- identifikacija automatiziranih rješenja
- omogućavanje operacija i upotrebe
- instalacija i akreditacija rješenja i promjena

Razvoj i podrška
- definiranje i upravljanje razinom usluga
- upravljanje izvedbom i kapacitetom
- osiguranje kontinuiranog servisa
- osiguranje sigurnosti sustava
- edukacija i trening korisnika
- upravljanje podacima
- upravljanje fizičkom okolinom

Nadzor i ocjenjivanje
- pravilno mjerenje i ocjenjivanje procesa

podršku za uslugu prema korisniku, upravljanje podacima i operativne usluge.

Nadzor i ocjenjivanje. Svaki je IT-proces potrebno kontrolirati: radi li prema korisničkim zahtjevima. U okviru te domene upravlja se izvedbom, nadgleda se interna kontrola i reguliraju se procesi.

Kroz te četiri domene i 34 procesa u okviru tih domena, COBIT ostvaruje svoju svrhu, a to je podrška ostvarenju poslovnih usluga. No, osim što je usmjeren na procese, COBIT je fokusiran na djelatnost, usmjeren na kontrolu i vođen mjerenjem uspješnosti ostvarenja ciljeva i procesa. Fokusiranje COBIT-a na djelatnost znači da on nije alat samo za donositelje IT-usluga, korisnike i kontrolore, već on predstavlja jasan vodič menadžerima i vlasnicima poslovnih procesa. To je činjenica jer su kvalitetne informacije ključne za odlučivanje, a upravljanje i kontrola informacija srž su COBIT-a. COBIT osigurava da informacije budu učinkovite, djelotvorne, povjerljive, ukoliko je to potrebno, te dostupne, zakonite, sigurne i provjerene. COBIT je usmjeren na kontrolu i to kroz kontrolne ciljeve kojima se osigurava kvalitetno odvijanje svakog od 34 procesa. Osim ciljeva koji se odnose samo na određeni proces, postoje i globalni ciljevi koji se istovremeno odnose na sve procese u svim domenama. Unutar COBIT-a primjenjuje se mjerenje uspješnosti ostvarenja ciljeva i procesa. Konkretno, primjenjuje se CMM-model određivanja razine zrelosti određenog IT-procesa kako bi se odredilo stanje u kojem se proces trenutno nalazi, kao i potreba za unapređenjem. Postoji početna razina i pet daljnjih faza zrelosti. To su: inicijalna/*ad hoc* faza, ponavljajuća ali intuitivna, definirani proces, upravljiva i mjerena te optimizirana faza.

Osnovni COBIT-princip je sljedeći: na osnovi poslovnih zahtjeva pokreću se investicije u IT-resurse. IT-resursi se koriste u IT-procesima. IT-procesi isporučuju informacije o poslovanju. Te informacije o poslovanju odgovaraju na zahtjeve korisnika.

Kroz taj princip COBIT podržava osnovna područja upravljanja poslovanjem:

Strateško poravnavanje (veza između poslovnog i IT-plana; definiranje, održavanje i vrednovanje IT-vrijednosti, usklađivanje IT-a i poslovnih operacija),

Isporuka vrijednosti (osiguranje da IT isporučuje informacije vrijedne za poslovanje, a u skladu sa strategijom),

Upravljanje resursima (optimalno investiranje u resurse*),

Upravljanje rizikom (zahtjeva se svjesnost postojanja rizika od strane menadžmenta, razumijevanje potrebe da rizika mora biti, dogovor oko značajnog rizika, definiranje odgovornosti za rizike u organizaciji).

Mjerenje izvedbe (prati implementaciju strategija, izvođenje projekata, upotrebu resursa, izvođenje procesa i isporuku IT-usluga; za praćenje se koristi BSC).

Koncept cilja u COBIT-u je od ključne važnosti. Tu postoji hijerarhija ciljeva. Na najvišoj razini je poslovni cilj. On se ostvaruje kroz IT-ciljeve. Svaki IT-cilj realizira se kroz ostvarenje ciljeva procesa. Svaki cilj procesa se sastoji od niza ciljeva aktivnosti. Indikator ostvarenja svakog cilja u COBIT-u se zove mjerilo rezultata (u ranijim verzijama je to bio tzv. ključni indikator cilja). Mjerilo rezultata pokazuje je li neki cilj ostvaren ili nije. Ono se uvijek koristi nakon događaja. Uz cilj i njegovo ostvarenje vezani su i indikatori izvedbe (ranije ključni indikatori procesa). Indikatori izvedbe pokazuju ima li šanse da se neki cilj ostvari. On pokazuje zapravo

* Po COBIT-u resursi su: aplikacije, informacije, infrastruktura i ljudi.

sposobnost nekog procesa da ostvari cilj pa se ponekad zove i pokretač izvedbe (primjerice u BSC).

Zbog hijerarhije ciljeva ista stvar koja je na višoj razini bila mjerilo rezultata na nižoj razini postaje indikator (pokretač) izvedbe. U COBIT-u svaki IT-proces ima određenu strukturu prikaza (tablica 2).

COBIT predstavlja dobru praksu ovladavanja IT-om u organizaciji te ovladavanja IT-rizicima na razini srednjeg menadžmenta. Procesi unutar COBIT-a koji se koriste kod upravljanja rizicima prikazani su u tablici 3.

Proces procjenjivanja i upravljanja rizikom. Cilj je postaviti okvir za upravljanje IT-rizicima. To znači da treba dokumentirati prihvatljivu razinu rizika, strategije smanjivanja rizika i prihvatljiv preostali rizik. Bitno je da postoji usklađenost poslovnih i IT-ciljeva vezanih uz rizike. Svaki neželjeni događaj koji bi mogao imati utjecaj na poslovanje treba se moći identificirati, analizirati i procijeniti njegov značaj. Zadatak strategija smanjivanja mora biti svođenje rizika na prihvatljivu razinu. Rezultat procjene rizika mora biti razumljiv vlasnicima i mora biti izražen u financijskim terminima kako bi oni koji odlučuju mogli svesti rizik na prihvatljivu razinu tolerancije.

TABLICA 4. Postupci za praćenje upravljanja informacijskom sigurnošću

kontrole koje su zakonski propisane • zaštita osobnih podataka • zaštita organizacijskih zapisa • zaštita intelektualnog vlasništva
kontrole koje predstavljaju „dobru praksu“ u ostvarivanju informacijske sigurnosti • politika informacijske sigurnosti • raspodjela odgovornosti za postizanje informacijske sigurnosti • svjesnost postojanja potrebe za informacijskom sigurnošću, edukacija i trening • pravilne obrade u aplikacijama • upravljanje tehničkim ranjivostima • upravljanje kontinuitetom poslovanja • upravljanje incidentima informacijske sigurnosti i njezinim unapređenjem

TABLICA 5. Kritični faktori uspjeha za postizanje informacijske sigurnosti

- postojanje politike informacijske sigurnosti, ciljeva i aktivnosti koji su odraz poslovnih ciljeva
- definiranje pristupa ka stvaranju, održavanju, nadzoru i unapređenju informacijske sigurnosti koji je u skladu s organizacijskom kulturom
- vidljiva podrška i posvećenost svim razinama menadžmenta
- dobro razumijevanje zahtijeva informacijsku sigurnost, procjenu rizika, upravljanje rizicima
- učinkovito informiranje o informacijskoj sigurnosti svih menadžera, zaposlenika i svih drugih zainteresiranih (dioničari, partneri…)
- distribucija vodiča za informacijsku sigurnost (zasnovanog na politici i standardu) svima u organizaciji
- stvaranje i povećavanje fonda aktivnosti za ostvarivanje informacijske sigurnosti
- omogućavanje stvaranja „kulture rizika“, edukacije i treninga
- uspostavljanje učinkovitog upravljanja incidentima kod informacijske sigurnosti
- implementacija sustava mjerenja kojim se procjenjuje izvedba upravljanja informacijskom sigurnošću (povratna informacija za unapređenje čitavog procesa)

TABLICA 6. Specifične prijetnje sigurnosti IT–a u zdravstvu

- neovlašteni pristup podacima iznutra i izvana (ostanak u programu nakon prestanka rada – druga osoba koristi program pod tuđom lozinkom; narušena povjerljivost i integritet)
- neautorizirana uporaba zdravstvenog informacijskog sustava – loša identifikacija i autentifikacija korisnika, loša kontrola pristupa i upravljanje privilegijama
- otvorenost prema malicioznom softveru (virusi, trojanci, crvi…)
- upadi u komunikaciju i uništenje poruka
- odbijanje prijema ili slanja osjetljivih informacija zbog nepostojanja digitalnog potpisa
- greške kod povezivanja na mrežne servise (npr. plaćanje putem Centralnog zdravstvenog informacijskog sustava Republike Hrvatske – CEZIH)
- nehotično slanje osjetljivih podataka na krive adrese
- tehničke greške (serveri, mreža, kompjutori…)
- nepostojanje rezervnih varijanti kod nestanka struje, požara, poplava…
- greške u funkcioniranju sustava – nemogućnost korištenja servisa
- greške u funkcioniranju aplikacijskog softvera
- greške operatera (sustav administratora, mrežnih administratora)
- greške u održavanju
- greške korisnika
- manjak osoblja
- krađe podataka unutar organizacije/izvan organizacije
- namjerno uništenje opreme iznutra i izvana
- terorizam

OPERATIVNA RAZINA – KONKRETNE AKTIVNOSTI

ISO 27799:2008 je standard za uspostavu informacijske sigurnosti u medicinskim ustanovama. Informacijska sigurnost podrazumijeva zaštitu informacija od prijetnji.[8,9] Cilj informacijske sigurnosti je osiguranje kontinuiteta poslovanja, minimiziranje poslovnog rizika, maksimaliziranje povrata investicija i poslovnih mogućnosti.

Informacijska sigurnost se postiže implementacijom kontrola, uključujući politike, procese, procedure, organizacijske strukture, te softverske i hardverske funkcije. Sve ove kontrole trebaju osigurati, implementirati, nadgledati i omogućiti izvješćivanje o poslovnim ciljevima. Informacijska sigurnost je važna u svim organizacijama jer štiti kritičnu imovinu koja ima određenu vrijednost. Informacijska sigurnost se postiže:

- upravljanjem rizicima u organizaciji
- poštovanjem zakona, propisa, ugovora, pravilnika…
- ispunjavanjem poslovnih zahtjeva koji propisuju način procesiranja informacija kako bi bili potpora operacijama unutar organizacije

Preduvjet za kvalitetno upravljanje informacijskom sigurnošću jest upravljanje rizicima. Rezultati upravljanja rizicima podloga su menadžerima za donošenje odluka o povećanju informacijske sigurnosti i implementaciji kontrola. Skup kontrolnih postupaka koje se moraju implementirati u svakoj organizaciji, kritični faktori uspjeha za postizanje informacijske sigurnosti i specifične prijetnje u zdravstvu prikazani su u tablicama 4-6.

PODRŠKA UPRAVE (OVLADAVANJE IT-om KAO BITNA PRETPOSTAVKA)

Kod uspostave sustava upravljanja informacijskom sigurnošću ključna je podrška uprave. Uprava mora biti u potpunosti posvećena i aktivno uključena u proces uvođenja sustava upravljanja informacijskom sigurnošću. Potpora uprave ogleda se kroz pisane i usmene izjave kroz koje se treba naglašavati važnost sigurnosti medicinskih informacija. Uprava mora stvarati klimu spremnosti na promjene, mora biti spremna suprotstaviti se otporima. S druge strane, uprava mora definirati strateške prijetnje, tj. područja informacijske sigurnosti koja su bitna za poslovanje. Uprava mora oformiti tijelo za provedbu sustava za upravljanje informacijskom sigurnošću. U tom tijelu trebao bi biti: predstavnik uprave, pravnik, voditelj financija, voditelj kvalitete i voditelj informatike te liječnik koji u potpunosti poznaje medicinske procese.

Ovo tijelo bi trebalo definirati:

- ciljeve zaštite informacija u zdravstvu
- zdravstvene informacije koje treba štititi
- sustav upravljanja informacijskom sigurnošću.

Zdravstvene informacije koje se trebaju zaštititi. Postoji nekoliko tipova informacija čije se dostupnost, integritet i pouzdanost trebaju štititi. To su:

- osobne zdravstvene informacije pacijenata
- pseudoinformacije o pacijentima generirane za potrebe nekih istraživanja
- informacije prikupljane za potrebe statističkih istraživanja, uključujući i anonimne informacije izvedene iz osobnih zdravstvenih informacija (u kojima nema identifikacijskih podataka)
- kliničko/medicinsko znanje koje nije povezano sa specifičnim predmetom medicinske njege, uključujući podatke koji služe za donošenje odluka u klinici (npr. podaci o reakciji na lijekove)
- informacije o zdravstvenim djelatnicima, osoblju i volonterima
- informacije vezane uz javni nadzor zdravstva
- informacije vezane uz sudske procese povezane s liječenjem pacijenata

PRILOG 1. Etape i postupci izgradnje sustava upravljanja informacijskom sigurnošću

Planiranje

Korak 1: Definiranje područja djelovanja sustava za upravljanje infomacijskom sigurnošću informacija
Korak 2: Planiranje politika unutar sustava za upravljanje infomacijskom sigurnošću
Korak 3: Planiranje sustavnog pristupa procjeni rizika
Korak 4: Identifikacija rizika (procjena faktora rizika i informacijske imovine)
Korak 5: Izvedba procjene rizika
Korak 6: Planiranje odnosa prema riziku
Korak 7: Izbor upravljačkog cilja i kontrola
Korak 8: Priprema „Izjave o prihvatljivosti"
Korak 9: Priznavanje preostalog rizika i omogućavanje funkcioniranja sustava upravljanja informacijskom sigurnošću
Dokumentacija: opis sustava koji se prati, identificirana sigurnosna politika, dijagram upravljačke strukture sustava za upravljanje informacijskom sigurnošću (tko je za što odgovoran), procedure identifikacije informacijske imovine, popis informacijske imovine, lista rizika, procedure procjene rizika, izvješće o procjeni rizika, procedure tretiranja rizika, izvješće o tretiranju rizika, plan tretiranja (odnosa prema) rizika, kriteriji mjerenja informacijske sigurnosti, izjava o prihvatljivosti.

Izrada

Korak 1: Izvođenje postupka smanjivanja rizika
Korak 2: Alociranje poslovnih resursa od strane menadžmenta
Korak 3: Uporaba kontrole (planiranje potrebnih procedura)
Korak 4: Izvedba obuke i treninga
Korak 5: Upravljanje operacijama
Korak 6: Upravljanje poslovnim resursima
Korak 7: Definiranje akcija u slučaju pojave sigurnosnih incidenata
Dokumentacija: plan za tretiranje rizika, plan za sustav zaštite informacija, plan kontinuiteta poslovnih informacija, plan edukacije i treninga, priručnik procedura za edukaciju i trening, procedure za upravljanje dokumentima o zaštiti informacija, izvješća o provedenom treningu i edukaciji, o provedenim sigurnosnim operacijama, plan za mjerenje ozbiljnosti sigurnosnih incidenata, izvješće o mjerenjima sigurnosnih incidenata.

Provjera

Korak 1: Nadgledanje procedura i kontrola
Korak 2: Nadzor nad sustavom upravljanja informacijske sigurnosti (nadzor učinaka sustava, preostalog i prihvatljivog rizika).
Korak 3: Izvješće za upravu
Dokumentacija: plan, procedure i liste provjere internog audita (kontrole); izvješća o treningu i edukacijama u vezi sa sustavom upravljanja informacijskom sigurnošću, izvješća o operacijama povećanja informacijske sigurnosti, izvješća o mjerilima kojima se određuje ozbiljnost informacijskih incidenata, izvješća internih audita; zapisnici sa sastanaka na kojima se izvješćuje uprava o poduzetim radnjama, zapisnici sa sastanaka radne skupine za uspostavu sustava upravljanja informacijskom sigurnošću.

Korekcija (djelovanje)

Korak 1: Definirati mjere poboljšanja sustava sigurnosti informacija (korektivne i preventivne akcije)
Korak 2: Raspraviti kroz organizaciju o akcijama koje se poduzimaju.
Dokumentacija: plan odnosa prema rizicima (prihvaćanje, izbjegavanje, smanjivanje ili prenošenje rizika), korekcijske i preventivne procedure.

- informacije koje produciraju informacijski sustavi; tu se misli i na kontrolu i na informacije koje služe za pristup osjetljivim informacijama (lozinke, korisnička imena, PIN-ovi i sl.).

Strogost čuvanja dostupnosti, integriteta i pouzdanosti informacija ovisi o prirodi informacija koje se štite. Primjerice, statistički podaci ne moraju biti toliko povjerljivi (svatko ih može vidjeti, javno su dostupni, ali integritet im mora biti potpun – ne može ih svatko mijenjati). Primjerice: zapisnici sa suđenja vezani uz tijek liječenja ne trebaju zahtijevati dostupnost (u smislu da moraju biti dostupni istu sekundu – vrijeme odziva ne mora biti trenutno), ali njihov sadržaj mora biti u potpunosti pouzdan (do tih podataka ne smiju svi moći doći).

Koje informacije će se čuvati i u kojoj mjeri ovisi o postupku procjene rizika. Procjenom rizika određuje se razina sigurnosti, tj. potreba za čuvanjem dostupnosti, integriteta i pouzdanosti informacija. Vrste medicinskih podataka koje je potrebno čuvati prikazani su u tablici 7.

Etape izgradnje sustava upravljanja informacijskom sigurnošću, tzv. Demingov krug, prikazani su u prilogu 1.

Područja informacijske sigurnosti. Upravljanje sigurnošću informacija u zdravstvu ne svodi se samo na sigurnost korisničkih imena i lozinki, već je potrebno voditi računa o 11 glavnih područja (prilog 2).

Procjena rizika sigurnosti informacija i njihov tretman osnova je za postavljanje okvira informacijske sigurnosti. Kroz identifikaciju, kvantifikaciju, određivanje važnosti rizika te određivanje odgovora na rizik, određuju se aktivnosti i prioriteti za upravljanje informacijskom sigurnošću.

TABLICA 7. Medicinski podaci koji zahtijevaju čuvanje dostupnosti, povjerljivosti i pozdanosti

- osobni podaci o zdravlju pacijenata (elektronički zdravstveni karton)
- podaci o pacijentima unutar kojih je identifikacija pacijenta onemogućena kriptografijom (za potrebe statističkih obrada)
- ostali medicinski podaci za potrebe statistike (podaci koji nisu nužno vezani uz pacijente)
- medicinski podaci koji nisu vezani uz pacijente (npr. podaci o reakcijama na lijekove, o bolničkim infekcijama i sl.)
- podaci o medicinskom osoblju i liječnicima
- podaci vezani uz javno zdravstvo
- kontrolni podaci, derivirani iz bolničkog informacijskog sustava
- podaci o lozinkama, korisničkim imenima, tj. podaci bitni za provođenje kontrole povjerljivosti, integriteta i dostupnosti.

PRILOG 2. Područja informacijske sigurnosti

1. Politika informacijske sigurnosti
- izrada dokumenta informacijske sigurnosti
- pregled dokumenta informacijske sigurnosti (i promjena ako je potrebno)

2. Organizacija informacijske sigurnosti

Unutarnja organizacija
- posvećenost menadžmenta informacijskoj sigurnosti
- koordinacija informacijske sigurnosti
- podjela odgovornosti za informacijsku sigurnost
- autorizacija procesa obrade informacija od strane odgovornih
- ugovori o povjerljivosti
- komunikacija sa stručnjacima
- komunikacija s interesnim grupama
- neovisna ocjena informacijske sigurnosti

Vanjska organizacija
- identifikacija rizika povezanih s vanjskim partnerima
- određivanje rizika kada omogućujemo partnerima pristup do organizacijske imovine
- određivanje mjera sigurnosti u ugovorima o *outsourcingu*

Outsourcing (vanjske usluge)

3. Upravljanje imovinom

Odgovornost za imovinu
- inventura imovine
- vlasništvo nad imovinom
- prihvatljiva uporaba imovine

Klasifikacija informacija
- vodič za klasifikaciju (kako klasificirati informacije u kategorijama njihove vrijednosti, osjetljivosti, važnosti za organizaciju)
- upravljanje i označavanje informacija

4. Pouzdanost ljudskih resursa

Aktivnosti prije zaposlenja
- uloge i odgovornosti
- nadzor (provjera zaposlenika)
- uvjeti zaposlenja

Aktivnosti za vrijeme zaposlenja
- odgovornost menadžmenta da upozna zaposlenika s politikom informacijske sigurnosti
- razvijanje svijesti, trening i edukacija o informacijskoj sigurnosti
- disciplinski postupak za kršenje sigurnosti
- završetak ili promjena posla
- odgovornosti kod završetka rada
- povrat imovine
- gašenje prava pristupa

5. Fizička sigurnost i sigurnost okoline

Sigurna područja
- definiranje fizičkih sigurnosnih barijera
- fizička kontrola ulaza
- sigurne sobe, uredi i sl. (sistemska soba)
- zaštita protiv vanjskih prijetnji i prijetnji iz okoline
- rad u sigurnim područjima
- pristup javnosti, područja isporuke

Nastavak na slijedećoj stranici

Sigurnost opreme
- smještaj i zaštita opreme
- usluge podrške (napajanje, strujom, zaštita od požara, klimatizacija…)
- sigurnost kablova
- održavanje opreme
- održavanje rezervne opreme
- sigurno odlaganje i ponovna uporaba opreme

Izuzimanje opreme (uklanjanje opreme mora biti autorizirano)

6. Upravljanje komunikacijama i operativom

Operativne procedure i odgovornosti
- dokumentirane operativne procedure
- upravljanje promjenama
- podjela dužnosti
- odvajanje funkcija razvoja, testiranja i operacija

Upravljanje isporukama outsourcinga
- isporuka usluga (SLA-ugovori)
- nadzor i izvješćivanje o uslugama *outsourcinga*
- upravljanje promjenama usluga *outsourcinga*

Planiranje i prihvaćanje sustava (minimizacija rizika od sustavnih grešaka)
- upravljanje kapacitetima (kontrolirana uporaba resursa)
- prihvaćanje sustava (novi IS, nove verzije, promjene…)

Zaštita od malicioznog i mobilnog koda
- kontrole protiv malicioznog koda
- kontrole protiv mobilnog koda

Backup
- sigurnosne kopije informacija
- upravljanje sigurnošću mreže
- kontrola mreže
- sigurnost mrežnih servisa

Upravljanje medijima
- upravljanje prijenosnim medijima
- odlaganje medija
- procedure upravljanja informacijama
- sigurnost informacija o sustavu

Razmjena informacija
- politika i procedure razmjene informacija
- ugovori o razmjeni (misli se na partnere izvan organizacije)
- osiguranje fizičkih medija u tranzitu
- definiranje elektroničkih poruka
- način razvoja poslovnih informacijskih sustava

Usluge elektroničke trgovine
- zaštita elektroničke trgovine
- *on-line* transakcije
- javno dostupne informacije

Nadzor
- zapisi kontrola
- definiranje uporabe informacija nadzora u sustavu
- zaštita zapisa o nadzoru
- postojanje zapisa administratora i operatera
- zapisi o greškama
- sinkronizacija vremena

7. Kontrola pristupa

Poslovni zahtjevi za kontrolu pristupa
- politika kontrole pristupa

Upravljanje korisničkim pristupom
- registracija korisnika
- upravljanje privilegijama
- upravljanje korisničkim lozinkama
- pregled korisničkih prava

Odgovornost korisnika
- uporaba lozinki
- oprema korisnika pravilno zaštićena
- zaštita osjetljivih informacija na radnom stolu i kompjutoru

Kontrola pristupa mreži
- politika uporabe mrežnih servisa
- autentifikacija korisnika kod vanjskog pristupa
- identifikacija opreme na mreži
- daljinska dijagnostika i konfiguracija mrežnih ulaza (mora biti pod kontrolom)
- podjela mreže na manje segmente radi lakšeg upravljanja
- kontrola usmjeravanja mreže

Kontrola pristupa operacijskom sustavu
- procedure sigurne prijave
- korisnička identifikacija i autentifikacija
- sustav upravljanja lozinkama
- uporaba sistemskih servisa
- vremensko ograničenje sesija

Kontrola pristupa aplikacijama i informacijama
- ograničenje pristupa informacijama
- izolacija osjetljivih sustava

Mobilno računalstvo i rad na daljinu
- definiranje uvjeta mobilnog računalstva i komunikacija
- definiranje uvjeta rada na daljinu

8. Nabavka, razvoj i održavanje informacijskih sustava

Sigurnosni zahtjevi informacijskih sustava
- specifikacija i analiza sigurnosnih zahtjeva

Pravilno procesiranje u aplikacijama
- validacija ulaznih podataka
- kontrola internih procesa
- integritet poruka
- validacija izlaznih podataka

Kriptografske kontrole
- politika uporabe kriptografskih kontrola
- upravljanje ključevima za kriptografsku zaštitu

Sigurnost sistemskih datoteka
- kontrola operativnog softvera (softvera u okviru operacijskog sustava)
- zaštita testnih, sistemskih podataka
- kontrola pristupa u programski izvorni kod

Sigurnost u razvoju i podršci procesa
- procedure kontrola promjene
- tehnički pregled aplikacija nakon promjena
- ograničenja promjena aplikacija
- sprječavanje curenja informacija
- kontrola razvoja aplikacija u *outsourcing*

Upravljanje tehničkom ranjivošću
- kontrole tehničke ranjivosti

9. Upravljanje incidentima informacijske sigurnosti

Izvješćivanje o događajima i slabostima unutar informacijske sigurnosti
- izvješćivanje o događajima vezanim uz informacijsku sigurnost

Nastavak na slijedećoj stranici

- izvješćivanje o sigurnosnim slabostima

Upravljanje incidentima informacijske sigurnosti i unapređivanje tog upravljanja

- definiranje procedura i odgovornosti
- učenje iz incidenata
- skupljanje dokaza

10. Aspekti informacijske sigurnosti kod upravljanja kontinuitetom poslovanja

- uključivanje informacija o informacijskoj sigurnosti u proces upravljanja kontinuitetom poslovanja
- procjena rizika i kontinuitet poslovanja
- postavljanje okvira za planiranje kontinuiteta poslovanja
- testiranje, održavanje i ponovna procjena planova za kontinuitet poslovanja

11. Uskladivost

- sukladnost sa zakonskim zahtjevima
- identifikacija primjenjive legislative
- prava na intelektualno vlasništvo
- zaštita organizacijskih zapisa
- zaštita podataka i osobito osobnih podataka
- prevencija pogrešne uporabe obrade informacija
- regulacija kriptografskih kontrola

Sukladnost sa sigurnosnim politikama i standardima i tehnička usklađenost

- sukladnost sa sigurnosnim politikama i standardima
- provjera tehničke uskladivosti sa sigurnosnim standardima

Razmatranja o kontroli informacijskih sustava

- kontrole nadzora informacijskih sustava
- zaštita alata za kontrolu informacijskih sustava (specijalni softver ili podaci)

Osnovni sigurnosni zahtjevi su povjerljivost, integritet i dostupnost informacija. U zdravstvu posebna pažnja polaže se na povjerljivost, tj. osiguravanja mogućnosti pristupa informacijama samo ovlaštenim osobama. Na drugom mjestu je integritet podataka, tj. zabrana neovlaštenog mijenjanja podataka o pacijentu jer to može biti opasno, čak i po život pacijenta. Budući da u zdravstvu treba reagirati točno na vrijeme, dostupnost sustava u svakom trenutku je neophodna.

ZAKLJUČAK

Područje upravljanja rizicima u zdravstvu vrlo je kompleksno i zahtijeva timski rad informatičkih stručnjaka i menadžera zdravstvenih ustanova. Menadžerska vještina upravljanja rizicima ne može se svesti na informatiku, na korisnička imena i lozinke. Upravljanje rizicima u zdravstvu mora se organizirati kao projekt s multidisciplinarnim pristupom ukoliko se problem želi kvalitetno riješiti.

Management of information safety in healthcare

SUMMARY *Whether manufacturing or service, public or private, organisations increasingly depend on information and communication technology (ICT). ICT is present to such an extent that its users are not even aware of its influence. It is a normal part of any organization. However, the dependence on ICT holds a potential hazard for organization's performance. There are several issues about the ICT safety that should be addressed in every organisation. First, is the management of an organisation is aware of the potential risks and problems in the ICT area, such as potential ICT unavailability (risk culture) or accidental damage? Is there a systematic approach to threat identification, vulnerability exploration, and evaluation of the impact of realized threats on the business? Is an organization aware of the value of ICT, which should be treated in the organisation as any other asset influencing business efficiency and effectiveness? Preventive and corrective actions (systems of control) are warranted for mitigating the risk of destruction or abuse of ICT. In this paper, we discuss these questions and suggest possible solutions.*

KEY WORDS *health care sector; information systems; risk; risk management*

LITERATURA

1. **Panian Ž, SpremićM i sur.** Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri – nakladništvo i informatika d.o.o.; 2007.
2. **Crouhy M, Galai D, Mark R.** The Essentials of Risk Management. New York: The McGraw-Hill Company; 2006.
3. **Pritchard CL.** Risk Management: Concepts and Guidance. Arlington: ESI International Press; 2001.
4. **Chavas JP.** Risk Analysis in Theory and Practice. London: Elsevier Academic Press; 2004.
5. **Westermann G, Hunter R.** IT Risk: Turning Business Threats into Competitive Advantage. Boston: Harvard Business School Press; 2007.
6. **ISACA.** The RISK IT Practitioner Guide. ISACA Press; 2010.
7. **"COBIT 4.1"** ISACA Press, 2007.
8. **HR EN ISO 27799:2008 Medicinska informatika – Upravljanje informacijskom sigurnošću u zdravstvenim ustanovama uz pomoć ISO/ IEC 27002 (ISO 27799:2008; EN ISO 27799:2008).**
9. **ISO/ IEC 17799:2005 Information technology – security techniques-Code of practice for information security management.**
10. **Moeller RR.** COSO Enterprise Risk Management. New Jersey: John Willey & Sons Inc.; 2007.
11. **ISO/ IEC 31000:2008 Risk management – Principle and guidelines on implementation.**
12. **ISO/ IEC 31010:2009 Risk management – Risk assessment techniques.**
13. **Kaplan RS, Norton DP.** The Strategy Focused Organization. Boston: Harvard Business School Press; 2001.
14. **Monahan G.** Enterprise Risk Management: A Methodology for Achieving Strategic Objectives. New Jersey: John Wiley & Sons Inc.; 2008.
15. **ISACA, IT Governance Institute.** COBIT 4. 1, COBIT 5.0 Framework, COBIT Mapping ISO/ IEC 17799:2005 with COBIT 4.0. London: ISACA Press; 2001-2006.

ADRESA ZA DOPISIVANJE

Mr. sc. Velibor Božić, dipl. inf., CCNA
OB „Dr. Tomislav Bardek", Koprivnica
E-mail: informatika@obkoprivnica.hr
Telefon: +385 99 7312 142