Merjenje učinkovitosti sistema za upravljanje informacijske varnosti

Stane Moškon, Vris d.o.o., Ljubljana
Alenka Brezavšček, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj

Povzetek

Namen prispevka
V prispevku so predstavljene različne metrike in metodologije za merjenje učinkovitosti sistema za upravljanje informacijske varnosti (SUIV) v organizaciji. Izpostavljene so prednosti in slabosti posameznih metodologij kakor tudi uporabnost metrik v praksi. Poudarjeno je, da je za kontinuirano spremljanje učinkovitosti sistema za upravljanje informacijske varnosti v organizaciji potrebno definirati ustrezna merila in sistem merjenja. Pri tem je potrebno izhajati iz glavnih poslovnih procesov in ne zgolj iz IT procesov v organizaciji.

Metodologija
Na podlagi detajlnega pregleda tuje in domače strokovne literature so oblikovani različni pogledi na merjenje učinkovitosti SUIV v organizaciji. Podana je zasnova sistema za merjenje informacijske varnosti, ki temelji na analizi učinkovitosti ključnih poslovnih procesov organizacije.

Ugotovitve
Pomemben dejavnik pri zagotavljanju neprekinjenega poslovanja organizacije je vzpostavitev ustreznega SUIV, ki mora temeljiti na principu PDCA (Plan – Do – Check – Act). Princip PDCA narekuje, da je potrebno delovanje SUIV stalno nadzirati in spremljati njegovo učinkovitost. Da bi ugotovili, v kaki meri služi obstoječi SUIV svojemu namenu, je potrebno definirati različne metrike in metodologijo za merjenje. S pomočjo ustreznega sistema merjenja učinkovitosti SUIV lahko po eni strani spremljamo, ali so zastavljeni cilji glede informacijske varnosti doseženi, po drugi strani pa tak sistem omogoča analizo učinkov planiranih izboljšav in proučevanje smotrnosti uvedbe le-teh.

Omejitve/uporabnost raziskave
Na osnovi pregleda in analize uveljavljenih metrik in metodologij za merjene učinkovitosti SUIV je nakazana problematika in možnost razvoja novega modela, ki naj bi temeljil na procesnem pristopu pri upravljanju SUIV.

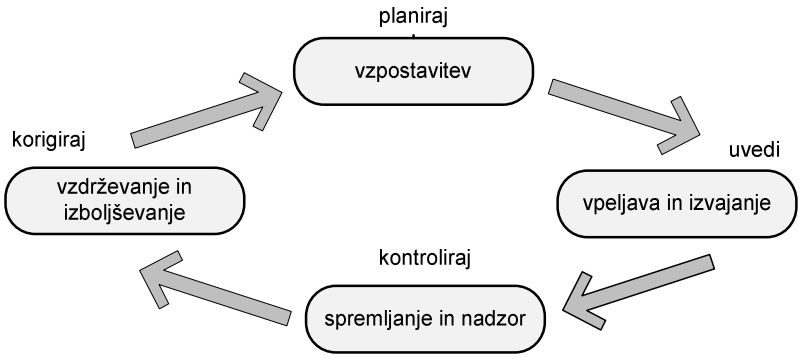
Praktična uporabnost
Organizacije se čedalje bolj zavedajo večjo pomembnosti vzpostavitve SUIV. Zavedajo se tudi, da vzpostavitev SUIV ne more biti enkraten dogodek ampak, da je to kontinuiran proces, v katerega mora biti vgrajen princip neprestanega izboljševanja. V ta namen pa moramo v organizaciji vzpostaviti model merjenja učinkovitosti SUIV, ki bo omogočal spremljanje njegove učinkovitosti in služil kot osnova za planiranje izboljšav.

Izvirnost/pomembnost prispevka
V prispevku bo izpostavljen procesni pristop pri razumevanju pomembnosti merjenja učinkovitosti SUIV v organizaciji.

Ključne besede: informacijski sistem, varnost, upravljanje, SUIV, učinkovitost, merjenje, metrike, metodologija

1. Uvod

Danes se organizacije v vse večji meri zavedajo pomembnosti informacijskega sistema pri izvajanju poslovnih procesov in zagotavljanju neprekinjenega poslovanja. S tega stališča se zagotavljanju informacijske varnosti posveča vse več pozornosti. Organizacije se zavedajo, da je nujno vzpostaviti ustrezen *sistem za upravljanje informacijske varnosti - SUIV*, (angl. Information Security Management System – ISMS). Vzpostavitev SUIV v organizaciji naj bi temeljila na procesnem pristopu *planiraj-uvedi-kontroliraj-korigiraj* (angl. Plan – Do – Check – Act - PDCA), ki je prikazan na sliki 1. V literaturi najdemo različne dobre prakse, smernice in priporočila, ki jih organizacije pri vzpostavitvi SUIV lahko uporabijo (glej npr. Brezavšček in Moškon, 2009).



Slika 1: Procesni pristop pri vzpostavitvi SUIV v organizaciji

Princip PDCA iz slike 1 narekuje, da je potrebno delovanje SUIV stalno nadzirati in spremljati njegovo učinkovitost. V ta namen je potrebno vzpostaviti ustrezen sistema merjenja. Definirati je potrebno različne metrike in metodologijo za merjenje in vrednotenje. S pomočjo ustreznega sistema merjenja učinkovitosti SUIV lahko po eni strani spremljamo, ali obstoječi SUIV služi svojemu namenu in so zastavljeni cilji glede informacijske varnosti doseženi, po drugi strani pa tak sistem merjenja omogoča analizo učinkov planiranih izboljšav in proučevanje smotrnosti uvedbe le-teh.

V tuji strokovni literaturi najdemo kar nekaj prispevkov, ki se ukvarjajo s problematiko merjenja informacijske varnosti (glej npr. Brotby, 2009; Maloney, 2009; Payne, 2006; Hinson, 2006; Herrera, 2005; Pironti, 2007; Covert in Nielsen, 2005). Pristopi avtorjev so različni, prav tako uporabljene metodologije. Celovit pogled na problematiko merjenja informacijske varnosti je podan v priročniku NIST SP 800-55 (glej Chew idr., 2008). V slovenski strokovni literaturi prispevkov na temo merjenja učinkovitosti informacijsko varnostnih kontrol še ni zaslediti.

V pričujočem prispevku bo izpostavljen pomen merjenja učinkovitost SUIV v organizaciji. Predstavljene bodo lastnosti dobrih meril in različne metrike, ki se jih v organizaciji lahko poslužujemo. Podana bo zasnova vzpostavitve sistema merjenja. Poleg tega bodo opisane različne metodologije merjenja učinkovitosti SUIV, ki so v praksi najbolj razširjene. Izpostavljene bodo prednosti in slabosti posameznih metodologij kakor tudi njihova uporabnost. Poudarjeno bo, da je potrebno pri definiranju sistema za merjenje informacijske varnosti v organizaciji izhajati iz glavnih poslovnih procesov in ne zgolj iz IT procesov organizacije.

2. Merjenje informacijske varnosti

2.1 Motivi za uvedbo sistema merjenja

Uvedba ustreznega sistema za merjenje informacijske varnosti prinaša organizaciji kar nekaj organizacijskih kakor tudi finančnih prednosti. Med njimi bi izpostavili naslednje:

- *Porast zavedanja za odgovornost za informacijsko varnost med zaposlenimi.*
- Z ustreznim merjenjem lahko ugotovimo, kateri varovalni ukrepi in kontrole niso uvedene, niso uvedene ustrezno ali so neučinkovite. Zbiranje ustreznih podatkov in analiza procesov lahko pospeši oziroma spodbudi procese dodeljevanja odgovornosti za informacijsko varnost znotraj posameznih segmentov organizacije in njenega informacijskega sistema.
- *Analiza učinkovitosti vpeljanih kontrol, odkrivanje priložnosti za izboljšave in možnost spremljanja napredka.*
- Sistem merjenja učinkovitosti SUIV omogoča natančno vrednotenje izboljšav v smislu povečanja učinkovitosti obstoječih varovalnih ukrepov. Podrobno je možno spremljati napredek pri doseganju zastavljenih ciljev glede informacijske varnosti.
- *Možnost ugotavljanja skladnosti SUIV s postavljenimi zahtevami.*
- Organizaciji je omogočeno, da na razmeroma enostaven način hitro ugotovi, ali so določila znotraj njenega SUIV skladna z obstoječimi regulativami in zakonodajo. V primeru ugotovljene neskladnosti je možno hitro ukrepanje.
- *Merljiva osnova za planiranje virov za zagotavljanje informacijske varnosti in načrtovanje smotrne izrabe le-teh.*
- Zaradi omejenega proračuna morajo organizacije vložke v informacijsko varnost planirati nadvse skrbno. Merila učinkovitosti SUIV omogočajo, da se izboljšave planirajo smotrno in ekonomično. Dodatne resurse in vložke naj se planira na področjih, kjer je to zares potrebno.

2.2 Lastnosti dobrih meril

Učinkovitost sistema merjenja in uporabnost rezultatov je odvisna od ustreznosti izbranih meril. Uporaba neustreznih meril ne prinaša nikakršne dodane vrednosti. V takem primeru je učinek isti, ali pa morda še slabši, kot če se merjenje učinkovitosti SUIV sploh ne izvaja.
Kot navaja Jaquith (2007), je potrebno pri izbiri meril za merjenje učinkovitosti vpeljanih varovalnih ukrepov in mehanizmov upoštevati naslednje kriterije:

- konsistentnost, neodvisnost od subjektivne presoje,
- izražanje v numerični obliki (število ali odstotek), predstavljena naj bo absolutna in ne relativna vrednost,
- jasnost in nedvoumnost merske enote,
- dosegljivost podatkov, potrebnih za vrednotenje,
- ekonomičnost procesa merjenja, po možnosti naj bo avtomatiziran z možnostjo ponavljanja,
- pomembnost merila za skrbnika SUIV in uporabnost le-ga v procesu odločanja in planiranja izboljšav.

3. Vzpostavitev sistema merjenja učinkovitosti SUIV v organizaciji

Da bi z merjenjem učinkovitosti SUIV dosegli želene rezultate, moramo zagotoviti, da bo samo merjenje kontinuirana dejavnost, ki bo omogočala spremljanje rezultatov skozi čas. S tega stališča mora biti proces merjenja ponovljiv, merila pa morajo biti jasno definirana. Slednje

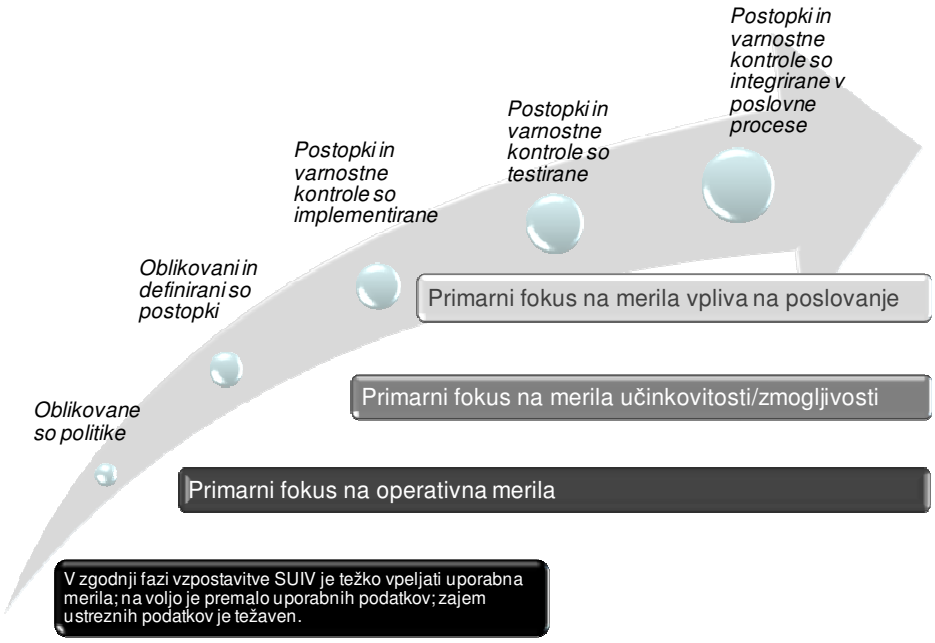
bomo lahko zagotovili samo v primeru, da bomo k problematiki merjenja informacijske varnosti pristopili sistematično. V nadaljevanju je opisan sam proces izbire meril in proces vzpostavitve sistema merjenja učinkovitosti SUIV skozi različne faze.

3.1 Vrste meril in njihova izbira v organizaciji

Kot je navedeno v NIST SP 800-55 (Chew idr., 2008), se merila za merjenje učinkovitosti SUIV v organizaciji delijo na tri skupine:

- *Operativna merila*
- S pomočjo teh meril ugotavljamo, ali se varnostne politike sploh izvajajo. Kot primer tovrstnega merila bi lahko navedli npr. odstotek informacijskih sistemov z definiranim varnostnim načrtom ali odstotek informacijskih sistemov z ustrezno definirano politiko gesel, ipd.
- *Merila učinkovitosti/zmogljivosti*
- Ta merila služijo za ugotavljanje učinkovitosti izvajanja varnostnih politik. Vpeljemo jih, kadar operativna merila kažejo zadovoljive rezultate. Kot primer takega merila bi lahko navedli odstotek vdorov v informacijski sistem zaradi neustrezno konfigurirane kontrole logičnega dostopa.
- *Merila vpliva na poslovanje*
- So merila na najvišjem nivoju in merijo posledice varnostnih incidentov na izvajanje poslovnih procesov v organizaciji. Ta merila so običajno specifična za posamezno organizacijo, saj so odvisna od vrste organizacije in njenega poslanstva na trgu. Ta merila omogočajo spremljanje izboljšav poslovnih rezultatov organizacije zaradi vpeljave SUIV, merjenje ugleda organizacije na tržišču ipd.

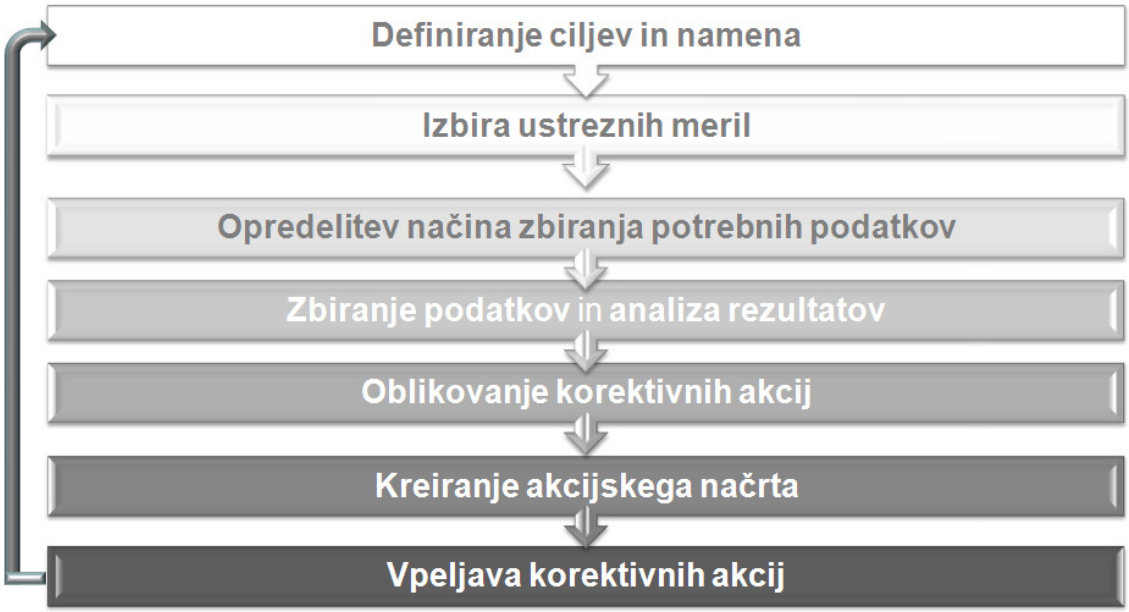
Izbira meril glede na navedene tri skupine je odvisna od stopnje zrelosti poslovnih procesov in posledično vpeljanega SUIV v organizaciji. Organizacija, ki je SUIV šele zasnovala in je v začetni fazi njegove vpeljave, se bo najbrž posluževala meril iz prve skupine. Za organizacijo, ki ima SUIV natančno definiran in vpeljan v poslovanje, pa bodo veliko bolj koristna merila iz zadnje skupine. Odvisnost izbire meril glede na stopnjo zrelosti SUIV v organizaciji je ponazorjena na sliki 2.



Slika 2: Izbira meril za merjenje učinkovitosti informacijske varnosti je odvisna od stopnje zrelosti SUIV v organizaciji (prirejeno po Payne, 2008, NIST SP 800-55)

3.2 Faze pri vzpostavitvi sistema merjenja

Vzpostavitev sistema merjenja učinkovitosti SUIV je kompleksna aktivnost, ki se je moramo lotiti postopoma. Kot je razvidno iz slike 3, lahko proces vzpostavitve prikažemo kot zaporedje sedmih faz. Znotraj prve faze je potrebno jasno definirati namen in cilje samega merjenja. Nato je potrebno opredeliti ustrezna merila, pri čemer je potrebno upoštevati stopnjo zrelosti obstoječega SUIV. Nadalje je potrebno natančno opredeliti način in pogostost zbiranja podatkov, potrebnih za samo vrednotenje. Zagotoviti je potrebno točnost podatkov in definirati ustrezne procedure za pretvarjanje surovih podatkov v izbrana merila. Dobljene rezultate je nato potrebno analizirati in o njih poročati. Na podlagi dobljenih rezultatov je potrebno zasnovati korektivne akcije, oblikovati načrt za izboljšanje SUIV ter korektivne akcije dejansko tudi izvesti. Rezultati enkratnega merjenja za organizacijo nimajo velikega pomena, zato mora biti postopek merjenja ponovljiv.
Zaključimo lahko, da je proces merjenja učinkovitost SUIV kontinuirana dejavnost, ki zahteva stalno nadgradnjo. V praksi je koristno, da se merjenje izvaja periodično. Rezultati naj se hranijo v ustrezni bazi, saj predstavljajo koristno osnovo za spremljanje trendov in planiranje izboljšav na področju zagotavljanja informacijske varnosti.



Slika 3: Faze pri vzpostavitvi sistema merjenja učinkovitosti SUIV v organizaciji (prirejeno po Payne, 2008 in NIST SP 800-55)

4. Metodologije za merjenje učinkovitosti SUIV v praksi

Iz številnih prispevkov v literaturi je razvidno, da je problematika merjenja informacijske varnosti aktualen in pereč problem. Nekateri avtorji razvijajo svoje, specifične metodologije, medtem ko se drugi naslanjajo na že uveljavljene pristope. Slednji pristopi imajo po našem mnenju večjo praktično vrednost in boljše možnosti za implementacijo.
Sistemi merjenja informacijske varnosti, ki se v praksi uporabljajo, najpogosteje temeljijo na eni izmed naslednjih znanih metodologij:

- NIST SP 800-55

- ISO 27001, 27002 in 27004
- COBIT

4.1 NIST SP 800-55 Performance Measurement Guide for Information Security

Dokument, ki ga je izdal National Institute of Standards and Technology, je vodilo kot pomoč pri izbiri, razvoju in uvedbi meril za merjenje informacijske varnosti. Ta merila so namenjena ugotavljanju učinkovitosti uporabljenih varnostnih kontrol in podpori programom za zagotavljanje informacijske varnosti. NIST SP 800-55 določa sisteme merjenja ter njihove prednosti: sistemi merjenja so orodja, namenjena za pomoč pri odločanju in izboljševanju izvajanja skozi celoten proces zbiranja, analize in poročanja o podatkih, vezanih na samo merjenje. Namen merjenja učinkovitosti SUIV je nadzor nad izvajanjem aktivnosti in njihovem stalnem izboljševanju z uvajanjem korektivnih akcij na osnovi opazovanih meritev. Na sliki 4 je prikazan primer merila za spremljanje učinkovitosti mehanizmov kontrole dostopa, kot ga predlaga NIST SP 800-55.

Measure 3: Access Control (AC) (system-level)

Field	Data
Measure ID	Remote Access Control Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Restrict information, system, and component access to individuals or machines that are identifiable, known, credible, and authorized.
Measure	Percentage (%) of remote access points used to gain unauthorized access NIST SP 800-53 Controls: AC-17; Remote Access
Measure Type	Effectiveness/Efficiency
Formula	(Number of remote access points used to gain unauthorized access/total number of remote access points) *100
Target	This should be a low percentage defined by the organization.
Implementation Evidence	1. Does the organization use automated tools to maintain an up-to-date network diagram that identifies all remote access points (CM-2)? ☐ Yes ☐ No 2. How many remote access points exist in the organization's network? _____ 3. Does the organization employ Intrusion Detection Systems (IDS) to monitor traffic traversing remote access points (SI-4)? ☐ Yes ☐ No 4. Does the organization collect and review audit logs associated with all remote access points (AU-6)? ☐ Yes ☐ No 5. Does the organization maintain a security incident database that identifies standardized incident categories for each incident (IR-5)? ☐ Yes ☐ No 6. Based on reviews of the incident database, IDS logs and alerts, and/or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period? _____
Frequency	Collection Frequency: Organization-defined (example: monthly) Reporting Frequency: Organization-defined (example: quarterly)

Slika 4: Primer merila za merjenje učinkovitost mehanizmov kontrole dostopa iz dokumenta NIST SP 800-55 (Chew, 2008).

4.2 ISO 27001, 27002 in 27004

ISO 27001, 27002 in 27004 so predstavniki družine standardov ISO 27000, ki jih izdaja International Organization for Standardization. Ti standardi predstavljajo osnovo za razvoj lastnih standardov za področje informacijske varnosti v organizaciji kakor tudi osnovo za vpeljavo SUIV.
ISO 27001 (glej BSI, 2005) podaja specifikacije za sistem za upravljanje informacijske varnosti. Ponuja smernice in splošne principe za vzpostavitev, uvedbo, vzdrževanje in izboljševanje SUIV v organizaciji v skladu s principom PDCA. Primeren je za vse vrste organizacij, ne glede na dejavnost in velikost.
ISO 27002 (glej BSI, 2005a) je kodeks dobre prakse na področju varovanja informacij. Nastal je v letu 2007 s preimenovanjem BS ISO/IEC 17799:2005 v ISO 27002.
Učinkovitost SUIV in njegovo skladnost s standardom ISO 27001 oziroma 27002 merimo z ustreznimi vprašalniki. Vprašalnik lahko izdelamo sami, ali pa uporabimo vnaprej pripravljenega. Primer takega vprašalnika najdemo npr. na spletni strani http://www.praxiom.com/iso-17799-audit.htm.
ISO 27004 je uradno ime novo nastajajočega standarda, ki bo pokrival področje meril in sistemov za merjenje učinkovitosti SUIV. Njegov cilj in namen bo pomoč organizaciji pri ugotavljanju njegove učinkovitosti in nenehnega izboljševanja po principu PDCA.

4.3 COBIT

COBIT (Common Objectives for Information and Related Technologies; glej IT Governance Institute, 2007) je okvir in sklop podpornih orodij, ki vodstvu omogočajo premostitev vrzeli na področjih nadzora, tehnike in poslovnih tveganj. Omogoča razvoj jasnih politik in dobre prakse za nadzor IT. Neprestano se posodablja in usklajuje z drugimi standardi in smernicami. Zato je COBIT postal integrator za dobre prakse na področju IT in krovni okvir za upravljanje, ki pomaga pri razumevanju in obvladovanju tveganj in koristi povezanih z IT. Procesna struktura COBIT-a, usmerjenost na višji nivo ter poslovno usmerjen pristop nudijo celovit vpogled na IT in z njo povezane odločitve.
Procesna usmeritev COBIT-a je prikazana s procesnim modelom, ki ločuje IT v štiri domene in 34 procesov v skladu s področji odgovornosti načrtovanja, izgradnje, delovanja in spremljanja. S tako delitvijo omogoča COBIT celovit pogled na IT. Koncepti arhitekture organizacije pomagajo prepoznati sredstva, ki so bistvena za uspešnost procesov, tj. aplikacije, informacije, infrastrukturo in ljudi.
Za izpolnitev poslovnih ciljev morajo biti informacije v skladu z nekaterimi kontrolnimi merili, ki jih COBIT imenuje poslovne zahteve po informacijah. Na podlagi širših zahtev glede kakovosti, fiduciarnosti in varnosti, opredeljuje COBIT sedem različnih meril za informacije, ki se med seboj prekrivajo:

- *Uspešnost* zadeva informacije, ki so pomembne za poslovni proces in so njegov del, prav tako zadeva njihovo pravočasno zagotovitev, pravilnost, skladnost in uporabnost.
- *Učinkovitost* zadeva zagotavljanje informacij z optimalno (najbolj produktivno in varčno) uporabo sredstev.
- *Zaupnost* zadeva varovanje občutljivih informacij pred nepooblaščenim razkritjem.
- *Celovitost* se nanaša na pravilnost in popolnost informacij ter njihovo veljavnost v skladu s poslovno vrednostjo in pričakovanji.
- *Razpoložljivost* se nanaša na informacije, ki morajo biti na voljo v vsakem trenutku, ko so v poslovnem procesu potrebne.
- *Skladnost* obravnava uskladitev z zakoni, predpisi in pogodbenimi dogovori, ki veljajo za določeni poslovni proces.

- *Zanesljivos*t je povezana z zagotavljanjem ustreznih informacij za vodstvo, da le-to lahko upravlja podjetje in izvaja svoje odgovornosti glede zaupnosti in vodenja.

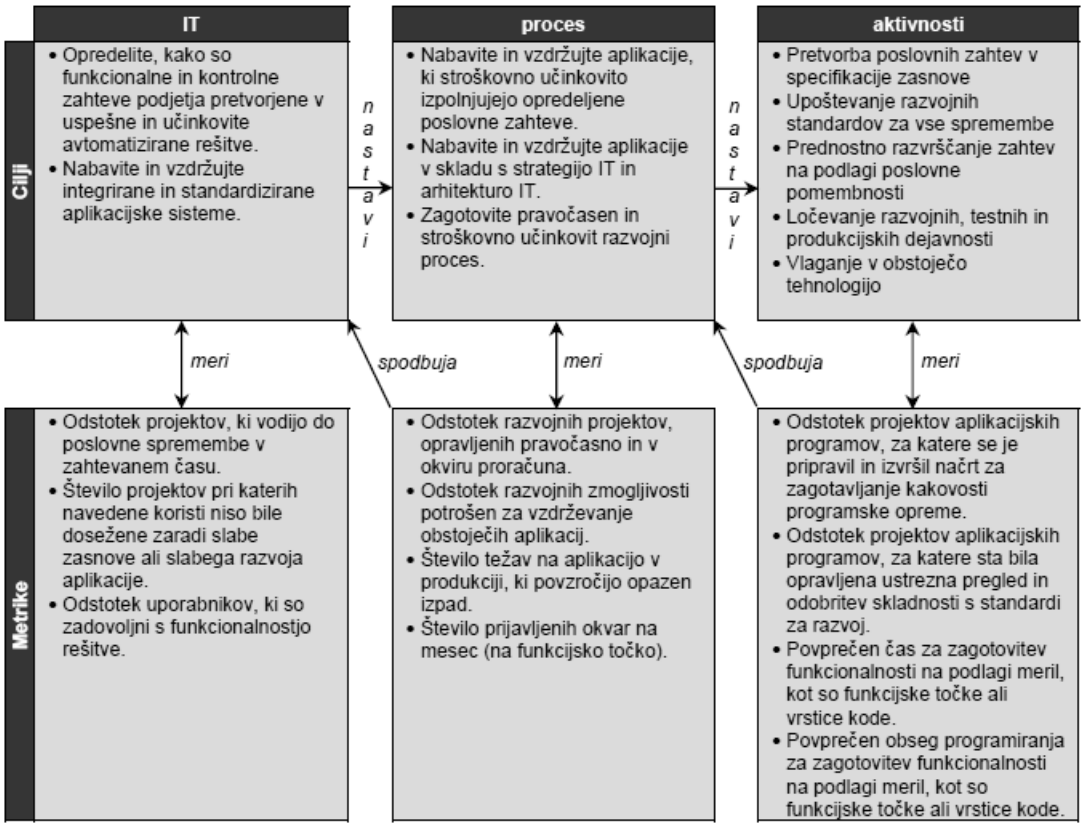
Pridobivanje objektivnega vpogleda v lastne ravni zmogljivosti podjetja ni preprosto. Kaj je treba meriti in kako? Organizacije morajo meriti, kakšno je njihovo stanje in katere izboljšave so potrebne. Poleg tega morajo vpeljati orodja za upravljanje za spremljanje izboljšav. COBIT obravnava ta vprašanja z zagotovitvijo:

- zrelostnih modelov, ki omogočajo primerjalno analizo in prepoznavanje potrebnih izboljšav;
- ciljev zmogljivosti in metrik za procese IT, ki kažejo, kako procesi uresničujejo poslovne cilje in cilje IT. Uporabljajo se tudi za merjenje zmogljivosti notranjih procesov na podlagi principov uravnoteženih kazalnikov;
- ciljev dejavnosti za omogočanje uspešne zmogljivosti procesov.

V COBIT-u so cilji in sistemi merjenja opredeljeni na treh ravneh:

- cilji IT in merila, ki opredelijo, kaj organizacija pričakuje od IT in kako to meriti;
- procesni cilji in merila, ki opredelijo, kaj morajo ustvariti procesi IT za podporo ciljev IT in kako to meriti;
- cilji dejavnosti in merila, ki opredelijo, kaj se mora zgoditi znotraj procesa, da se doseže zahtevana storilnost in kako to meriti.

Primer definiranja ciljev in meril za proces »AI2 – Nabavite in vzdržujte aplikacijske programe« v COBIT-u je prikazan na sliki 5.



Slika5: Cilji in merila za proces »AI2 – Nabavite in vzdržujte aplikacijske programe« vCOBIT-u

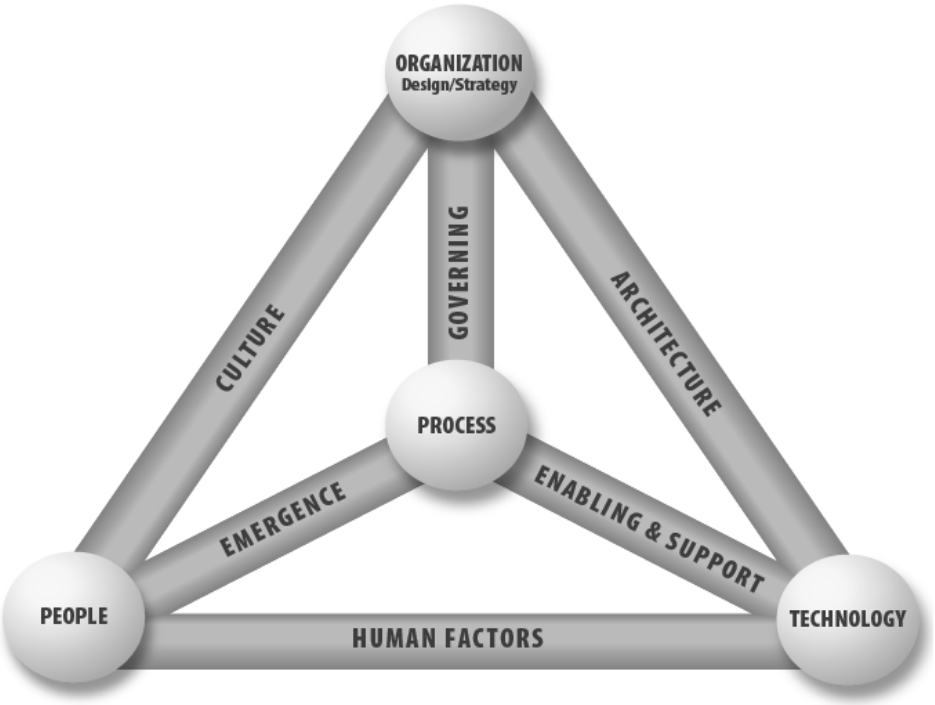
5. Procesni pristop k merjenju informacijske varnosti

Standardi in metodološki okvirji, predstavljeni v prejšnjem poglavju, so organizacijam vodilo in pomoč pri:

- vzpostavitvi programov za merjenje informacijske varnosti v organizaciji,
- definiranju ciljev merjenja učinkovitosti SUIV,
- definiranju meril za izvedbo merjenja,
- predstavljajo nabor dobre prakse.

Njihov skupni problem je, da problematiko merjenja učinkovitosti SUIV obravnavajo preveč statično. Ukrepi se namreč definirajo na osnovi analiz podatkov za neko zaključeno časovno obdobje. Sodobni organizacijski koncepti postavljajo procese v središče razumevanja in upravljanja organizacije, kar omogoča drugačen pogled na SUIV in posledično tudi na sistem merjenja njegove učinkovitosti.
Na sliki 6 je predstavljen poslovni model informacijske varnosti, ki postavlja v središče poslovne procese organizacije. Poleg poslovnih procesov so ključni elementi tega modela še organizacija, v kateri se le-ti izvajajo, ljudje, ki jih izvajajo, in tehnologija, ki omogoča njihovo izvajanje. Pomembni so tudi povezovalni elementi, ki so:

- organizacijska kultura, ki povezuje ljudi in organizacijo,
- človeški faktor, ki je vez med tehnologijo in ljudmi, ki-le to uporabljajo pri svojem delu,
- arhitektura informacijskega sistema, ki povezuje tehnologijo in organizacijo,
- vzpostavitev in podpora, ki povezuje procese s tehnologijo,
- upravljanje, ki povezuje procese in organizacijo in
- vzpostavitev procesov, ki povezuje ljudi in procese.



Slika 6: Poslovni model informacijske varnosti (povzeto po ISACA,2009)

Vzpostavitev SUIV v tem modelu temelji na osnovni predpostavki, da je ključna vloga informacijskega sistema v zagotavljanju podpore izvajanju poslovnih procesov v organizaciji in da okvir in nivo informacijske varnosti izhaja iz zahtev posameznih poslovnih procesov. Eno od ključnih vprašanj pri tem modelu je, kako vzpostaviti sistem merjenja učinkovitosti SUIV, ki bo izhajal iz zahtev poslovnih procesov in bo zagotavljal merjenje v času, ko se poslovni že procesi izvajajo.

6. Zaključek

Zagotavljanje varnosti informacijskega sistema je dandanes pomembna naloga vsake organizacije, ki želi zagotoviti neprekinjeno izvajanje svojih poslovnih procesov. V organizacijah si prizadevajo, da bi vpeljali učinkovit sistem za upravljanje informacijske varnosti – SUIV. Če želimo ugotoviti, ali obstoječi SUIV dejansko služi svojemu namenu oziroma, če želimo obstoječi SUIV izboljšati, je potrebno vpeljati ustrezen sistem merjenja učinkovitosti.
V prispevku je izpostavljen pomen merjenja učinkovitosti SUIV. Predstavljene so lastnosti dobrih meril. Ugotovljeno je, da je sama izbira meril pogojena od stopnje zrelosti SUIV v organizaciji. Organizacije, ki SUIV šele uvajajo, naj izbirajo med operativnimi merili. Za tiste organizacije, ki pa so v svoje poslovanje SUIV že vpeljale, pa so bolj koristna merila vpliva na poslovanje. Rezultati merjenja učinkovitosti SUIV bodo uporabni, če bo proces samega merjenja jasno definiran in periodično ponovljiv. Da zadostimo tem zahtevam, je potrebno k procesu merjenja pristopiti sistematično. V prispevku je definiranih sedem faz pri vzpostavitvi sistema za merjenje učinkovitosti SUIV.
Tako kot ima organizacija proste roke pri zasnovi samega SUIV, se lahko tudi za merjenje njegove učinkovitosti poslužuje različnih pristopov. Na kratko so opisane različne metodologije merjenja, ki se v praksi najbolj pogosto uporabljajo. Celovite, eksaktne in splošno uporabne metodologije za merjenje učinkovitosti SUIV v organizaciji za enkrat še ni zaslediti. Strokovnjaki iz prakse si veliko obetajo od standarda ISO 27004, ki je trenutno v pripravi, bo pa specializiran za področje merjenja. Ugotavljamo pa, da je pri definiranju sistema za merjenje učinkovitosti SUIV v organizaciji potrebno izhajati iz zahtev glavnih poslovnih procesov. Slednje pa zahteva vpeljavo proaktivnega sistema merjenja informacijske varnosti, ki bo zagotavljal ustrezne rezultate že v času, ki se procesi izvajajo, in ne le za nazaj.

7. Literatura

Boehmer, W. (2008). Appraisal of the effeciveness and efficiency of an Information Security Management System based on ISO 27001, Second International Conference on Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Published in *IEEE Computer Society*.

Brezavšček, A. in Moškon, S. (2009). Smernice za vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. *Nove tehnologije, novi izzivi,* 28. mednarodna konferenca o razvoju organizacijskih znanosti, 25. - 27. marec 2009, Portorož, Slovenija, Moderna organizacija, str. 202-209.

Brotby, W.K. (2009). *Information security management metrics: a definitive guide to effective security monitoring and measurement.* Boca Raton, CRC.

Chew, E. idr. (2008). *Performance Measurement Guide for Information Security*, NIST Special Publication 800-55, Revision 1. National Institute of Standards and Technology.

BSI (2005). *British standard. BS ISO/IEC 27001:2005, Information technology, security techniques, information security, management systems*, British Standards Institution, cop., London, 2005.

BSI (2005a). *British standard. BS ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management*, British Standards Institution, cop., London, 2007.

Covert, E. in Nielsen, F. (2005). Measuring Risk Using Existing Frameworks, Information Security Management, March/April 2005, str. 21-25.

Herrera, S.O.S. (2005). Information security management metrics development, International Carnahan Conference on Security Technology, 2005. CCST '05. 39th Annual 2005, Available in IEEE Xplore.

Hinson, G. (2006). Seven myths about information security metrics, *ISSA Journal*, July 2006. (dosegljivo na http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf, september 2009).

ISACA (2009a). *An Introduction to the Business Model for Information Security*. (dosegljivo na http://www.jtsi2009.tn/fileadmin/template/Documents_en_ligne/JTSI2/Intro_Modele_Economique_Securite_Information.pdf, september 2009).

IT Governance Institute (2007). COBIT 4.1, (dosegljivo na spletnih straneh organizacije ISACA: www.isaca.org/cobit, september 2009).

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Pearson Education.

Maloney, J. (2009). *Security Metrics Roadmap: A Guide for Information Security Professionals*. White paper series, The Santa Fe Group. (dosegljivo na http://santa-fe-group.com/papers/santa-fe-group-security-metrics-0209.pdf, september 2009).

Payne, S.C. (2006). *A Guide to Security Metrics.* SANS Institute InfoSec Reading Room. (dosegljivo na: http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55?show=55.php&cat=auditing, september 2009).

Pironti, J.P. (2007). Developing Metrics for Effective Information Security Goverance, Information System Control Journal, Vol. 2, str. 1-5.