Uporaba razširjenega modela za oceno tveganja s pomočjo računalniškega programa DEXi

Marko Potokar, Informacijski pooblaščenec, Ljubljana
Igor Bernik, Univerza Maribor, Fakulteta za varnostne vede
Blaž Markelj, Univerza Maribor, Fakulteta za varnostne vede

Namen prispevka
Namen prispevka je prikaz kvalitativne analize tveganja in opis modela za kvalitativno analizo tveganja, ki je bil razvit s pomočjo računalniškega programa za večparametrsko odločanje DEXi.

Cilj
Prispevka je predstavitev uporabe razširjenega kvalitativnega modela za analizo tveganja za proces on-line procesiranje.

Metodologija
Za izvedbo analize tveganja je bil uporabljen sistematičen pristop, ki sestoji iz postavitve modela za oceno tveganja, identifikacije neželenih dogodkov, analize neželenih dogodkov in ocene stopnje tveganja.

Ugotovitve in omejitve
Opisani model predstavlja kvalitativni pristop k analizi tveganja, kar pomeni, da so tako dobljene ocene posameznih tveganj subjektivne narave. Kljub temu pa so rezultati takega modela še vedno dovolj dobri za prepoznavanje kritičnih tveganj. Dobra lastnost predstavljenega modela je njegova razširljivost in prenosljivost na druge vrste tveganj. V prispevku smo se omejili na prve tri korake v procesu upravljanja tveganj

Izvirnost
Opisana rešitev predstavlja z dodatnimi kriteriji razširjen osnovni model za kvalitativno analizo tveganj. Rešitev je bila razvita in pilotsko vpeljana za proces analize operativnih tveganj v procesnem centru.

Ključne besede: SUVI, upravljanje tveganj, tveganje, ocena tveganja, odločitvena matrika, DEXi.

1. UVOD

Upravljanje tveganj je eden izmed bistvenih procesov vsake organizacije. Vsak dogodek, ki negativno vpliva na doseganje ciljev organizacije in povzroči moteno poslovanje organizacije je potrebno določiti, analizirati in oceniti njegov vpliv na izvajanje procesov organizacije. Za oblikovanje učinkovitega sistema upravljanja varovanja informacij (SUVI), je potreben sistematičen pristop k obvladovanju informacijskih tveganj, ki mora ustrezati danemu okolju organizacije in biti usklajen s splošnim upravljanjem tveganj v njej. Upravljanje tveganj mora biti vgrajeno v aktivnosti upravljanja varovanja informacij in stalno se izvajajoč proces (BS ISO/IEC 27001, 2005).
Bistvo pri določanju stopnje tveganja je negotovost neželenega dogodka. Poznamo dva osnovna načina za analizo in oceno tveganja: kvantitativni in kvalitativni. Oba načina imata svoje prednosti in pomanjkljivosti. Prednost kvantitativnih modelov je v njihovi objektivnosti in eksplicitnosti dobljenih rezultatov. Podprti so s statistično analizo. Pomanjkljivost tovrstnih modelov je v težavnosti pridobivanja dovolj velike količine merodajnih podatkov in uporaba kompleksnih matematičnih izračunov. Dodatna težava je oblikovanje primerne interpretacije rezultatov za vodstvo, ki se odloča o sprejetju oziroma zavrnitvi določenih aktivnosti za zmanjšanje tveganja. Lažji za razumevanje so kvalitativni modeli za analizo tveganj. Njihovi rezultati so sicer v osnovi subjektivne narave, a nam ti modeli omogočajo dobro predstavo, kaj določeno tveganje pomeni za dani proces. Da bodo rezultati

jasni in pot do njih razumljiva, moramo v procesu analize tveganja in njegovi oceni uporabljati ustrezna orodja.

2. UPRAVLJANJE TVEGANJ

Upravljanje tveganj je proces zmanjševanja tveganj na sprejemljivo stopnjo (Bankart, 2007). Je nepretrgan proces, sestavljen iz naslednjih faz:

- identifikacija neželenih dogodkov;
  Iz identificiranih neželenih dogodkov se oblikuje t.i. baza neželenih dogodkov. Bazo neželenih dogodkov sestavljajo dogodki ugotovljeni pri revizijskih pregledih in varnostnih incidentih ter del dogodkov, ki jih navajajo različni standardi (COBIT, 2005).
- analiza neželenih dogodkov;
  Analiza neželenih dogodkov se izvede tako, da se posamezni dogodki navežejo na procese. Dogodki, ki za dane procese niso relevantni se pri nadaljnji analizi tveganja ne upoštevajo.
- ocena stopnje tveganja;
  Vsak neželeni dogodek (v nadaljevanju dogodek) se za dani proces oceni po naslednjih kriterijih (parametrih):
  - stopnja možnosti nastopa dogodka (Likelihood),
  - stopnja posledic nastopa dogodka (Consequence).

  Oceno kriterijev podajo zaposleni, ki so kompetentni za posamezen proces. Iz posameznih ocen za določen kriterij se izračuna skupna ocena po enem izmed naslednjih pravil:
  - pravilo minimuma (skupna ocena določenega kriterija je najnižja izmed posameznih ocen),
  - pravilo maksimuma (skupna ocena določenega kriterija je najvišja izmed posameznih ocen),
  - pravilo povprečja (skupna ocena določenega kriterija je navzgor zaokrožena povprečna vrednost posameznih ocen).
- priprava načrta za zmanjšanje stopnje tveganja;
  Načrt za zmanjševanje stopnje tveganja predstavlja formalni načrt za uvajanje ukrepov za zmanjševanje tveganj, katerih stopnja tveganja je ocenjena z visoko ali srednje. V njem so opredeljene:
  - aktivnosti za zmanjšanje tveganja (KAJ),
  - odgovorni za izvedbo aktivnosti (KDO),
  - roki za izvedbo aktivnosti (KDAJ),
  - prioritete,
  - stroški uvedbe in izvajanja ukrepov,
  - potrebe po človeških virih,
  - potrebne nove tehnologije,
  - potrebno delo za vpeljavo in izobraževanje.
- poročanje o rezultatih ocene stopnje tveganja;
  Rezultati analize neželenih dogodkov in ocene stopnje tveganja ter načrt za zmanjšanje stopnje tveganja se predstavijo vodstvu v obliki poročila. Načrt za zmanjšanje stopnje tveganja potrdi vodstvo družbe.
- izvedba načrta za zmanjšanje stopnje tveganja;
  Cilj izvedbe načrta je zmanjšanje stopnje tveganja na raven, določeno s kriterijem sprejemljivosti. Vsa tveganja, ki so nad postavljeno ravnijo, so nesprejemljiva in morajo biti zmanjšana z:
  - odstranitvijo vzroka tveganja,
  - izbiro ustreznih kontrol (nadzorstev),
  - zavarovanjem tveganj pri zavarovalnici,
  - prenosom tveganj na drugo osebo s pogodbo.

  Vsa tveganja pod izbrano ravnijo sprejemljivosti zavestno sprejmemo, saj so premajhna, da bi upravičila stroške za njihovo zmanjševanje.
- spremljanje in ponovna ocena stopnje tveganja;

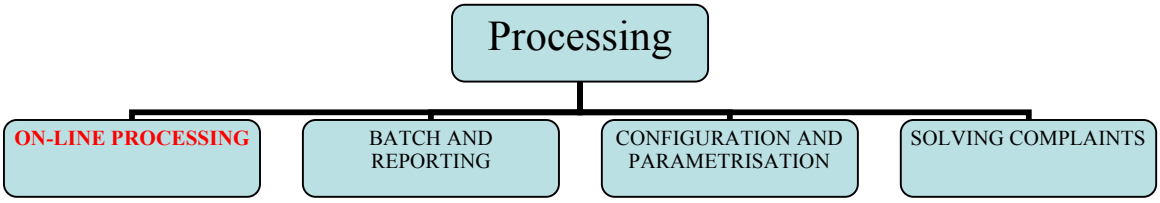
Ta faza procesa upravljanja tveganj zajema vzdrževanje baze neželenih dogodkov (brisanje nerelevantnih in dodajanje novih dogodkov), ocenjevanje uspešnosti izvedbe načrta za zmanjšanje stopnje tveganja in se nadaljuje v naslednji krog izvedbe analize in ocene stopnje tveganja.

Proces upravljanja s tveganji kompleksnih sistemov pa je možno prenesti v programe za podporo odločanju, s katerimi si pomagamo pri ocenjevanju posameznih tveganj v primeru večkriterijske izbire. Eden izmed tovrstnih programov pa je tudi DEXi.

3 MODEL ZA OCENO TVEGANJ S PROGRAMOM DEXI

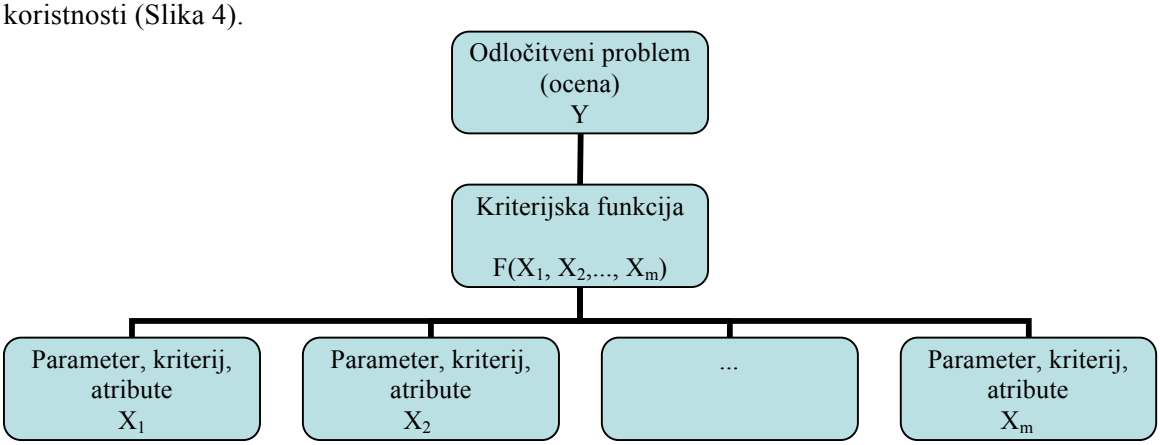
Za izvedbo opisane metodologije se uporablja kvalitativni model za oceno stopnje tveganja, razvit z orodjem DEXi. DEXi je prosto uporaben računalniški program za večparametrsko odločanje in sloni na metodologiji ekspertnih sistemov (Jereb, Bohanec in Rajkovič, 2003). Razvit je bil v sodelovanju UM, FOV in Inštitutom Jožef Stefan. Od ostalih metodologij večparametrskega odločanja se razlikuje predvsem po kvalitativnem pristopu in neposrednem določanju funkcij koristnosti več spremenljivk, kar pomembno poveča transparentnost izgradnje in uporabe odločitvenih modelov in s tem razumevanje zakaj je do dane odločitve prišlo. Program pomaga odločevalcu oblikovati ustrezen odločitveni model, ovrednotiti posamezne možne odločitve (variante), ter utemeljiti, razložiti in dokumentirati sprejete odločitve.

V predstavljeni oceni tveganja je bil analiziran podproces ON-LINE PROCESSING, ki je del procesa PROCESSING (Slika 2). Za izbrani podproces določimo neželene dogodke, ki lahko vplivajo na izvedbo podprocesa.



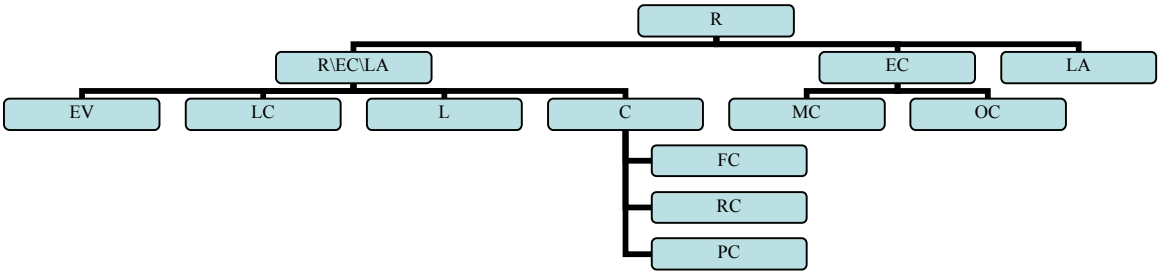
Slika 2: Podproces ON-LINE PROCESSING

V procesu večparametrskega odločanja razgradimo odločitveni problem Y na manjše podprobleme (Jereb et al., 2003). Podprobleme predstavimo s parametric (atributi, kriteriji) X_1, X_2,..., X_m. Kriterijska funkcija $F(X_1, X_2,..., X_m)$ združi vrednosti posameznih parametrov v končno oceno koristnosti (Slika 4).



Slika 4: model večparametrskega odločanja

V nadaljevanju določimo parametre neželenih dogodkov in njihovo strukturo (Slika 3).



Slika 3: struktura parametrov za posamezne dogodke za podproces On-line processing

R – evaluated Risk
- LA – Last Audit (last time the audit for the process was provided)
- EC – Existing Controls
  - MC – Management Controls
  - OC – Operational Controls
- R\EC\LA – evaluated Risk without considering Existing Controls and Last Audit
  - EV – Event Velocity (how fast the event is happening)
  - LC – Level of Control (how much the event can be controlled)
  - L – Likelihood of the event
  - C – Consequence of the event
    - FC – Financial Consequence of the event
    - RC – Reputation Consequence of the event
    - PC – Performance Consequence

V predstavljenem odločitvenem modelu smo vsak neželen dogodek določili kot glavni odločitveni problem, katerega smo v nadaljnji analizi razdelili v podprobleme, ki smo jih opisali z njihovimi parametri (atributi). Za vsak parameter smo določili možne vrednosti. V naslednjem koraku smo določili posamezne kriterijske funkcije za parameter istega nivoja (Slika 5).

Drevo kriterijev

Kriterij	Opis
RISK	The level of risk
├Last Audit	last time the audit for the process was provided
├**Existing Controls**	the controls that are already provided
│├Management Controls	the controls that are already provided
│└Operation Controls	the controls that are already provided
└**Risk\EC\LA**	The level of risk without considering Existing controls and Last Audit
├Event Velocity	how fast the event is going on
├Level of Control	how much the event can be controled
├Likelyhood	Level of Likelyhood
└**Consequence**	Level of consequence
├Finance	Finance consequence
├Reputation	Reputation consequence on the organization
└Performance	Performance consequence

Zaloge vrednosti

Kriterij	Zaloga vrednosti
RISK	*low*; moderate; **high**
├Last Audit	*frequently*; medium ; **long**
├**Existing Controls**	*good*; medium; **bad**
│├Management Controls	*good*; medium; **bad**
│└Operation Controls	*good*; medium; **bad**
└**Risk\EC\LA**	*low*; moderate; **high**
├Event Velocity	*slow*; medium; **fast**
├Level of Control	*high*; medium; **low**
├Likelyhood	*Low*; Medium; **High**
└**Consequence**	*low*; medium; **high**
├Finance	*low*; **high**
├Reputation	*low*; **moderate**
└Performance	*low*; **high**

RISK

The level of risk

1.	*low*	no mitigation of risk is needed
2.	moderate	mitigation is recommended in near future
3.	**high**	mitigation is needed ASAP

Last Audit

last time the audit for the process was provided

1.	*frequently*	audit is provided regular in periods of 6 months
2.	medium	audit is provided regular once a year
3.	**long**	nonregular, last audit more than 1 year ago

Existing Controls

the controls that are already provided

1.	*good*	all controls (MC and OC) are in place for all process
2.	medium	all controls (MC and OC) are in place but not for entire process
3.	**bad**	controls are poor and in place for some part of the process

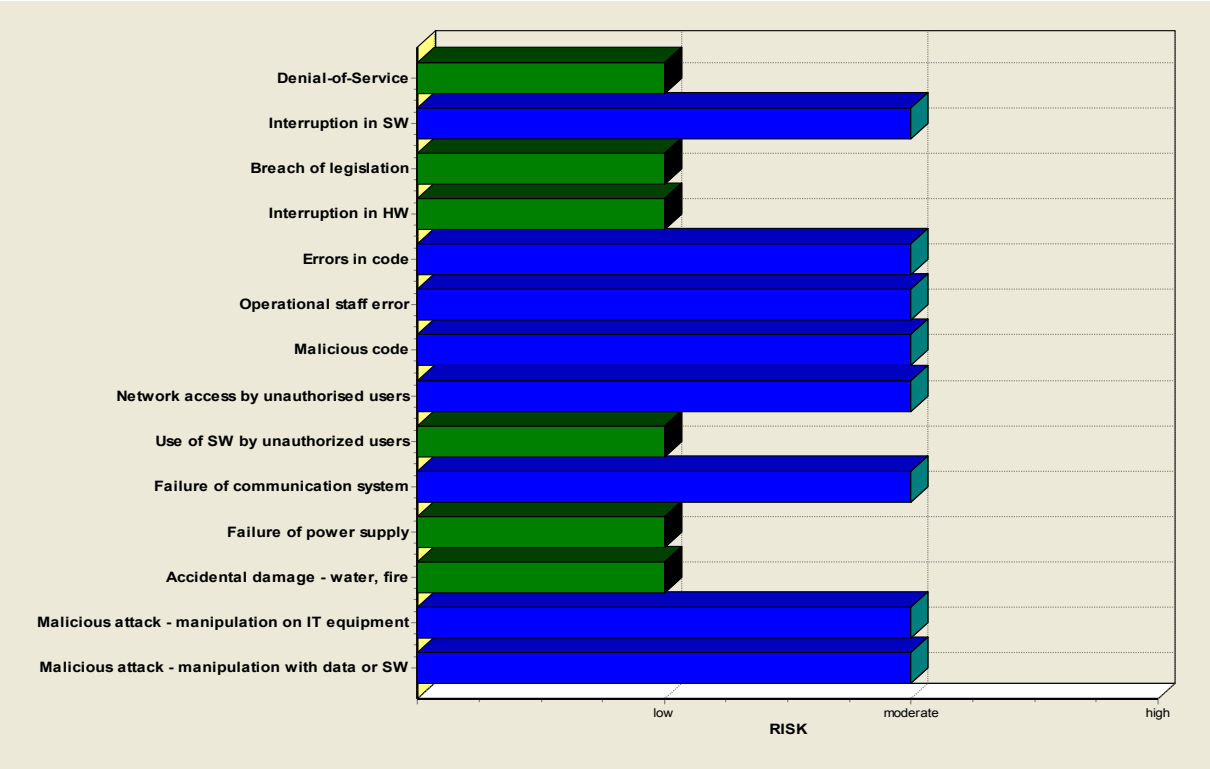
Management Controls

the controls that are already provided

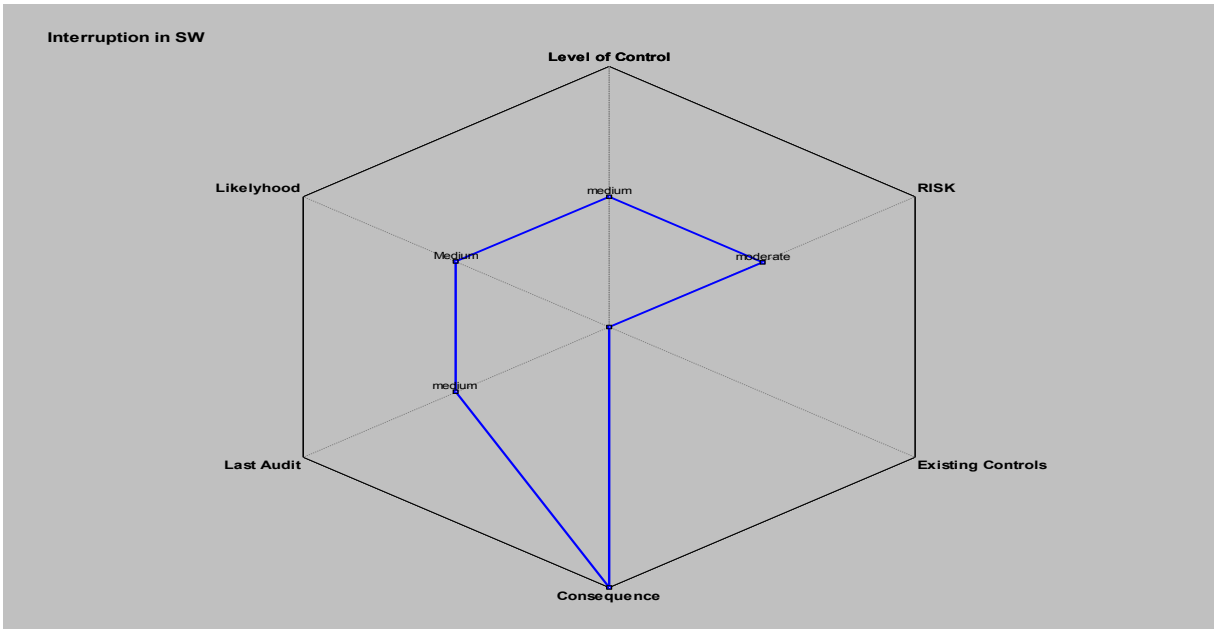
1.	*good*	the controls are in place for all process
2.	medium	controls are in place but not for entire process
3.	**bad**	controls are poor and in place for some part of the process

Slika 5: določitev strukture parametrov in njihovih zalog vrednosti

Na Sliki 6 so prikazana posamezna tveganja in njihove ocene za podproces ON-LINE PROCESSING. Iz grafa so jasno razvidne velikosti posameznih tveganj.



Slika 6: prikaz ocene tveganj za podproces ON-LINE PROCESSING



Slika 7: podrobnejši prikaz posameznega tveganja

Razviti model omogoča, da tveganja, ki so za nas zanimivejša, analiziramo podrobneje (Slika 7). Orodje nam tudi omogoča preigravanje različnih scenarijev, tako da za posamezno tveganje poljubno spreminjamo vrednosti parametrov in analiziramo dobljene rezultate. Na podlagi teh, lahko za zmanjševanje tveganja na sprejemljivi nivo, izberemo optimalne kontrole.

4 ZAKLJUČEK

V prispevku je predstavljen kvalitativni model za analizo in oceno tveganj, razvit s pomočjo programa DEXi in prikazan primer uporabe v praksi. Čeprav gre za kvalitativni model, čigar vrednost tveganj temelji na subjektivnih ocenah posameznikov, so dobljeni rezultati dovolj dobri za pomoč pri odločanju, katera tveganja so tako velika, da zahtevajo prioritetno reševanje.
Prav tako so dobljeni rezultati ocene tveganj s pomočjo razvitega modela jasni in razumljivi, pot do njih pa transparentna za odločevalca. Rezultati so prikazani s pomočjo grafov in tako z lahkoto predstavljivi tudi nestrokovnjakom za področje ocene tveganja. Model omogoča podrobnejši pregled posameznega tveganja in vzrokov zanj ter izvedbo t.i. what-if analize, tako da spremenimo vrednosti posameznih parametrov in primerjamo dobljene rezultate. Obstoječi model je zlahka prenosljiv tudi na druge vrste tveganj.

VIRI

Bankart d.o.o. (2007). *Metodologija upravljanja tveganj.* Ljubljana: Bankart d.o.o.

Bankart d.o.o.(2007) *Procesna shema.* Ljubljana: Bankart d.o.o.

Bertoncelj, B. (2007). *Operativna tveganja*. Ljubljana: Banka Slovenije.

Bradeško, L., Kušar, J. in Starbek, M.(2007). *Obvladovanje tveganj pri projektih naročil izdelkov/storitev.* Podčetrtek: Projektni forum.

BS ISO/IEC 17799:2005: *Code of practice for information security management.* BSI. 2005.

BS ISO/IEC 27001:2005: *Information Security Management Systems - Requirements.* BSI. 2005.

Department of Defence (2006). *Risk Management Guide for DoD Acquisition; sixth edition*. Pridobljeno 10. 08. 2006 na http://www.dau.mil/pubs/gdbks/docs/RMG%206Ed%20Aug06.pdf.

Information Systems Audit and Control Association (2006). *CISM Review Manual.* Pridobljeno 10. 12. 2006 na https://www.isaca.org/Pages/default.aspx

IT Governance Institute (2005). *COBIT*. Pridobljeno 12. 10. 2005 na http://www.itgi.org/

Jereb, E., Bohanec, M. in Rajkovič V. (2003). *DEXi - Računalniški program za večparametrsko odločanje*. Kranj: Založba Moderna organizacija.

NLB d.d. (1999). *Analiza tveganosti.* Ljubljana: NLB d.d.

Tipton F., H. in Krause, M. (2004) . *Information Security Management Handbook.* New York: Auerbach Publications.