Obvladovanje tveganj pri uporabi informacijske tehnologije v univerzitetnem okolju

Nataša Žabkar, Viljan Mahnič
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
natasa.zabkar@email.si, viljan.mahnic@fri.uni-lj.si

Povzetek

Vse večja uporaba informacijskih tehnologij (IT) v univerzitetnem okolju zahteva, da zagotovimo ustrezno stopnjo kakovosti, varnosti in zaupanja v rezultate pri uporabi IT. Vse to lahko dosežemo z upravljanjem IT. Pomemben del le-tega pa je obvladovanje tveganj, ki izvirajo iz uporabe IT. Namen tega prispevka je predstaviti pristop k obvladovanju IT tveganj, ki temelji na ogrodju za upravljanje informacijske tehnologije COBIT in je nadgrajen z uporabo "Standarda za obvladovanje tveganj" in standarda BS 7799. Najprej podamo pregled navedenih treh pristopov in potem opišemo naš pristop. Na koncu podamo še zgled, kako bi lahko uporabili predlagani pristop na primeru informacijskega sistema univerze za področje študijske informatike.
Ključne besede: COBIT, "Standard za obvladovanje tveganj", BS 7799.

Abstract

IT Risk Management in the University Environment

The increasing use of information technology (IT) in the university environment raises the importance of achieving quality and security, as well as satisfying fiduciary requirements of IT usage. These goals can be achieved through IT governance, an important part of which is IT risk management. The aim of this paper is to present an approach to IT risk management that is based on the IT governance framework COBIT and refined using of the standards "A Risk Management Standard" and BS 7799. We first give an overview of these three approaches and then describe our approach. Finally, we give an example of its usage in the Student Records Information System.
Keywords: COBIT, "A Risk Management Standard", BS 7799.

1 Uvod

Univerzitetni informacijski sistem je zelo pomemben za doseganje ciljev univerze, zato predstavlja pomembno sredstvo, ki ga je treba ustrezno varovati. Upravljanje informacijske tehnologije (angl. information technology governance) in obvladovanje tveganj informacijske tehnologije (angl. IT risk management) nam pri tem lahko pomagata. Za upravljanje IT je odgovorno poslovodstvo. Upravljanje IT zajema vodenje, organizacijsko strukturo in procese, ki zagotavljajo, da IT univerze ohranja in razširja strategijo in cilje univerze [16].

Dva glavna cilja upravljanja IT sta:

- zagotoviti, da bodo pričakovanja glede uporabe IT izpolnjena;
- zagotoviti, da bodo tveganja, povezana z uporabo IT ustrezno obvladovana.

V tem prispevku se bomo osredotočili na drugi cilj.

Obvladovanje tveganj IT dodaja in ohranja vrednost organizacije [01]. Ohranjanje ali varovanje vrednosti sredstev zajema tudi kontrole, s katerimi znižujemo tveganja na stopnjo, ki jo je opredelilo poslovodstvo v procesu obvladovanja tveganj. Eden izmed pogojev za ustrezno upravljanje IT je sistematični pristop k obvladovanju tveganj. Poznamo več pristopov, ponavadi pa se poslovodstvo odloči za tisto kombinacijo obstoječih pristopov, ki je po njegovi presoji za organizacijo najbolj ustrezna.

V finančnih organizacijah je obvladovanje tveganj določeno z zakonom, za razliko od univerzitetnega okolja, kjer je odločitev glede obvladovanja tveganj prepuščena poslovodstvu. Slovenska zakonodaja med drugim[1] določa, da morajo banke v poslovanju upoštevati slovenska standarda SIST BS 7799-2:2003 in SIST ISO/IEC 17799:2003, ki ju izdaja slovenski inštitut za standardizacijo oziroma drug pooblaščeni organ (UL RS št. 83/2004, 29.07.2004). Zahteva po obvladovanju tveganja je opredeljena v standardu BS 7799-2:2002

[05] v poglavju A.4.2 "Vzpostavitev in upravljanje SUVI (sistema za upravljanje varovanja informacij)". Obvladovanje tveganj je velikega pomena v bankah, kjer kakovost obvladovanja tveganj vpliva na zahteve glede najnižje zakonske kapitalske obveznosti za kritje tveganja. Tveganja IT uvrščamo med operativna tveganja, ki so predmet Novega baselskega sporazuma (New Basel Capital Accord) oziroma Basel II [04]. Spremljevalne dokumetne odprtega tipa, kot so "Postopki dobre prakse za obvladovanje in nadziranje operativnega tveganja" [03], je mogoče uporabiti tudi v drugih okoljih, npr. prvo načelo: "Nadzorni svet bi moral pomembnejše vidike operativnih tveganj banke obravnavati kot posebno in obvladljivo skupino tveganj ter sprejeti in občasno preverjati strategijo banke v odnosu do operativnih tveganj. Strategija naj bi odražala odpornost banke do teh tveganj in njeno poznavanje in razumevanje posebnih značilnosti tovrstnih tveganj. Potrditi oz. sprejeti bi moral tudi osnovno obliko organiziranosti za obvladovanje operativnega tveganja in zagotoviti, da uprava dejansko izvaja svoje naloge v zvezi z obvladovanjem tega tveganja."

Namen tega prispevka je predstaviti metodo za obvladovanje tveganj IT, ki bi bila primerna za univerzitetno okolje. Čeprav za univerze uporaba prej omenjenih standardov ni predpisana z zakonom, menimo, da je uporaba le-teh lahko v pomoč pri uvajanju obvladovanja tveganj IT v univerzitetnem okolju.

V naslednjem razdelku bomo opredelili obvladovanje tveganj in predstavili nekatere možne rešitve za zmanjšanje tveganj IT. Potem bomo predstavili naš pristop k obvladovanju tveganj IT kot eno izmed mogočih rešitev (razdelek 3) in podali zgled uporabe tega pristopa (razdelek 4). Na koncu bomo podali sklepne ugotovitve.

2 Obvladovanje tveganj IT

Obstaja več definicij tveganja, npr. "možnost, da se zgodi nekaj, kar bo vplivalo na cilje" [02]. V tem prispevku bomo uporabili naslednjo definicijo: "kombinacija verjetnosti dogodka in njegovih posledic (ISO/IEC Guide 73)" [01], ker vključuje pozitiven in negativen vidik tveganja.

Obstaja tudi več definicij obvladovanja tveganj. Ena izmed njih je "kultura, procesi in strukture, ki so usmerjeni k uspešnemu obvladovanju možnih priložnosti in neželenih učinkov" [02]. V tem prispevku bomo uporabili naslednjo definicijo: "proces, v katerem se organizacija metodično ukvarja s tveganji za vsako aktivnost in sicer z namenom doseganja stalne koristi v okviru vsake posamezne aktivnosti ter za portfelj vseh aktivnosti" [01] in sicer zato, ker poudarja doseganje ciljev.

Obvladovanje tveganj v splošnem je opisano v dokumentu "Standard za obvladovanje tveganj" (angl. "A Risk Management Standard") [01], ki je odprt standard in so ga razvile večje organizacije za obvladovanje tveganj v Veliki Britaniji. Podobno velja za avstralsko-novozelandski standard AS/NZS 4360:1999 "Obvladovanje tveganj" [02], ki pa je zaprt standard. Oba standarda podajata splošno ogrodje za obvladovanje tveganj, ki ni odvisno od posamezne panoge. Pred kratkim je bil objavljen še en dokument, ki opisuje ogrodje za obvladovanje tveganj v podjetjih – COSO-ERM: "Enterprise Risk Management Framework" [09] in je prav tako splošne narave.

Do sedaj smo opredelili obvladovanje tveganj v splošnem. V tem prispevku se bomo ukvarjali z obvladovanjem tveganj IT, ki je del splošnega obvladovanja tveganj. Obvladovanje tveganj IT je usmerjeno predvsem na operativna tveganja, ki so v Basel II [03] opredeljena na naslednji način: "tveganje izgube zaradi neustreznih ali neuspešnih notranjih postopkov, ljudi in sistemov ali zaradi zunanjih dogodkov". Nekateri primeri operativnih tveganj so: prekinitev poslovanja in sistemske napake (napake v strojni in programski opremi, telekomunikacijski problemi, izpadi sistema itn.), napake pri izvedbi procesov in upravljanju postopkov (napačen vnos podatkov, vzdrževanje ali polnjenje podatkov v bazo, napačno delovanje sistema/modela, vzdrževanje referenčnih podatkov, napačni podatki o komitentu itn.), poškodbe fizičnih sredstev (potresi, požari, poplave itn.) in drugi.

Obstaja večje število dokumentov, ki opisujejo proces obvladovanja tveganj IT, nekateri pa se nanašajo predvsem na varnostna tveganja IT:

[1] *Slovenska zakonodaja določa, da morajo prireditelji pri trajnem prirejanju klasičnih iger na srečo pri uporabi programske, računalniške, mrežne in telekomunikacijske opreme upoštevati določila slovenskega standarda s področja varovanja informacij (UL RS št. 70/2000, 8. 8. 2000); družbe za upravljanje morajo pri svojem poslovanju smiselno upoštevati slovenski standard PSIST BS 7799 Kodeks varovanja informacij (UL RS št. 80/2003, 14. 8. 2003); klirinška družba mora pri poslovanju upoštevati slovenski standard PSIST BS 7799 (UL RS št. 7/2003, 23. 01. 2003); pri družbah za izdajo elektronskega denarja mora revizor v dodatku revizorjevega poročila oceniti zlasti usklajenost s slovenskim standardom PSIST BS 7799 (UL RS št. 87/2002, 17. 10. 2002).*

- COBIT: Kontrolni cilji za IT in sorodne tehnologije (angl. "Control Objectives for Information and Related Technology") [07];
- PD 30002:2002: Vodič za oceno tveganj po BS 7799 (angl. "Guide to BS 7799 Risk Assessment") [23];
- NIST 800-300: Vodič za obvladovanje tveganj za sisteme informacijske tehnologije – priporočila Nacionalnega inštituta za standarde in tehnologijo [21];
- ISO/IEC TR 13335-n: Informacijska tehnologija – Smernice za obvladovanje varnosti IT (angl. "Information Technology – Guidelines for the management of IT security" [13];
- HB 231:2000: Smernice za obvladovanje tveganj informacijske varnosti (angl. "Information Security Risk Management Guidelines") [10];
- CCTA Metoda za analizo in obvladovanje tveganj [25];
- Microsoft Operations Framework v3.0: Obvladovanje tveganj v operativi [20].

Podrobnejši pregled drugih dokumentov s področja obvladovanja IT je podan v [18], opis enega izmed pristopov ("Analiza varnostne ogroženosti") pa v [17].

V naslednjem razdelku bomo podali kratek opis treh standardov oziroma smernic, ki smo jih uporabili pri oblikovanju našega pristopa: COBIT [07], "Standard za obvladovanje tveganj" [01] in BS 7799 [05]. Želeli smo uporabiti samo odprt pristop, opisan v COBIT-u, vendar smo ugotovili, da potrebujemo bolj podroben opis procesa obvladovanja tveganj. Tega smo našli v odprtem pristopu, opisanem v "Standardu za obvladovanje tveganj". Vendar pa je ta standard splošne narave, mi pa smo potrebovali smernice za obvladovanje tveganj IT. Le-te smo našli v zaprtem pristopu BS 7799, ki je zelo razširjen in velja za najboljšo prakso na področju varnosti IT.

2.1 COBIT: PO9 "Oceniti tveganja"

COBIT [07] je izdal Inštitut za upravljanje IT in predstavlja zbirko dokumentov, ki so najboljša praksa za upravljanje IT, kontrolo in zagotavljanje. Večina komponent COBIT je odprtega tipa.

COBIT ima 34 procesov in za vsak proces so opredeljeni podrobni cilji. Eden izmed teh procesov je PO9: "Oceniti tveganja" (oznaka PO9 je okrajšava za "Planiranje in organizacijo", kar je ena od štirih domen, v katere so razvrščeni vsi procesi v COBIT-u). Proces PO9 ima na nižjem nivoju 8 kontrolnih ciljev [07]:

- PO9.1: Ocena poslovnih tveganj (vzpostavitev ogrodja za sistematično oceno tveganj);
- PO9.2: Pristop k oceni tveganj (opredelitev obsega, metodologije, odgovornosti in veščin);
- PO9.3: Opredelitev tveganj (poslovnih, regulativnih, pravnih, tehnoloških, povezanih s poslovnimi partnerji in s človeškimi viri);
- PO9.4: Merjenje tveganj (kvalitativno in kvantitativno rangiranje tveganj);
- PO9.5: Plan aktivnosti za obravnavanje tveganj (izogibanje, blažitev, prevzem ali prenos tveganja);
- PO9.6: Prevzem tveganja (formalen prevzem preostalega tveganja);
- PO9.7: Izbira kontrol (kontrole, ki imajo največje koristi in najmanjše stroške – angl. "quick win");
- PO9.8: Zavezanost oceni tveganj (spodbujanje uporabe ocene tveganja).

Primerjava COBIT-a in standardov ISO/IEC 17799:2000 ter ISO/IEC TR 13335 (in drugih) je podana v [08].

Prednosti uporabe pristopa COBIT za obvladovanje tveganj IT sta:

- primernost za organizacije, ki že uporabljajo COBIT;
- primernost za brezplačen prenos znanja (odprt pristop).

Pomanjkljivosti uporabe pristopa COBIT pa sta:

- zahtevnost in pomanjkanje formalnega izobraževanja za organizacije, ki še ne uporabljajo COBIT-a;
- uporaba COBIT-a ni tako razširjena kot uporaba BS 7799.

2.2 "Standard za obvladovanje tveganj" (SOT)

Standard za obvladovanje tveganj (SOT) [01] je odprt standard, ki so ga razvile večje organizacije za obvladovanje tveganj v Veliki Britaniji: (1) Inštitut za obvladovanje tveganj (IRM), (2) Združenje menedžerjev za zavarovanja in tveganja (AIRMIC) in (3) ALARM Nacionalni forum za obvladovanje tveganj v javnem sektorju (ALARM). Standard za obvladovanje tveganj predstavlja najboljšo prakso, ki jo organizacije lahko uporabijo za primerjavo oziroma merjenje. V skladu s tem standardom je proces obvladovanja tveganj sestavljen iz naslednjih korakov:

- Korak 1: Strateški cilji organizacije;
- Korak 2: Ocena tveganja;
- Korak 3: Poročanje in komuniciranje o tveganjih (Grožnje in priložnosti);

- Korak 4: Odločitev;
- Korak 5: Obravnavanje tveganj (izbira in uvedba ukrepov za obravnavanje tveganj, stroški in koristi kontrol);
- Korak 6: Poročanje o preostalem tveganju (notranje, zunanje);
- Korak 7: Nadzor in pregled procesa obvladovanja tveganj (spremembe, zagotavljanje).

Drugi korak ima naslednje podkorake:

- Korak 2.1: Analiza tveganj;
- Korak 2.1.1: Opredelitev tveganj (strateška, operativna, finančna, obvladovanje znanja, skladnost);
- Korak 2.1.2: Opis tveganj (strukturiran format, ki zajema naziv, obseg, naravo, deležnike, kvantifikacijo, tolerance/odnos do tveganj (angl. risk tolerance/appetite), obravnavanje tveganj in kontrolne mehanizme, možne aktivnosti za izboljšavo, razvoj strategije in politike);
- Korak 2.1.3: Ocena tveganja (kvantitativna, semikvantitativna, kvalitativna);
- Korak 2.2: Ovrednotenje tveganj (primerjava ocenjenih tveganj glede na izbrani kriterij, stroški/koristi, regulativne zahteve, socioekonomski in okoljski dejavniki).

Prednosti uporabe SOT sta:

- enostavnost;
- primernost za brezplačen prenos znanja (odprt pristop).

Pomanjkljivosti pristopa SOT pa sta:

- ne vsebuje posebnosti obvladovanja tveganj IT;
- uporaba SOT ni tako razširjena kot uporaba BS 7799.

2.3 Standard BS 7799-2:2002

Standard BS 7799-2:2002 "Sistemi za upravljanje varovanja informacij – specifikacija s smernicami za uporabo" [05] opredeljuje naslednje korake vzpostavitve sistema za upravljanje varovanja informacij (SUVI):

- Opredeliti namen SUVI;
- Opredeliti politiko SUVI;
- Opredeliti sistematičen pristop k ocenjevanju tveganja;
- Določiti tveganja;
- Oceniti tveganja;
- Določiti in ovrednotiti možnosti za obravnavanje tveganja;
- Izbrati kontrolne cilje in kontrole za obravnavanje tveganj;
- Pripraviti izjavo o primernosti;
- Pridobiti odobritev vodstva za preostala predlagana tveganja in odobritev za uvedbo in izvajanje SUVI.

V dokumentu PD 3002: 2002 [23] so podane smernice za uporabo standarda BS 7799. V skladu s PD 30002:2002 je proces obvladovanja tveganj sestavljen iz naslednjih korakov:

- Korak 1: Opredelitev sredstev (izhod: popis sredstev, lokacij in lastnikov);
- Korak 2: Vrednotenje sredstev (izhod: pomen vsakega sredstva);
- Korak 3: Opredelitev varnostnih zahtev (izhod: seznam groženj in ranljivosti za vsako sredstvo, pravne/pogodbene in poslovne zahteve za vsako sredstvo);
- Korak 4: Ocena varnostnih zahtev (izhod: ocena za vsako varnostno zahtevo);
- Korak 5: Izračun varnostnih tveganj (izhod: seznam izmerjenih tveganj za vsako sredstvo);
- Korak 6: Opredelitev in ovrednotenje možnosti za obravnavanje tveganj (izhod: možnosti obravnavanja tveganja za vsako tveganje);
- Korak 7: Izbor varnostnih kontrol (izhod: izbrane kontrole za vsako tveganje).

Prvi korak je v [12] predstavljen z uporabo procesnega pristopa:

- Korak 1.1: Opredelitev poslovnih procesov znotraj obsega;
- Korak 1.2: Opredelitev povezav med izbranimi procesi;
- Korak 1.3: Opredelitev sredstev za izbrane procese: informacijski vhodi, izhodi, zapisi in viri (človeški viri, okolje, oprema, orodja, komunikacije in drugo).

Razumevanje in komunikacijo pri začetnih korakih je mogoče izboljšati z grafično predstavitvijo procesov in sredstev.

Prednosti pristopa BS 7799 so:

- razširjenost uporabe in določila v zakonodaji;
- podprtost z ustrezno dokumentacijo in izobraževanjem;
- možnost certificiranja.

Pomanjkljivosti pristopa BS 7799 pa sta:

- ni primeren za brezplačen prenos znanja (zaprt pristop);
- omejen je samo na varnostna tveganja.

3 Opis pristopa "UN-OT"

Pristop "UN-OT" (univerzitetno okolje – obvladovanje tveganj), ki ga predlagamo za obvladovanje tveganj IT

v univerzitetnem okolju, temelji na pristopu COBIT in je nadgrajen z uporabo pristopov SOT in BS 7799. Pristop "UN-OT" vključuje tiste dele prej omenjenih pristopov, ki so po našem mnenju najbolj primerni za uporabo v univerzitetnem okolju.

Pristop COBIT smo izbrali za osnovo zato, ker je odprt in ker imamo na univerzi že nekaj izkušenj z njegovo uporabo. Da bi zmanjšali pomanjkljivost glede zahtevnosti, smo ga nadgradili z uporabo pristopa SOT, ki je zelo enostaven za uporabo. Ker pa SOT ni prilagojen za tveganja IT, smo končno prilagoditev izvedli z uporabo pristopa BS 7799.

V okviru pristopa "UN-SOT" smo proces obvladovanja tveganj razdelili na 7 korakov, katerih opis sledi v nadaljevanju. Pri vsakem koraku je v oklepaju naveden pristop, ki je bil uporabljen kot osnova za njegovo oblikovanje.

- Korak 1: Strateški cilji organizacije na področju IT (pristop SOT);
- Korak 2: Opredelitev in ovrednotenje sredstev (pristop BS 7799);
- Korak 3: Ocena groženj in ranljivosti (pristop BS 7799);
- Korak 4: Merjenje tveganj (pristopi COBIT, SOT, BS 7799);
- Korak 5: Prevzem tveganj (pristopi COBIT, SOT, BS 7799);
- Korak 6: Obravnavanje tveganj (pristopi COBIT, SOT, BS 7799);
- Korak 7: Nadzor in pregled (pristop SOT).

3.1 Strateški cilji organizacije na področju IT

Proces obvladovanja tveganj se prične z opredelitvijo strateških ciljev organizacije na področju IT [01], ki so ponavadi navedeni v ustreznih strateških dokumentih.

V tem koraku opredelimo cilje in jim določimo prioriteto: zelo visoka (ZV), visoka (V), srednja (S) in nizka (N). Za cilje z najvišjo prioriteto opredelimo procese. En cilj ima lahko več procesov: za vsak proces najprej opredelimo njegovo prioriteto, nato pa določimo še povezave med procesi [12]. Pri tem nam je lahko v pomoč grafična predstavitev obsega v obliki diagrama procesov.

Rezultat prvega koraka je register ciljev in procesov. Register ciljev in procesov vključuje številko cilja, naziv cilja in njegovo prioriteto. Za vsak cilj so v registru navedeni procesi, ki so potrebni za doseganje tega cilja. Opis vsakega procesa obsega številko procesa, naziv procesa in njegovo prioriteto.

Viri za obvladovanje tveganja so pogosto omejeni in ponavadi ni mogoče izvesti ocene tveganj za vse cilje že pri prvem poskusu. Zato izberemo cilje in procese, ki imajo najvišjo prioriteto in so v našem obsegu.

3.2 Opredelitev in ovrednotenje sredstev

V tem koraku najprej opredelimo sredstva za izbrane procese: informacijske vhode, izhode, zapise in vire (človeške vire, okolje, opremo, orodja, komunikacije in drugo). Potem določimo pomen vsakega sredstva: zelo visok (ZV), visok (V), srednji (S) ali nizek (N). Pravilnost ocene pomena preverijo lastniki procesov in poslovodstvo [12].

Rezultat opredelitve in ovrednotenja sredstev je register sredstev, v katerem so za vsak proces iz koraka 1 navedena pripadajoča sredstva (številka in naziv sredstva), njihova lokacija, lastnik in pomen.

3.3 Ocena groženj in ranljivosti

Standardi, ki obravnavajo obvladovanje tveganj IT, vključujejo opredelitev groženj in ranljivosti. Povezava med tveganjem, grožnjo in ranljivostjo je podana v [13]: tveganje je možnost, da bo določena grožnja izrabila ranljivost sredstva ali skupine sredstev in povzročila škodo ali uničenje sredstev.

Grožnja je možen vzrok neželenega incidenta, ki ima lahko za posledico škodo na sistemu ali v organizaciji (npr. požar v sistemski sobi). Ranljivost je pomanjkljivost sredstva ali skupine sredstev, ki jih lahko grožnja izrabi [13] (npr. pomanjkanje protipožarne zaščite v sistemski sobi). Nekateri seznami splošnih groženj in ranljivosti so odprtega tipa, npr. [22], [19] in [11].

V tem koraku opredelimo grožnje in ranljivosti za sredstva, ki so navedena v registru sredstev. Za namen tega prispevka bomo kombinacijo grožnje in ranljivosti poimenovali škodni dogodek. Za vsak škodni dogodek moramo oceniti verjetnost, da se bo zgodil, ter posledice tega dogodka. V oceno groženj in ranljivosti lahko vključimo oceno priložnosti (pozitivni vidik tveganja). V tem primeru moramo oceniti verjetnost, da se bo priložnost realizirala ter posledice njene realizacije.

Rezultat ocene groženj in ranljivosti je register groženj in ranljivosti, v katerem so za vsako sredstvo iz koraka 2 navedene vse grožnje (številka grožnje in naziv grožnje), za vsako grožnjo pa vse ranljivosti (številka ranljivosti, naziv ranljivosti). Vsako kombinacijo grožnje in ranljivosti označimo kot škodni dogodek ter ocenimo njegovo verjetnost in možne posledice.

3.4 Merjenje tveganj

V četrtem koraku izračunamo tveganje glede na vrednosti sredstev, groženj in ranljivosti. Izračun tveganja je lahko kvalitativen ali kvantitativen. V pristopu UN-OT smo uporabili kvalitativen način, ki je predstavljen v tabeli 1. Vsak element tabele predstavlja stopnjo tveganja v odvisnosti od verjetnosti, da pride do nekega škodnega dogodka, in posledic, ki jih ta škodni dogodek ima za organizacijo.[2] Če je npr. verjetnost dogodka visoka in posledica srednja, je stopnja tveganja visoka.

Rezultat merjenja tveganj je register tveganj, ki za vsak škodni dogodek iz koraka 3 vsebuje izračunano stopnjo tveganja tega dogodka [12].

Tabela 1: **Merjenje tveganj**

Verjetnost /Posledica	Nizka	Srednja	Visoka	Zelo visoka
Nizka	Nizka	Srednja	Srednja	Visoka
Srednja	Srednja	Srednja	Visoka	Visoka
Visoka	Srednja	Visoka	Visoka	Zelo visoka
Zelo visoka	Visoka	Visoka	Zelo visoka	Zelo visoka

3.5 Prevzem tveganj

V petem koraku poslovodstvo določi stopnjo tveganja, ki je še sprejemljiva. Stopnja sprejemljivega tveganja določa profil tveganj, ki je osnova za profil kontrol (korak 6).

Uporabili smo stopnjo sprejemljivega tveganja, ki je podana v tabeli 2. Če je stopnja tveganja nizka ali srednja, potem bo poslovodstvo sprejelo tveganje. Če pa je stopnja tveganja visoka ali zelo visoka, potem poslovodstvo tveganja ne bo sprejelo.

Tabela 2: **Stopnja sprejemljivega tveganja**

Verjetnost /Posledica	Nizka	Srednja	Visoka	Zelo visoka
Nizka	Nizka	Srednja	Srednja	**Visoka**
Srednja	Srednja	Srednja	**Visoka**	**Visoka**
Visoka	Srednja	**Visoka**	**Visoka**	**Zelo visoka**
Zelo visoka	**Visoka**	**Visoka**	**Zelo visoka**	**Zelo visoka**

Rezultat tega koraka je dopolnjen register tveganj, v katerem je za vsako tveganje dodana še stopnja sprejemljivega tveganja. Tako dopolnjenen register predstavlja t. i. "profil tveganj", ki prikazuje, katera tveganja je poslovodstvo sprejelo in katerih ne [12].

3.6 Obravnavanje tveganj

V tem koraku poslovodstvo izbere način obravnavanja tveganj. Možni načini obravnavanja so štirje (angl. "4T"):

- zmanjšanje tveganja (angl. treat);
- prenos tveganja (angl. transfer);
- izogibanje tveganju (angl. terminate) in
- sprejem tveganja (angl. tolerate).

Za tveganja, za katera je poslovodstvo izbralo prvi način (tj. zmanjšanje tveganja), lahko izberemo kontrole iz standardov oziroma smernic, kot so:[3]

- BS 7799 [05];
- COBIT [07];
- ISF: "The standard of good practice for information security" [14];
- BSI: "The Baseline Protection Manual" [06];
- OIT: "Information Security Guideline for NSW Government – Part 3: Information security baseline controls" [22];
- SSE-CMM: "System Security Engeneering Capability Maturity Model" [15] in drugi.

Rezultat obravnavanja tveganj je register tveganj, ki poleg elementov, navedenih v točki 3.5, vključuje še način obravnavanja in kontrole, stopnjo zagotavljanja ter stopnjo preostalega tveganja.

3.7 Nadzor in pregled

Z nadzorom pridobimo zagotovilo, da so kontrole ustrezne in da zaposleni razumejo in izvajajo predpisane postopke [01]. Tveganja niso nikoli statična, zato je potreben nadzor in pregled tveganj, ki zagotavlja ažurnost registra tveganj.

Rezultat obravnavanja tveganj je register tveganj, ki poleg elementov, navedenih v točki 3.6, vključuje še dopolnitve, pripravljene na osnovi poročil o nadzoru in pregledu.

4 Primer uporabe pristopa UN-OT

Uporabo pristopa UN-OT bomo podali na namišljenem primeru informacijskega sistema za področje študijske informatike.

---

[2] *Vrstice tabele predstavljajo stopnjo verjetnosti, da pride do škodnega dogodka, stolpci pa resnost posledic, ki jih le-ta povzroči.*

[3] *V ta namen so uporabne tudi naloge za pridobitev certifikatov s področja varnosti informacij [24].*

4.1 Strateški IT cilji organizacije

Izhajali bomo iz predpostavke, da je eden izmed ciljev univerze nuditi uporabnikom (predvsem profesorjem in študentom) visoko kakovost administrativnih storitev. Ta cilj je povezan z informacijskim sistemom za področje študijske informatike, ki je del univerzitetnega informacijskega sistema in vsebuje naslednje module:

- obdelava vpisnih podatkov (zajem podatkov o vpisanih študentih, seznami vpisanih študentov, razna statistična poročila);
- izpitna evidenca (razpisovanje izpitnih rokov, prijavaljanje na izpite, podatki o doseženih ocenah);
- evidenca diplomantov (administrativni postopki od dviga teme do zagovora, izdelava priloge k diplomi, seznami diplomantov);
- analize uspešnosti študija (prehodnost iz letnika v letnik, napredovanje čiste generacije, analiza opravljanja izpitov pri posameznih predmetih, povprečne ocene, rang lestvica študentov).

Informacijski sistem je realiziran kot spletna aplikacija, ki uporabnikom omogoča oddaljen dostop do podatkov, kar je še posebej pomembno za študente in profesorje, ki lahko uporabljajo sistem od koderkoli, pomembno je le, da imajo na razpolago dostop do interneta.

Za doseganje na začetku omenjenega cilja so najpomembnejši tisti procesi, v katere je vključenih največ uporabnikov. V našem primeru sta to obdelava vpisnih podatkov in izpitna evidenca, ker vključujeta komunikacijo s profesorji in študenti, ki pričakujejo dogovorjeni nivo storitev.

Rezultat tega koraka je register ciljev in procesov, podan v tabeli 3. Na enak način bi lahko opisali še druge cilje in za vsak cilj določili procese, ki so potrebni za njihovo realizacijo.

4.2 Opredelitev in ovrednotenje sredstev

Rezultat tega koraka je register sredstev, podan v tabeli 4. Vrednost sredstev se nanaša na pomembnost sredstev pri izvajanju izbranih procesov, kar je možno zapisati v komentarju. Vrednosti sredstev naj bi določili lastniki procesov in poslovodstvo. Na koncu je podan rang vsakega sredstva, ki odraža prioriteto tega sredstva.

ID Cilja	Opis	Prioriteta	ID procesa	Opis	Prioriteta	Komentar
1	2	3	4	5	6	7
C001	Zagotoviti uporabnikom visoko kakovost administrativnih storitev	Zelo visoka	P001	Obdelava vpisnih podatkov	Zelo visoka	
			P002	Izpitna evidenca	Zelo visoka	Problemi v preteklosti
	Drugi cilji					

Tabela 3: **Korak 1: Strateški IT cilji organizacije**

ID Sredstva	Opis	Lastnik	Lokacija	Pomen sredstva	Rang	Komentar
1	2	3	4	5	6	7
S001	Programi za vodenje izpitne evidence	Vodja oddelka IT	Strežnik fakultete	Zelo visoka	1	Ključna komponenta
S002	Strežnik	Vodja oddelka IT	Sistemska soba fakultete	Visoka	2	
S003	Podatki o izpitnih rokih	Vodja študentske pisarne	Študentska pisarna	Visoka	3	
S004	Podatki o študentih, ki so prijavljeni na izpit	Vodja študentske pisarne	Študentska pisarna	Visoka	4	
S005	Podatki o vpisanih študentih	Vodja študentske pisarne	Študentska pisarna	Srednja	5	
S006	Zaposleni v študentski pisarni		Študentska pisarna	Visoka	6	
	Druga sredstva					

Tabela 4: **Korak 2: Opredelitev in ovrednotenje sredstev za cilj C001 in proces P002**

4.3 Ocena groženj in ranljivosti

V tem koraku opredelimo grožnje in ranljivosti za vsako sredstvo. Za vsak škodni dogodek (kombinacija grožnje in ranljivosti) ocenimo verjetnost in posledico. Ocene podajo lastniki in uporabniki sredstev. Zgled za sredstvo S001 je podan v tabeli 5, ki je del registra groženj in ranljivosti.

4.4 Meritev tveganj

Sedaj moramo določiti stopnjo tveganja za vsak škodni dogodek. Stopnjo tveganja izračunamo kot produkt verjetnosti dogodka in posledice dogodka (glej tabelo 1).

V tabeli 6 je podan zgled meritve tveganj za škodne dogodke D001 (napaka v programski opremi kot posledica nizke kakovosti specifikacij programske opreme), D002 (napaka v programski opremi kot posledica nizke stopnje sodelovanja z uporabniki) in D003 (napaka v programski opremi kot posledica nizke stopnje kakovosti testiranja programske opreme), do katerih lahko pride zaradi grožnje G001 (napake v programski opremi) in ranljivosti R001 (nizka kakovost specifikacij programske opreme), R002 (nizka stopnja sodelovanja z uporabniki) in R003 (nizka stopnja kakovosti testiranja programske opreme).

4.5 Prevzem tveganja

V praksi bi bilo predrago, če bi se ukvarjali z vsemi tveganji. Zato poslovodstvo določi pomembnost tveganj in prioriteto porabe pogosto omejenih virov z namenom izboljšanja stopnje tveganja.

ID dogodka	Verjetnost	Posledica	Izračunana stopnjatveganja (2x3)	Komentar
1	2	3	4	5
D001	Zelo visoka	Zelo visoka	Zelo visoka	Ključna komponenta
D002	Zelo visoka	Zelo visoka	Zelo visoka	
D003	Zelo visoka	Zelo visoka	Zelo visoka	Ključna komponenta

Tabela 6: **Korak 4: Merjenje tveganj za dogodke D001, D002 in D003**

Stopnja sprejemljivega tveganja določa stopnjo tveganja, ki ga je poslovodstvo še pripravljeno sprejeti. Če stopnja sprejemljivega tveganja ni enaka stopnji izračunanega tveganja, nastopi razkorak, ki ga skušamo premostiti v koraku obravnavanja tveganj. Navedeno lahko zapišemo v obliki formule:

Razkorak = + Izračunana stopnja tveganja
- Stopnja sprejemljivega tveganja

V tabeli 7 je podan zgled za dogodke D001, D002 in D003. Za dogodka D001 in D003 je stopnja sprejemljivega tveganja nizka, za dogodek D002 pa je stopnja sprejemljivega tveganja srednja. To pomeni, da bo poslovodstvo moralo ukrepati tako, da se bo izračunana stopnja tveganja znižala in postala enaka sprejemljivi, tj. nizka za dogodka D001 in D003 oziroma srednja za dogodek D002. Da bi premostilo razkorak, lahko poslovodstvo visoka in zelo visoka tveganja zmanjša, prenese ali se jim izogne.

ID Grožnje	Grožnja	ID Ranljivosti	Ranljivost	Dogodek	Verjetnost	Posledica
1	2	3	4	5	6	7
G001	Napake v programski opremi	R001	Nizka kakovost specifikacij programske opreme	D001	Zelo visoka	Zelo visoka
		R002	Nizka stopnja sodelovanja z uporabnikom	D002	Zelo visoka	Zelo visoka
		R003	Nizka kakovost testiranja programske opreme	D003	Zelo visoka	Zelo visoka
G002	Uporabniške napake	R004	Nizka kakovost funkcije nudenja pomoči	D004	Srednja	Srednja
		R005	Nizka kakovost navodil	D005	Srednja	Srednja
G003	Napake v podatkih	R006	Nizka kakovost vhodnih kontrol	D006	Srednja	Zelo visoka
		R007	Nepričakovane vrednosti	D007	Nizka	Zelo visoka
	Druge grožnje					

Tabela 5: **Korak 3: Ocena groženj in ranljivosti za sredstvo S001**

ID dogodka	Izračunana stopnja tveganja	Stopnja sprejemljivega tveganja	Komentar
1	2	3	4
D001	Zelo visoka	Nizka	Razkorak (Zelo visoka - Nizka)
D002	Zelo visoka	Srednja	Razkorak (Zelo visoka - Srednja)
D003	Zelo visoka	Nizka	Razkorak (Zelo visoka - Nizka)

Tabela 7: **Korak 5: Stopnja sprejemljivega tveganja za dogodke D001, D002 in D003**

4.6 Obravnavanje tveganj

Potem ko je bila v koraku 5 določena stopnja še sprejemljivega tveganja, v koraku 6 izberemo tveganja, s katerimi se bomo najprej ukvarjali. Ker že imamo profil tveganj (korak 5), lahko ustrezno prilagodimo profil kontrol. Kontrole izberemo tako, da je stopnja tveganja, ki še ostane po uvedbi ustrezne kontrole, manjša ali enaka stopnji sprejemljivega tveganja. Navedeno lahko zapišemo v obliki formule:

Stopnja
preostalega tveganja = + Izračunana stopnja tveganja
- Stopnja zagotavljanja

Kontrole, s katerimi želimo doseči zahtevano stopnjo zagotavljanja, lahko izberemo iz ogrodja COBIT, standarda BS 7799 ali drugih dokumentov, navedenih v točki 3.6. Izbor ustreznih kontrol opravi poslovodstvo.

V tabeli 8 je prikazan del registra tveganj, iz katerega so razvidne kontrole, ki lahko pripomorejo k zmanjšanju tveganja zaradi dogodka D003.

Pri določitvi kontrol smo izhajali iz naslednjih procesov ogrodja COBIT [07]:

- COBIT AI5: "Namestiti in potrditi sisteme" ter
- COBIT AI6: "Obvladovati spremembe".

V teh procesih so vključene naslednje kontrole:

- distribucija programske opreme je dovoljena samo po izvedenem testiranju;
- testiranje se izvaja v okolju, ki ustreza produkcijskemu okolju;
- napake po testiranju se analizirajo in izvedejo se ustrezne aktivnosti.

4.7 Nadzor in pregled

V tem koraku izvajamo nadzor in pregled tako, da analiziramo incidente in ugotavljamo stopnjo skladnosti s standardi in postopki. Eden izmed možnih rezultatov je del registra tveganj, podan v tabeli 9.

5 Sklep

Dva osnovna cilja upravljanja IT sta: zagotoviti, da bo uporaba IT dala pričakovane rezultate, in zagotoviti, da bodo tveganja IT ustrezno obvladovana. Uspešno obvladovanje tveganj IT je pomembno za univerzo, ker pomaga dodati in zaščititi vrednost njenih sredstev, kot je univerzitetni informacijski sistem.

V prispevku smo predstavili pristop k obvladovanju tveganj IT v univerzitetnem okolju, ki smo ga poimenovali UN-OT. Naš pristop temelji na odprtem ogrodju za upravljanje informacijske tehnologije COBIT in je nadgrajen z uporabo odprtega standarda

ID dogodka	Izračunana stopnja tveganja	Stopnja sprejemljivega tveganja	Kontrole	Stopnja zagotavljanja	Stopnja preostalega tveganja	Komentar
1	2	3	4	5	6	7
D003	Zelo visoka	Nizka	COBIT AI5, AI6 Distribucija programske opreme je dovoljena samo po izvedenem testiranju	Visoka	Nizka (Zelo visoka – Visoka)	Hitra izboljšava (ang. quick win)
			COBIT AI5, AI6 Testiranje se izvaja v okolju, ki ustreza produkcijskemu okolju	Zelo visoka	Nizka (Zelo visoka – Zelo visoka)	Višji stroški priprave ustreznega testnega okolja
			COBIT AI5, AI6 Napake po testiranju se analizirajo in izvedejo se ustrezne aktivnosti	Srednja	Srednja (Zelo visoka – Srednja)	Reaktivni pristop

Tabela 8: **Korak 6: Obravnavanje tveganj za dogodek D003**

ID dogodka	Izračunana stopnja tveganja	Stopnja sprejemljivega tveganja	Kontrole	Stopnja zagotavljanja	Stopnja preostalega tveganja	Nadzor in pregled
1	2	3	4	5	6	7
D003	Zelo visoka	Nizka	COBIT AI5, AI6 Distribucija programske opreme je dovoljena samo po izvedenem testiranju	Visoka	Nizka	Testiranje se izvaja vedno.
			COBIT AI5, AI6 Testiranje se izvaja v okolju, ki ustreza produkcijskemu okolju	Zelo visoka	Nizka	Okolje, ki ustreza produkcijskemu, bo pripravljeno do roka X.
			COBIT AI5, AI6 Napake po testiranju se analizirajo in izvedejo se ustrezne aktivnosti	Srednja	Srednja	Vzroki napak niso bili ugotovljeni za X % vseh napak.

Tabela 9: **Korak 7: Nadzor in pregled za dogodek D003**

"Standard za obvladovanje tveganj" (SOT) in zaprtega standarda za varovanje informacij BS 7799. Da bi ilustrirali ustreznost pristopa UN-OT za univerzitetno okolje, smo predstavili njegovo uporabo na primeru informacijskega sistema za področje študijske informatike. V prikazanem primeru smo se lotili zmanjševanja stopnje tveganja napak v programski opremi z uvedbo kontrol, ki zagotavljajo višjo kakovost testiranja programske opreme.

Literatura

[01] AIRMIC, ALARM, IRM: "A Risk Management Standard". The Association of Insurance and Risk Managers (AIRMIC), ALARM The National Forum for Risk Management in Public Sector, The Institute of Risk Management (IRM), Velika Britanija, (2000). www.airmic.com, www.alarm-uk.com, www.theirm.org

[02] AS/NZS 4360:1999 "Risk Management". Australian standards, Australija, (1999).

[03] Basel Committee on Banking Supervision: "Sound Practices for the Management and Supervision of Operational Risk", (February 2003). www.bis.org/publ/bcbs96.pdf Prevod Banke Slovenije: www.bsi.si/html/basel2/03_aktivnosti/dokumenti/Operativno%20tveganje_bs-nbp.pdf

[04] Basel Committee on Banking Supervision: "The New Basel Capital Accord - Annex 7: Detailed loss event type classification", (April 2003). www.bis.org/publ/cp3annex.pdf Prevod Banke Slovenije: www.bsi.si/html/basel2/05_publikacije/dokumenti/C/povzetki/Operativno%20tveganje_CP_3.pdf

[05] BS 7799-2:2002: "Sistemi za upravljanje varovanja informacij – specifikacije s smernicami za uporabo", slovenski prevod BS 7799-2:2002: "Information security management systems – Specifications with guidance for use" (British Standard Institute). Inštitut za informacijsko varnost, Šempeter pri Gorici, 2003.

[06] BSI: "The Baseline Protection Manual". Das Bundesamt für Sicherheit in der Informationstechnik (BSI), Nemčija. www.bsi.de/gshb/english/download/index.html

[07] "COBIT 3rd edition: Control Objectives for Information and Related Technology". IT Governance Institute, ZDA (2000). www.isaca.org, www.itgi.org

[08] "COBIT Mapping: Overview of International IT Guidance". IT Governance Institute, ZDA, (2004). www.itgi.org

[09] COSO-ERM: "Enterprise Risk Management Framework". The Committee of Sponsoring Organizations of the Treadway Commission, ZDA, 2004. www.coso.org/

[10] HB 231:2000 "Information Security Risk Management Guidelines". Australian standards, Australija, (2000).

[11] ICAT: "Metabase of computer vulnerabilities". NIST, ZDA. http://icat.nist.gov/icat.cfm

[12] "Implementing BS 7799-2: 2002". British Standard Institution, Delegate Workbook for IT06, Issue 9, (september 2002).

[13] ISO/IEC TR 13335-n "Information Technology – Guidelines for the management of IT Security". ISO/IEC, Switzerland, (1998).

[14] ISF: : "The standard of good practice for information security". Information Security Forum, ZDA (2003). www.securityforum.org/html/frameset.htm

[15] ISSEA: "System Security Engeneering Capability Maturity Model" (SSE-CMM – ISO/IEC 21827) The International Systems Security Engineering Association (ISSEA). www.sse-cmm.org/lib/lib.asp

[16] IT Governance Institute: "IT Governance Executive Summary". IT Governance Institute, USA. www.itgi.org

[17] Jaušovec, Matjaž, Brumen, Boštjan, Welzer - Družovec, Tatjana: "Analiza varnostne ogroženosti". Uporabna informatika, Ljubljana, letnik 2003, št. 2, str. (61–67).

[18] Lalovič, Dušan: "Sistematični pristopi obvladovanja varnosti informacijskih sistemov združb". Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, magistrska naloga (2003).

[19] MITRE: "Common Vulnerabilities and Exposures". MITRE, ZDA. http://cve.mitre.org/cve/

[20] MOF: "Risk Management Discipline for Operations". Microsoft Operations Framework v3.0, ZDA (January 2004) http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofrisk.mspx

[21] NIST: "Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology". National Institute of Standards and Technology, ZDA (2001). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[22] OIT: "Information Security Guideline for NSW Government". Department of Commerce, Office of Information Technology, Australia. www.oit.nsw.gov.au/content/2.3.Guidelines.asp

[23] PD 3002:2002 "Guide to BS 7799 Risk Assessment". British Standards Institution, UK, (2002).

[24] SANS-GIAC: "Seminarske naloge". The SANS (SysAdmin, Audit, Network, Security) Institute, GIAC (Global Information Assurance Certification), ZDA. http://www.giac.org/GCIH.php

[25] Šinigoj, Aleksander: "CRAMM kot orodje za oceno in upravljanje s tveganji". Slovenski inštitut za revizijo in slovenski odsek ISACA, Zbornik referatov 10. mednarodne konference o revidiranju in kontroli informacijskih sistemov (Čatež, 24.–26. 09. 2002), str. 315-324 (2002).

Nataša Žabkar je diplomirala leta 1989 na Fakulteti za računalništvo in informatiko in magistrirala leta 1998 na Ekonomski fakulteti Univerze v Ljubljani. Ukvarja se predvsem z revizijo informacijskih sistemov. Na tem področju je leta 2000 pridobila naziv preizkušeni revizor informacijskih sistemov leta in leta 2001 naziv "CISA – Certified Information Systems Auditor".

Viljan Mahnič je izredni profesor in predstojnik Laboratorija za tehnologijo programske opreme na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. V letih 1999–2003 je bil tudi prodekan za pedagoško delo. Ukvarja se z razvojem programske opreme za računalniško podprte informacijske sisteme s posebnim poudarkom na informacijskih sistemih za področje visokega šolstva. Od leta 1996 je predstavnik Slovenije v EUNIS (European University Information Systems Association), od leta 2002 pa tudi član sveta direktorjev omenjene organizacije.

Spoštovane bralke in spoštovani bralci,

člani uredništva revije Uporabna informatika

vam želimo

uspešno in ustvarjalno novo leto 2005