Ključna področja vodenja informatike kot izzivi vodjem služb za informatiko

Aleš Groznik, Luka Babnik*
Univerza v Ljubljani, Ekonomska fakulteta, Kardeljeva ploščad 17, 1000 Ljubljana
ales.groznik@ef.uni-lj.si
* Banka Slovenije, Slovenska c.35, 1000 Ljubljana
luka.babnik@bsi.si

Povzetek

Namen prispevka je predstaviti ključna področja vodenja informatike, ki predstavljajo izziv vodjem služb za informatiko. Dinamično poslovno okolje postavlja vodjem služb za informatiko številne kompleksne izzive, ki zahtevajo strukturirano obravnavo. Področja, ki predstavljajo ključne izzive vodjem služb za informatiko, so strateška usklajenost poslovanja in informatike, zagotavljanje poslovne vrednosti informatike, menedžment virov in menedžment tveganj. Prispevek podaja tuje in domače izkušnje ter priporočila vodjem služb za informatiko na ključnih področjih vodenja informatike.

Ključne besede: vodenje informatike, strateška usklajenost poslovanja in informatike, zagotavljanje vrednosti informatike, menedžment virov, menedžment tveganj

Abstract

The purpose of the article is to present key areas of IT governance. Volatile and dynamic business environment is causing numerous and complex challenges that IT managers have to cope with and overcome. Key areas are alignment of business and IT strategy, ensuring IT value delivery, resource management and risk management. The article also shows foreign and domestic experiences and recommendations to IT managers on IT governance key areas.

Keywords: IT governance, strategic alignment, value delivery, resource management, risk management

1 Uvod

Podatki in informacije o poslovanju predstavljajo enega ključnih elementov sodobnega poslovanja vsake organizacije. Vodenje informatike (angl. IT Governance) organizaciji prinaša številne koristi tako znotraj kot tudi zunaj nje. Vodenje informatike je ena izmed ključnih funkcij pri vodenju organizacije (angl. Corporate Management). Vodenje informatike je ena izmed funkcij, ki podjetjem omogoča poslovne uspehe oziroma je lahko vzrok za neuspehe. Ustrezna opredelitev funkcij vodje informatike, ustrezna struktura oddelka za informatiko, usklajenost poslovne strategije celotne organizacije s strategijo informatike so ključni dejavniki, ki organizaciji omogočajo kakovostno poslovanje. Zaradi njih mora biti ena izmed pomembnih nalog najvišjega vodstva tudi iskanje ustrezne usklajenosti informatike s poslovanjem celotne organizacije (Calder, 2005).

Vse hitrejše spremembe v poslovnem okolju so povezane tudi z različnimi poslovnimi tveganji, ki jih mora vsaka organizacija učinkovito in uspešno nadzorovati ter obvladovati. Eden izmed pomembnih dejavnikov pri doseganju tega cilja je vsekakor zagotovitev ustreznega okolja, ki omogoča kakovosten menedžment tveganj in vključuje uporabo sodobnih metodologij ocenjevanja, ugotavljanja in obvladovanja poslovnih tveganj. Menedžment tveganj organizaciji omogoča uspešno izvajanje poslovnih procesov ter s tem tudi večjo varnost poslovnih podatkov. Učinkovito in uspešno vodenje informatike ter uporaba sodobnih orodij in metodologij za kakovosten menedžment tveganj organizaciji lahko omogočijo konkurenčnost v poslovnem svetu ter uspešno, učinkovito in varno poslovanje.

2 Vodenje informatike

Vodenje informatike sestavlja splet medsebojno povezanih področij. Načelno je vodenje informatike namenjeno doseganju opredeljenih ciljev in upravljanju tveganj. Doseganje ciljev ni mogoče brez strateške usklajenosti strategije informatike s strategijo celotne organizacije (Groznik in Kovačič, 2001) in menedžmenta virov ter preglednosti in transparentnosti uspehov oziroma neuspehov. Le-to pa ni mogoče brez ustreznega menedžmenta zmogljivosti. Po zadnjih raziskavah podjetja AMR Group gre za hitro rastoč trg, ki naj bi po napovedih leta 2008 dosegel vrednost 30 milijard dolarjev. Organizacije se vse bolj zavedajo nujnosti učinkovitega vodenja informacijske tehnologije in obvladovanja tveganj. Le tako je mogoče

omejiti nezaželene vplive in izboljšati poslovanje celotne organizacije. Vodenje informatike je v zadnjem času eno izmed najpomebnejših področij, s katerimi se ukvarjajo najvišja vodstva v podjetjih in organizacijah. Po zadnjih raziskavah podjetja AMR Group 79 odstotkov direktorjev informatike (CIO) med najpomebneše cilje v svojih organizacijah omenja ravno področje vodenja informatike in obvladovanja tveganj kot ključni področji, ki podjetju lahko zagotovita enakoveden položaj v vse hitreje razvijajočem se konkurenčem poslovnem svetu (Emery, 2007). Temu trendu bi vsekakor morala slediti tudi slovenska podjetja, v katerih je kljub pozitivnim spremembam v zadnjih letih še mogoče opaziti zaostajanje za najbolj razvitimi svetovnimi podjetji.

Po raziskavah za leto 2005 v svetovnem merilu več kot 60 odstotkov podjetij uporablja svetovno razvite metodologije, kot so npr. ISO, standardi BS, ITIL, metodologija COBIT idr., s katerimi si podjetja poskušajo vzpostaviti ustrezno ogrodje za izvajanje kakovostnega menedžmenta tveganj ter čimbolj uspešno in učinkovito vodenje informatike. Ob tem dejstvu je treba opozoriti, da številna podjetja, ki uporabljajo lastne razvite metodologije (okrog 30 odstotkov), le-te razvijejo na podlagi standardnih metodologij, ki jih nato ustrezno prilagodijo lastnim potrebam. Vse kaže, da svetovno razvita in uspešna podjetja za obvladovanje tveganj in vodenje informatike v veliki meri dajejo poudarek metodologijam, ob pomoči katerih lahko zagotovijo kakovostno obvladovanje tveganj in vodenje informatike. Slovenska podjetja na tem področju še bistveno zaostajajo in bi morala v prihodnje temu področju nameniti večjo pozornost, če želijo poslovati kakovostneje v globalnem in vse bolj konkurenčnem poslovnem svetu.

Za uspešno in učinkovito vodenje informacijske tehnologije poleg sposobnega vodstvenega kadra pomembno vlogo igrajo tudi številni drugi pomembni pogoji. Razsežnost vodenja informacijske tehnologije se največkrat obravnava predvsem s treh vidikov in sicer:

- položaj in vloga vodje informatike;
- odnos med vodjem informatike (CIO) in generalnim direktorjem/predsednikom uprave;
- odnos najvišjega vodstva do informacijske tehnologije in sodelovanje generalnega direktorja ter ostalih članov vodstva pri aktivnostih informacijske tehnologije.

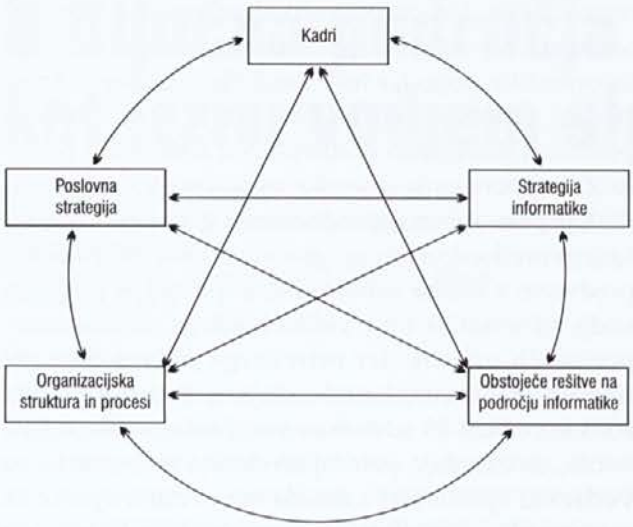
Položaj vodje informatike je velikokrat povezan s strateško pomembnostjo informacijske tehnologije za organizacijo, kar pa pogosto ni primeren kriterij. V sodobnih razvitih in uspešnih organizacijah se vodja informatike pojavlja tudi med člani uprave (Armstrong, Sambamurthy,1999). To je tudi v najuspešnejših slovenskih podjetjih bolj izjema kot pravilo. Za zagotavljanje strateške usklajenosti v organizacijah je pomemben tudi odnos med generalnim direktorjem/predsednikom uprave in vodjem informatike, predvsem z vidika neposredne in posredne podpore vodji informatike ter z vidika boljšega razumevanja poslovnih prioritet ter ustreznega prilagajanja aktivnosti informacijske tehnologije. V raziskavi leta 2005 je več kot 55 odstotkov vodij informatike odgovorilo, da zasedajo položaj direktorja informatike, le 4 odstotki vprašanih pa zaseda mesto člana uprave za informatiko. Rezultati omenjene ankete kažejo, da slovenska podjetja glede na položaj vodij informatike še vedno zaostajo za najbolj razvitimi evropskimi in svetovnimi organizacijami. Več kot 40 odstotkov vodij informatike je neposredno podrejenih predsedniku uprave oz. direktorju podjetja, še vedno pa so v slovenskih podjetjih vodje informatike pogostokrat (v več kot v 10 odstotkih) podrejeni vodjem financ in računovodstva (Šušnjar, 2005).

Glavna področja pri vodenju informatike so strateška usklajenost, zagotavljanje vrednosti, menedžment virov, menedžment tveganj in vrednotenje.

2.1 Strateška usklajenost

Za doseganje dolgoročnih uspehov organizacije je ključnega pomena razumevanje poslovnih ciljev organizacije. Eden izmed večjih problemov, ki se pojavlja v organizacijah, je, da nimajo ustrezno vzpostavljene strateške usklajenosti med informatiko in poslovanjem celotne organizacije (Groznik in Kovačič, 2001).

V slovenskih podjetjih informatika običajno nima takšne vloge, kot ji dejansko pripada. Velikokrat jo najvišje vodstvo jemlje kot nujno zlo in nikakor od nje ne dobi tistega, kar bi lahko. Menimo, da je treba na vseh področjih informatike vložiti še veliko naporov, da bi podjetja dojela njen pomen in izkoristila možnosti, ki jih ponuja informacijska tehnologija. Za slovenske velike in srednje organizacije je značilno, da slaba polovica (45 %) organizacij načrtuje razvoj informatike na strateški ravni, le tretjina (32 %) izmed njih kot izhodišče strateškemu načrtovanju informatike uporablja strateški poslovni načrt (Inštitut za poslovno informatiko, 2006). Z vidika uspešnosti



Slika 1: **Model skladnosti strateškega načrta informatike s strateškim načrtom podjetja in njegovim izvajanjem (Groznik in Kovačič, 2001)**

poslovanja je skladnost poslovne strategije in strategije informatike ključnega pomena, saj zagotavlja izkoriščanje možnosti, ki jih ponuja razvoj na področju informatike in učinkovito informatizacijo poslovanja. Vodja službe za informatiko se mora zavzemati za usklajenost med poslovno strategijo in strategijo informatike ter si prizadevati, da najvišjemu vodstvu ustrezno predstavi svojo strategijo ter dejstva, s katerimi lahko informatika prinese dodano vrednost k poslovanju organizacije. Na drugi strani pa mora vodstvo organizacije postati vse bolj izobraženo na področju informatike, saj jim to znanje pomaga pri doseganju sinergije med poslovno strategijo in strategijo informatike. Ključni dejavniki, ki vplivajo na skladnost poslovnega strateškega načrta s strateškim načrtom informatike in njegovim izvajanjem, so poslovna strategija, organizacijska struktura in procesi, strategija informatike, obstoječe rešitve na področju informatike in kadri (Groznik in Kovačič, 2001).

Rezultati raziskave, izvedene leta 2005, kažejo, da v polovici primerov vodjem informatike največje ovire predstavljajo nerealna in nezanana pričakovanja uporabnikov, takoj za tem pa sledijo (30 %) težave zaradi neusklajenosti med cilji informatike in celotne organizacije. Rezultati kažejo, da je v slovenskih podjetjih potrebno vložiti bistveno več truda v strateško usklajenost med oddelkom za informatiko in celotno organizacijo, saj le-to posameznih organizaciji omogoča uspešno in učinkovito delovanje (Šušnjar, 2005).

Poslovna strategija opredeljuje strateške usmeritve organizacije, ki naj bi podjetju zagotovile dolgoročno uspešno poslovanje. Organizacija ima za uspešen nastop na trgu več možnih strategij, ki so zasnovane s pomočjo dobrega poznavanja organizacijske strukture, procesov in okolja. Strategija informatike je v tesni povezavi s poslovno strategijo in drugimi ključnimi dejavniki. Opozarja na možnosti in nevarnosti, ki jih informacijski sistem ponuja oziroma predstavlja v poslovanju organizacije, in je usmerjena v najučinkovitejšo uporabo informacijske tehnologije v korist uspešnega poslovanja celotne organizacije. Podobno kot v primeru poslovne strategije in organizacijske strukture je tudi pri informatiki izrednega pomena dobro poznavanje obstoječih rešitev na področju informatike. Poleg poslovnih vidikov (poslovna strategija, organizacijska struktura in procesi) in informatike (strategija informatike, obstoječe rešitve na področju informatike) je pomemben tudi sociološki vidik. Kadri v organizaciji predstavljajo nabor kadrov, ki imajo potrebna strokovna znanja, s katerimi organizacija lahko doseže načrtovane strateške cilje.

Kot lahko razberemo iz zgornje slike, skladnost strateškega načrta informatike s strateškim načrtom podjetja in njegovim izvajanjem ni odvisna samo od informatike oziroma od službe za informatiko. Služba za informatiko mora zagotoviti kadre, znanje, poznavanje obstoječih rešitev na področju informatike ter ustrezno strategijo informatike. Vendar če želimo izrabljati informacijski sistem kot strateški sistem, ki prek verige dodane vrednosti organizaciji omogoča spremljanje, primerjavo in izboljšanje konkurenčne prednosti, potem so izrednega pomena tudi drugi kadri v organizaciji, zlasti vodilni, poslovna strategija, organizacijska struktura in procesi. Zavedati se je treba medsebojnih vplivov posameznih ključnih dejavnikov, ki v procesu strateškega načrtovanja ne smejo biti ločeni na poslovne (kadri, poslovna strategija, organizacijska struktura in procesi) in informacijske (kadri, strategija informatike, obstoječe rešitve na področju informatike). Ključni dejavniki so medsebojno odvisni in spremembe na posameznem dejavniku se odražajo na vseh drugih. Upoštevanje medsebojne odvisnosti ključnih dejavnikov in njihova harmoničnost v obdobju strateškega načrtovanja je ključnega pomena za uspeh načrtovanja in izvajanja. Vsaka organizacija mora nameniti veliko pozornost dobri pripravi strategije in zagotoviti ustrezno strateško usklajenost. Strategija mora omogočati udejanjanje in

postavitev ključnih vzvodov ali sistemov, prek katerih podjetje v praksi lahko uresničuje svojo strategijo.

2.2 Zagotavljanje vrednosti

Ena izmed pomembnih komponent vodenja informatike je zagotavljanje oziroma doseganje vrednosti, ki so bile opredeljene z investicijami, dodelitvami virov in sredstev. Z zagotavljanjem vrednosti je tesno povezana analiza investicij, virov in sredstev. Investicije, vključno z investicijami na področju informatike, naj ne bi bile izvedene brez celovitega analiziranja in predvidevanja stroškov ter pričakovanih koristi.

Zanimivo je, da le 38 odstotkov slovenskih velikih in srednjih organizacij vrednoti upravičenost naložb v informatiko pred realizacijo (Inštitut za poslovno informatiko, 2006). Za doseganje opredeljenih vrednosti mora vodja službe za informatiko posebno pozornost nameniti predvsem izvajanju posameznih aktivnosti, procesov v določenem obdobju, zagotavljanju, da informatika omogoča izvajanje poslovnih procesov skladno s strategijo, ter optimizaciji stroškov in doseganju ciljev. Zagotavljanje vrednosti bi lahko opredelili tudi kot izvajanje opredeljenih načrtov, nalog v okviru določenega časovnega cikla, v katerem informatika zagotavlja v strategiji opredeljene koristi ob osredinjenosti na optimizacijo stroškov. Strateška usklajenost med informatiko in poslovanjem celotne organizacije je eden izmed glavnih kriterijev za doseganje opredeljenih ciljev. Zagotavljanje vrednosti s pomočjo investicij v informatiko je ena izmed poglavitnih nalog vodje informatike. Vsaka investicija mora biti opredeljena s predvidenimi tveganji, ki jih je treba opredeliti in upoštevati pred realizacijo. Na uspešno zagotavljanje opredeljenih ciljev v informatiki lahko v veliki meri vplivajo ustrezno vodenje proračuna službe za informatiko, z usmerjenostjo v zniževanje stroškov, ustrezno opredeljevanje in menedžment projektov (Groznik in Vičič, 2006).

2.3 Menedžment virov

Učinkovit menedžment virov organizaciji omogoča boljše izvajanje poslovnih procesov, zato je pri tem pomembna predvsem osredotočenost na optimalno investiranje in menedžment virov (poslovni procesi, kadri, aplikacije, poslovni podatki, infrastruktura). Menedžment virov zajema sklop različnih nalog, vlog, odgovornosti, ciljev, kontrol, ki organizaciji omogočajo celovito in učinkovito identifikacijo potrebnih informacij, virov, poslovnih podatkov ter tako prispevajo k boljšemu poslovanju (IT Governance Institute, 2005: 5–27).

Menedžment virov organizaciji omogoča jasno preglednost in kontrolo nad svojimi viri, boljše načrtovanje, iskanje, dodeljevanje in prerazporejanje potrebnih virov ter njihovo optimizacijo. Z vidika poslovanja postajajo zaposleni vedno bolj pomemben dejavnik pri izpolnjevanju opredeljenih ciljev. Vodje služb za informatiko slovenskih velikih in srednjih organizacij ocenjujejo, da je raven znanja v službah za informatiko pod želenim, zlasti zaposlenim v službah za informatiko primanjkuje poslovnih znanj (Inštitut za poslovno informatiko, 2006).

2.4 Menedžment tveganj

V preteklosti so se podjetja pri menedžmentu tveganj skoraj izključno zanašala na mehanizme notranje kontrole za posamezna področja poslovanja in vlogo notranje revizije. Vse to je sicer še vedno pomembno, vendar se poleg tega v zadnjem času pojavljajo še posebne oblike organiziranosti ter orodja in postopki, namenjeni menedžmentu tveganj. Tako vedno več podjetij ugotavlja, da menedžment tveganj zagotavlja podjetju večjo varnost in boljše poslovanje ter varuje in povečuje vrednost podjetja lastnikom (Majič, 2002).

Menedžment tveganj je tudi pomembna funkcija vodje službe za informatiko, saj je s tem omogočeno doseganje strateških ciljev informatike. Tveganja, povezana z informatiko, so vse bolj pogosto predmet razprav. Najvišji menedžment jih povezuje s poslovanjem oziroma z vplivom, ki jih tveganja, povezana z informatiko, predstavljajo za poslovanje organizacije oziroma s posledicami, ki jih lahko ta tveganja prinesejo organizaciji. Tveganja, povezana z informatiko, se največkrat kažejo kot nezmožnost izrabe prednosti, ki nam jih ponuja informatika (npr. zamuda priložnosti za izboljšanje konkurenčne prednosti, učinkovitosti izvajanja itd.). Kakovosten menedžment tveganj podjetju omogoča učinkovito optimizacijo poslovnih procesov, ki je po raziskavah podjetja Gartner Group prva prioriteta vodij služb za informatiko v letih 2005 in 2006 (Gartner Group, 2006). Menedžment tveganj je oziroma mora biti del vsakodnevnega delovanja organizacije. Zahteva zavedanje tveganj najvišjega menedžmenta, (ne)naklonjenost organizacije tveganjem, nazoren pregled nad tveganji, ki se jih mora zavedati organizacija, vlaganje truda ter pridobivanje novega znanja za obvladovanje tveganj

znotraj organizacije. Tveganja, ki lahko vplivajo na poslovanje organizacije, se lahko pojavijo na številnih področjih in ne zajemajo samo finančnih tveganj.

Pri tveganjih, povezanih z informatiko, je posebna pozornost namenjena obvladovanju operativnih in sistemskih tveganj, pri čemer so pomembna predvsem tehnološka in varnostna področja. Splošno sprejeta definicija tveganj, povezanih z informatiko, ne obstaja, lahko pa tveganja opredelimo s pomočjo različnih skupin tveganj (IT Governance Institute: 5–18), in sicer:

- investicijska oziroma stroškovna tveganja (angl. investment or expensive risk) so tveganja, ki se navezujejo na investicije v informatiko, ki ne bi izboljšale obstoječega stanja oziroma izpolnile opredeljenih vrednosti, ciljev;
- tveganja varnosti oziroma dostopov (angl. security or access risk) so tveganja, da bi bile objavljene zaupne poslovne informacije, dostopne osebam, ki nimajo ustreznih pravic;
- integritetna tveganja (angl. integrity risk) so tveganja, da podatki in informacije ne bi bili zanesljivi, celoviti zaradi nepopolnosti, neažurnosti, nezakonitosti itd.;
- tveganja ustreznosti (angl. relevance risk) so tveganja, povezana z nedostopnostjo pravih, ažurnih informacij oziroma z neustreznim posredovanjem informacij določenim/pravim osebam oziroma poslovnim sistemom, procesom v določenem času ter s tem onemogočanje izvajanja določenih aktivnosti;
- tveganja razpoložljivosti (angl. availability risk) so tveganja za izgubo sistemov oziroma storitev, ki morajo biti razpoložljiva za izvajanje poslovnih procesov;
- tveganja infrastrukture (angl. infrastructure risk) so tveganja, da organizacija nima ustrezne infrastrukture, informacijskih sistemov, ki bi ustrezno podpirali poslovanje celotne organizacije na učinkovit, stroškovno ustrezen in ustrezno obvladljiv način;
- projektna tveganja (angl. project risk) so tveganja, ki se navezujejo na (ne)uspešnost projektov in s tem (ne)doseganje opredeljenih vrednosti, ciljev kot posledica pomanjkanja odgovornosti in neustreznega izvajanja opredeljenih obveznosti.

Pomen tveganj se sestoji iz vpliva (kakšen vpliv bo tveganje imelo na organizacijo, če se pojavi) in verjetnosti (verjetnost, da se določeno tveganje pojavi). Redno ocenjevanje tveganj je ena izmed ključnih aktivnosti, ki mora biti tesno povezana s poslovanjem organizacije, saj le poslovni uporabniki lahko ocenijo morebitni vpliv tveganj na poslovanje organizacije. Poslovna tveganja so povezana s poslovanjem celotne organizacije in so odvisna od številnih dejavnikov (npr. področje poslovanja, kultura organizacije, naklonjenost tveganjem, konkurenčnost itd.). Prek poslovanja organizacije lahko opredelimo tudi tveganja s področja informatike. Pomembno je predvsem zavedanje, da se tveganja s področja informatike nahajajo znotraj širšega kroga poslovnih tveganj, kar nam pomaga pri lažjem opredeljevanju tveganj.

Menedžment tveganj zajema dva pomembna elementa – analizo in obvladovanje tveganj.

- Analiza tveganj se ukvarja z zbiranjem informacij o izpostavljenosti organizacije tveganjem in odkrivanju novih tveganj, kar organizaciji omogoča sprejemanje ustreznih odločitev in primerno nadzorovanje tveganj.
- Obvladovanje tveganj zajema procese, s katerimi je omogočen prikaz, vrednotenje, analiziranje in identifikacija tveganj, vključno z ustreznimi informacijami o različnih tveganjih in tako predstavlja podporo pri sprejemanju poslovnih odločitev.

Ko ima organizacija opredeljeno naklonjenost in izpostavljenost tveganjem, lahko opredeli strategijo za menedžment tveganj in določi odgovornosti in obveznosti. Analiziranje tveganj je lahko časovno zelo obsežno, zato se pri tem pojavlja nevarnost pojava t. i. ohromele analize (angl. Analysis paralysis). Za zagotovitev učinkovite in hitre identifikacije tveganj je treba združiti znanja predstavnikov celotne organizacije tako poslovnih oddelkov kot informatike in pogosto tudi zunanjih svetovalcev, s pomočjo katerih je identifikacija tveganj lažja in tako omogoča hitrejše sprejemanje ustreznih ukrepov za njihovo obvladovanje.

Menedžment tveganj s področja informatike je ena izmed pomembnih domen vodje službe za informatiko, čeprav je pri tem zelo pomembna tudi prisotnost menedžmenta organizacije. Menedžment mora biti navzoč pri obvladovanju tveganj, kajti njegova nenavzočnost lahko povzroči, da so prezrta določena tveganja, opredeljene neustrezne akcije oziroma izvedene neustrezne investicije. Menedžment mora sodelovati pri opredeljevanju strateških usmeritev za učinkovito in uspešno obvladovanje poslovnih tveganj. Poslovni oddelki morajo zagotoviti obvladovanje poslovnih tveganj, vključno s tveganji s področja

informatike. Poslovni oddelki so zadolženi za opredelitev aktivnosti za obvladovanje poslovnih tveganj, zagotovitev ustreznih kadrov in drugih virov ter spremljanje tveganj. Ob vse večjem pomenu informatike za poslovanje celotne organizacije ter njenem vse hitrejšem razvoju in kompleksnosti, morajo poslovni oddelki tesno sodelovati z informatiko. Tesna povezava omogoča vzpostavitev ustreznih varnostnih meril za obvladovanje tveganj, ki se navezujejo tako na poslovanje kot na informatiko.

Menedžment tveganj primarno ne sme biti opredeljen kot povsem tehnična funkcija, ki se izvaja le ob pomoči informatikov, marveč je treba ta proces opredeliti kot eno izmed najpomembnejši skupnih funkcij celotne organizacije (IT Governance Institute: 5–18). Zaradi celovitosti in hitro spreminjajočega se poslovnega okolja je za ocenjevanje novih tveganj nujno ustrezno izobraževanje, zavedanje o tveganjih ter posredovanje informacij menedžmentu in drugim v organizaciji. Menedžment tveganj je eden izmed ključnih dejavnikov, ki organizaciji omogoča doseganje uspehov in dobrih poslovnih rezultatov.

2.5 Vrednotenje

Vrednotenje informatike je zelo celovito področje, ki je neposredno povezano z vrednostjo in pomenom informatike. Razprave o tem, kakšna je dejanska vrednost in pomen informatike v podjetju, so vse pogostejše tako v akademskih kot tudi v poslovnih krogih. Po eni strani smo bili vse do leta 2002 priča neprestani rasti naložb v informatiko, ki so v razvitih zahodnih državah dosegle 5–7 odstotkov vrednosti prihodkov prodaje (Gartner Group, 2002), z namenom povečevanja poslovne uspešnosti in konkurenčne prednosti. Po drugi strani pa so se vzporedno pojavljale raziskave, na podlagi katerih je mogoče sklepati, da naložbe v informatiko nimajo želenega vpliva na uspešnost poslovanja (Hitt in Brynjolfsson, 1994; Kraemer in Dedrick, 1994; Tam, 1998; Devaraj in Kohli, 2000; Groznik in Kovačič, 2003). Ne glede na to, kaj je razlog za takšne ugotovitve, je dejstvo, da vodstva podjetij želijo videti otipljive koristi, ki pa jih informatiki velikokrat ne znajo oziroma ne morejo pokazati. Informatika na ta način postane za podjetje zgolj strošek, posledice pa so vidne v zmanjševanju proračunskih sredstev (Gomolski, 2003).

Nastalega problema se je treba lotiti z dveh vidikov – z vidika izbire ustreznih kriterijev merjenja učinkov informatike in tudi z vidika izbiranja pravih naložb. Ko govorimo o naložbah v informatiko, ni pomembno le, koliko vlagamo, temveč tudi kam in kakšni so vplivi teh naložb. V praksi podjetja uporabljajo različne metode ugotavljanja vpliva informatike na uspešnost poslovanja, ki se pogosto usmerjajo zgolj na merljive oziroma otipljive (ang. tangible) učinke informatike. Le-ti pa zaradi specifične vloge informatike v podjetju večinoma niso dovolj. Iz tega razloga je treba v metode vključiti več kriterijev, ki poleg klasičnih finančnih in računovodskih parametrov vključujejo tudi druga področja vpliva, ki pa so pogosto težko merljiva oziroma jih lahko samo ocenimo. Govorimo o tako imenovanih neotipljivih (ang. intangible) učinkih, kot je na primer zadovoljstvo strank, kakovost informacij ipd. Kljub izbiri prave metode ocenjevanja informacijskih učinkov brez pravilnega načrtovanja in izbire projektov ne bo želenih rezultatov. Velja namreč dejstvo, da je mogoče učinkovito izvajati tudi napačne stvari, ki zgolj povečujejo stroške in s tega vidika tudi ne prispevajo k uspešnejšemu poslovanju podjetja. Pobuda oziroma podpora za izvedbo informacijskih projektov mora izhajati od vodstva, ki ima jasno izdelano strategijo podjetja in vlogo informatike v podjetju. Poslovna uspešnost je neposredno odvisna od uveljavljanja in zagotavljanja strateške vloge informatike. Če govorimo o poslovni uspešnosti kot o povečevanju vrednosti podjetja, lahko trdimo, da urejena, strateško načrtovana informatika povečuje vrednost podjetja. Naložbe v informatiko same po sebi ne prinašajo poslovne vrednosti. Postavlja se vprašanje, kje iskati potencialno vrednost informatike oziroma na katera področja investirati razpoložljiva sredstva. Podlaga za dolgoročni uspeh je prav gotovo strateško načrtovanje informatike, ki izhaja neposredno iz strateškega načrta podjetja. Ključni dejavniki strateškega načrtovanja informatike in tudi glavni nosilci vrednosti informatike so poslovni procesi, kadri in znanje, informacijska tehnologija ter povezave med njimi vključno z vsemi posledicami potrebnih organizacijskih sprememb v smeri procesne organiziranosti in položaja informatike v podjetju (Groznik in Vičič, 2005).

Ustvarjanje vrednosti informatike je torej kompleksen proces, odvisen od številnih spremenljivk, zaradi česar je nemogoče najti preprosto vzročno-posledično odvisnost. Kompleksni procesi ustvarjanja poslovne vrednosti informatike pogosto pomembno vplivajo na mnenje poslovnih uporabnikov o informatiki. Poslovni uporabniki pogosto niso navdušeni nad visokimi

investicijami v informatiko, saj menijo, da koristi ne upravičujejo visokih investicij. Enake skrbi se navezujejo tudi na stroške informatike, pri katerih ni jasne ocene, kakšne koristi so bile dosežene. Temu fenomenu pravimo t. i. črna luknja (angl. black hole). Ustvarjanje vrednosti s pomočjo informatike in njeno vrednotenje mora biti pomembna domena vodje službe za informatiko. Pri tem je treba upoštevati tako otipljive (npr. višja produktivnosti, nižji operativni stroški, višja dodana vrednost, nižji stroški administracije itd.) kot neotipljive (npr. višje zadovoljstvo strank, večja prilagodljivost poslovanja, višja kakovost informacij, izboljšanje kontrole virov, zvišanje naklonjenosti zaposlenih, boljši poslovni izgled organizacije itd.) koristi in učinke. V pomoč vrednotenju informatike lahko uporabimo metodologijo COBIT (angl. Control Objective for Information and related Technology), ki deli metrike in cilje za upravljanje zmogljivosti na tri ravni (IT Governance Institute, 2005: 22–23):

- cilji in metrike, ki opredeljujejo pričakovanja poslovnega sveta od informatike,
- procesni cilji in metrike, ki opredeljujejo doprinos procesov za podporo doseganju ciljev,
- metrike za merjenje procesov, ki so namenjene merjenju, kako dobro se procesi izvajajo ter s tem ugotavljanju verjetnosti, ali bodo opredeljeni cilji doseženi.

COBIT opredeljuje uporabo dveh vrst metrik, in sicer ciljne (angl. goals indicators) in zmogljivostne indikatorje (angl. performance indicators). Ciljni indikatorji opredeljujejo stopnje, na podlagi katerih je mogoče ugotoviti, ali so procesi dosegli opredeljene poslovne zahteve (npr. razpoložljivost informacij potrebnih za podporo poslovnim potrebam, celovitost informacij, odsotnost tveganj, učinkovitost procesov in operacij itd.). Zmogljivostni indikatorji pa opredeljujejo stopnje, na podlagi katerih je mogoče ugotoviti, kako dobro so izvajani procesi za doseganje opredeljenih ciljev. Dobro upravljanje zmogljivosti omogoča razumevanje poslovnim uporabnikom, kako informatika prispeva k doseganju poslovnih ciljev. Vrednotenje informatike naj bi prineslo odgovore na vprašanja, kot so npr. Kakšne koristi/prednosti nam prinaša dodatno vlaganje v informatiko? Ali so dosežene opredeljene poslovne zahteve z vidika informatike? Ali informatika vodi svojo strategijo skladno s poslovno strategijo? itn.

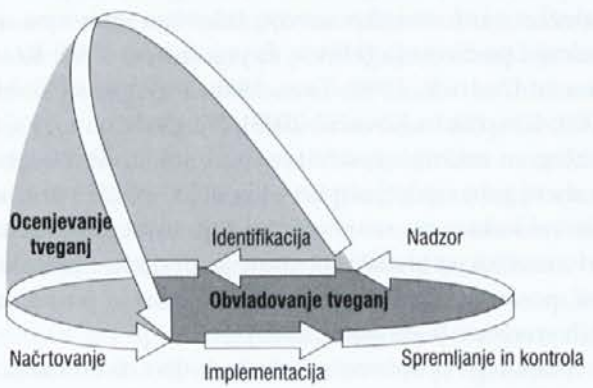
Vrednotenje naj bi bila ena izmed ključnih nalog vodje službe za informatiko ob močni podpori vodij poslovnih oddelkov, saj je tako laže predstavljiva dodana vrednost in koristi, ki jo prinese informatika k poslovanju.

3 Menedžment in ocenjevanje tveganj

Vsaka organizacija je stalno izpostavljena številnim novim oziroma spreminjajočim se tveganjem, ki lahko negativno vplivajo na poslovanje in s tem na doseganje opredeljenih ciljev. Namen menedžmenta tveganj je iskanje ustreznih načinov za učinkovito izpolnjevanje poslovnih priložnosti in zmanjševanje neuspehov ter nezaščitenosti. Baselski komite je tveganja opredelil kot tveganje direktnih ali indirektnih izgub, ki rezultirajo iz neprimernih ali neuspešnih procesov, ljudi, sistemov ali zunanjih dogodkov (Gornik, 2004).

Menedžment tveganj naj bi bil stalno ponavljajoč proces, ki se sestoji iz različnih faz ter omogoča stalno izboljševanje procesov za sprejemanje poslovnih odločitev in izvajanje storitev. K menedžmentu tveganj spada tudi proces ocenjevanja tveganj (angl. risk assessment). Ocenjevanje tveganj na področju informatike (angl. Information Technology risk management – ITRM) je lahko del širšega procesa celotne organizacije oziroma samostojen proces. Glede na razvoj na področju informatike je ocenjevanje tveganj praviloma vpeljan kot stalen proces znotraj vsake organizacije (ENISA, 2006: 1).

Proces menedžmenta tveganj je stalno ponavljajoč proces, ki se sestoji iz več aktivnosti, kot so načrtovanje, implementacija, spremljanje in kontroliranje vpeljanih dimenzij/kontrol, opredeljenih v varnostni politiki. Nasprotno temu je proces ocenjevanja tveganj izvajan točno ob določenih terminih (npr. enkrat na



Slika 2: **Proces menedžmenta in ocenjevanje tveganj (ENISA, 2006, str. 6)**

leto oz. na zahtevo) in omogoča prikaz trenutno ugotovljenih tveganj. Sestoji se iz treh aktivnosti, to so (ENISA, 2006: 19–23):

- identifikacija tveganj (angl. Identification of Risk); v tej fazi se identificirajo tveganja, kritične točke oziroma segmenti. Identifikacija tveganj se mora izvajati sistematično, obsežno ter kakovostno, tako da lahko identificiramo čim večje število potencialnih tveganj oziroma nevarnosti. Zelo pomembno je, da se vsa identificirana tveganja v tej fazi ustrezno opredelijo in zabeležijo, ne glede na to, ali so določena tveganja že znana oziroma ustrezno nadzorovana. Kakovostne informacije, dobro poznavanje organizacije in njenega notranjega ter zunanjega okolja ter sodelovanje strokovnjakov iz različnih poslovnih področij so zelo pomembni dejavniki, ki lahko pozitivno vplivajo na izvajanje procesa identifikacije tveganj;
- analiziranje tveganj (angl. Analysis of Risk) je faza, v kateri se doseže razumevanje identificiranih tveganj, med drugim tudi vrste ter stopnje tveganj. Te informacije pripomorejo k lažji odločitvi, kako obravnavati posamezna identificirana tveganja. Faza zajema natančno analizo izvora, vzroka tveganj, opredelitev posledic tveganj, opredelitev verjetnosti posameznih tveganj ter posledic in kriterijev, ki so povezani s tveganji, opredelitev oziroma iskanje že obstoječih kontrol oziroma procesov, ki omogočajo znižanje negativnih posledic opredeljenih tveganj. Stopnjo tveganj je mogoče opredeliti ob pomoči različnih statističnih analiz, izračunov v kombinaciji z vplivi in verjetnostmi posameznih tveganj. Pri uporabi različnih metod in izračunov je bistvenega pomena njihova skladnost s kriteriji, ki so opredeljeni v okviru strategije za menedžment tveganj. Pri analiziranju tveganj so nam lahko v veliko pomoč pretekle izkušnje, zgodovinski podatki in poročila, standardi, analize, prototipne rešitve in eksperimenti, različni modeli, specialistična in ekspertna znanja oziroma nasveti itd.;
- vrednotenje tveganj (angl. Evaluation of Risk); v tej fazi se opredelijo tveganja, ki jih je oziroma ni treba ustrezno obravnavati glede na prioriteto tveganj. Pri vrednotenju tveganj je treba poleg stopnje tveganja upoštevati tudi druge dejavnike, kot so posledice, verjetnost dogodkov, vpliv posameznih tveganj itd.

Identifikacija, analiziranje in vrednotenje tveganj so aktivnosti, s pomočjo katerih organizacija opredeli ter meri vpliv tveganj in s tem laže opredeljuje ustrezne kontrole za menedžment ugotovljenih tveganj. Proces ocenjevanja tveganj je pogosto nezadostno izvajan, čeprav je del procesa menedžmenta tveganj. Organizacije bi morale za učinkovito in uspešno obvladovanje poslovnih tveganj pomembno vlogo nameniti tudi ocenjevanju tveganj. Vsaka organizacija mora za menedžment tveganj zagotoviti ustrezno okolje ter opredeliti ustrezno poslovno strategijo za menedžment tveganj ter si s tem zagotoviti kontrolno ogrodje za njihovo obvladovanje (angl. control framework). Strategija menedžmenta tveganj večinoma opredeljuje parametre za celotno organizacijo in jo po navadi sprejme vodstvo organizacije. Strategija zajema in omogoča uporabo sodobnih metodologij in tehnik za oceno in menedžment tveganj. Vsaka organizacija mora sprejeti in korektno izvajati ustrezno politiko na področju poslovnih tveganj. Strategija za menedžment tveganj zajema tudi vzpostavitev ustreznega okolja – tako zunanjega kot notranjega –, v katerem organizacija deluje.

Eden izmed najpomembnejših pogojev za dobro opredelitev kontrol notranjega okolja je predvsem razumevanje poslovanja in delovanja celotne organizacije. Pri tem je treba upoštevati predvsem ključne poslovne procese, prednosti, slabosti, priložnosti, nevarnosti, katerim je izpostavljena organizacija, organizacijsko kulturo in strukturo, zaposlene kadre, cilje organizacije itd. Z vzpostavitvijo t. i. kontrolnega ogrodja organizacija opredeli osnovne parametre, ki služijo za menedžment posameznih tveganj ter s tem tudi področja delovanja, na katerih je potreben menedžment tveganj. To med drugim zajema definiranje glavnih predpostavk notranjega in zunanjega organizacijskega okolja ter skupne cilje, aktivnosti in procese za menedžment tveganj. Pri opredelitvi posameznih področij, tveganj ter s tem postavitvijo kontrolnega ogrodja za menedžment tveganj si organizacija lahko pomaga z različnimi orodji oziroma metodologijami, med katerimi je tudi COBIT (ENISA, 2006: 15–19).

4 Sklep

Ocenjevanje in menedžment tveganj predstavljata enega izmed glavnih dejavnikov pri vodenju informatike, saj sta ključnega pomena pri vzpostavljanju povezave med poslovnim svetom in informatiko ter omogočata kakovostno poslovanje in s tem doseganje opredeljenih ciljev. Številne raziskave kažejo, da je

mnogo projektov v organizacijah neuspešnih in da informatika v organizacijah še nikoli ni bila tako pomembna funkcija za poslovanje kot v sedanjem času (IT Governance Institute, 2006) ter predstavlja pomemben dejavnik pri zagotavljanju vrednosti, ki so opredeljene v poslovni strategiji organizacije.

Zaradi neustreznega vodenja informatike in neustrezno opredeljenega menedžmenta tveganj se v organizacijah problemi kažejo predvsem v visokih stroških, neuspešnih projektih, operativnih težavah in incidentih, neustreznem vrednotenju informatike ter v strateški nepovezanosti med informatiko in celotno organizacijo, neustrezni varnosti in zaščiti pred tveganji ter neuspešnem zagotavljanju opredeljenih vrednosti. Zaradi tega bi težko našli vodjo informatike, ki ne bi opredelil vodenja informatike in obvladovanja tveganj kot ključni nalogi vsake organizacije vse od začetka novega stoletja naprej (Segars, Hendrickson, 2000).

Vsaka organizacija bi morala zaradi zgoraj opredeljenih problemov veliko svoje pozornosti usmeriti k vzpostavitvi ustreznega menedžmenta tveganj in k kakovostnemu vodenju informatike. Druga ključna področja (strateška usklajenost, zagotavljanje vrednosti, menedžment virov, vrednotenje), ki poleg menedžmenta tveganj predstavljajo glavna področja vodenja informatike, so v raziskavah opredeljena kot področja, s katerimi si organizacija ali omogoči kakovostno poslovanje ali pa uspešno odpravlja probleme in težave ter obvladuje tveganja. Pri tem si lahko pomaga tudi s številnimi metodologijami in standardi, med katerimi je v zadnjem času vedno bolj prepoznavna metodologija COBIT, ki jo po zadnjih raziskavah v svetovnem merilu neposredno uporablja približno 10 odstotkov organizacij, še veliko več pa jo uporablja kot temelj, na podlagi katerega vsaka organizacija razvije svoje kontrolno ogrodje kot podporo pri vodenju informatike (IT Governance Global Status Report, 2006).

Na poti do želenega rezultata je pomembno, da se organizacije zavedajo, da uvajanje omenjenih področij velikokrat zahteva organizacijske in tehnološke spremembe, sama izvedba pa je pogosto povezana s številnimi dolgoročnimi projekti z visoko stopnjo tveganja. S tega vidika je nujno, da so cilji že pred začetkom uvajanja jasno definirani in usklajeni s strategijo podjetja, člani projektnih skupin pa morajo biti strokovnjaki na obravnavanih področjih.

5 Literatura in viri

1. Armstron Curtis P., Sambamurthy V.: Information Technology Assimilation in Firms: The influence of Senior Leadership and IT Infrastructures. Information Systems Research, Providence-10, 1999. str. 304–327.
2. Calder Alan: IT Governance; Guidelines for Directors, IT Governance Publishing, 2005. 170 str.
3. Clevland Scott: Manage Your Business Processes to Create a Competitive Advantage, Business Process Trends, 2006.
4. Culp L. Christopher: The Risk Management process, Business Strategy and Tactics, John Wiley & Sons, Inc, 2001.
5. Devaraj S. in Kohli R. (2000) Information Technology Payoff in the Health-Care Industry: A Longitudinal Study, Journal of Management Information Systems, 6 (4), 2000, 41–67.
6. Emery Adam: Unveils Solutions for Resilient Operations with Clearer Insight into Data, Assets and Security. New York, 15.05.2007, 4 str. [URL: http://www-03.ibm.com/press/us/en/pressrelease / 21549.wss], 01.08.2007
7. ENISA – European Network and Information Security Agency: Risk Management; Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006. 177 str.
8. Fisher Urs: Serving IT Governance Professionals, ISACA e-Symposium, 2006. 34 str.
9. Gartner Group: Growing IT's Contribution: The 2006 CIOAgenda, 2006 [URL: www.gartner.com].
10. Gornik Rado: Upravljanje operativnih tveganj v informatiziranih bankah, Magistrsko delo, Maribor, 2004.
11. Groznik Aleš, Kovačič Andrej: Skladnost poslovnega strateškega načrta s strateškim načrtom informatike. Uporabna informatika. Ljubljana, 2001, let. 9, št. 1, str. 12–15.
12. Groznik Aleš in Kovačič Andrej (2003): The real business value of it, Economic business review, 5 (1/2), 137–146.
13. Groznik Aleš in Vičič Dejan (2005) Pomen informatike pri prevzemih in združevanjih podjetij. Uporabna informatika, Ljubljana, jan./feb./mar. 2005, letnik 13, št. 1, str. 32–36.
14. Groznik Aleš, Vičič Dejan: Menedžment portfelja projektov službe za informatiko. Uporabna informatika. Ljubljana, okt/nov/dec 2006, letnik 14, št. 4, str. 219–225.
15. Groznik Aleš, Vičič Dejan: Management poslovnih procesov in operativnih tveganj. Dnevi slovenske informatike, Portorož, 11.–13. april 2007. Z informatiko do novih poslovnih priložnosti : zbornik posvetovanja. Ljubljana: Slovensko društvo Informatika, 2007, 7 str. CD ROM.

16. Hitt L. in Brynjolfsson E. (1994):
The Three Faces of IT Value: Theory and Evidence, Proceedings of the 15th International Conference on Information Systems.
17. Inštitut za poslovno informatiko, Raziskava stanje poslovne informatike v Sloveniji, 2006.
[URL: http://www.ef.uni-lj.si/enote/ipi/]
18. ISACA:
Revizija informacijskih sistemov – kaj in kako?
[URL: www.si-revizija.si/isaca/revizija_IS.php], 15.01.2007
19. IT Governance Institute:
IT Governance Global Status Report – 2006. IT Governance Institute, 2006. 48 str.
20. IT Governance:
Board Briefing on IT Governance, 2005. 3. str.
[URL:http://www.itgovernance.co.uk/files/download/Board_Briefing_on_IT_Governancev5.pdf], 06.01.2007
21. IT Governance Institute:
Measuring and Demonstrating the Value of IT, 2005. 23 str.
[URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagementContentDisplay.cfm&ContentID=27284]
22. IT Governance Institute:
Information Risks: Whose Business Are They?, 2005. 23 str.
[URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagementContentDisplay.cfm&ContentID=27288]
23. IT Governance Institute: Governance of Outsourcing, 2005. 25 str.
[URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27286]
24. IT Governance Institute:
Optimising Value Creation From IT Investments, 2005. 27 str.
[URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27249]
25. IT Governance Institute:
IT Alignment: Who Is in Charge?, 2005. 30 str.
[URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27282]
26. ENISA – European Network and Information Security Agency
[URL: http://www.enisa.europa.eu], 7.01.2007
27. ISACA – Information Systems Audit and Control Association
[URL: www.isaca.org], 10.01.2007
28. ISACA: Slovenski odsek ISACA mednarodnega Združenja za revizijo in kontrolo informacijskih sistemov
[URL: http://www.si-revizija.si/isaca/]
29. ITGI – Information Technology Governance Institute
[URL: http://www.itgi.org], 23.12.2005
30. Kraemer K. in Dedrick J. (1994):
Payoffs from Investment in Information Technology-Leasons from the Asia-Pacific Region, World Development, 22 (12), 1921–1931.
31. Majič Mojca:
Operativno tveganje; definicija, regulacija in merjenje, Banka Slovenije, Ljubljana, 2002.
32. Segars Albert, Hendrickson Anthony:
Value, Knowledge, and the Human Equation: Evolution of the Information Technology Function in Modern Organizations. Journal of Labor Research, XXI-3, 2000. str. 431–445.
33. Šušnjar Goran:
Profil slovenskega ravnatelja IT; rezultati ankete. CIO konferenca, 2005. 19 str.
34. Tam K. Y. (1998):
The Impact of Information Technology investments on Firm Performance and Evaluation: Evidence from Newly Industrialized Economies, Information Systems Research, 9 (1), 85–98.

▪

Aleš Groznik je docent s področja poslovne informatike, zaposlen na Ekonomski fakulteti Univerze v Ljubljani. Področje njegovega strokovnega in raziskovalnega dela je vloga sodobnega informacijskega sistema v poslovnem okolju. Ukvarja se s področji strateškega načrtovanja informatike, prenove poslovanja, elektronskega poslovanja ter revizije informacijskih sistemov. Raziskuje možnosti in vlogo informatike kot vzvoda zagotavljanja konkurenčnosti in uspešnosti poslovanja podjetij. Je revizor informacijskih sistemov (CISA).

▪

Luka Babnik je univerziteni študij končal leta 2004 na Fakulteti za organizacijske vede Univerze v Mariboru. Leta 2005 je vpisal podiplomski študij na Ekonomski fakulteti Univerze v Ljubljani, smer poslovna informatika, in leta 2006 zagovarjal magistrsko delo. Od leta 2004 je zaposlen kot projektant v oddelku informacijska tehnologija v Banki Slovenije, kjer dela na področju informacijskega sistema SAP.