UPRAVLJANJE IT RIZIKOM

IT RISK MANAGEMENT

Aida Habul, Docent Dr.
Univerzitet Sarajevo, Ekonomski fakultet
aida.habul@efsa.unsa.ba

REZIME
Poslovanje preduzeća može biti ugroženo unutrašnjim ili vanjskim prijetnjama koje iskorištavaju postojeće slabosti IT mreža i sistema. Kako preduzeća sve značajnije ovise o nivou primjene elemenata informacionih tehnologija, aktuelizira se i problem očuvanja informacija i hitna potreba za menadžmentom IT rizika, kao odvojenom funkcijom. Osnovni cilj procesa upravljanja IT rizikom unutar organizacije bi trebao biti zaštita same organizacije i njene sposobnosti za uspješno provođenje poslovnih ciljeva, a ne samo dijelova informacione tehnologije. Zbog toga bi proces upravljanja rizikom trebao biti tretiran primarno kao tehnička funkcija koju vrše IT eksperti, a u isto vrijeme i kao bitna funkcija menadžmenta same organizacije. Upravljanje IT rizikom je proces identifikacije rizika, pristupa riziku i preduzimanju koraka radi smanjenja rizika na prihvatljiv nivo. U ovom radu će biti objašnjene osnove razvoja efikasnog menadžmenta IT rizika, kao i koraci neophodni za uspješno provođenje ukupnog procesa.

Ključne riječi: informaciona tehnologija, IT rizik, upravljanje IT rizikom

SUMMARY
Business transactions can be imperilled by internal or outside threats that utilize existing weakness of IT networks and systems. Modern enterprises more and more depend on the level of using information technologies, therefore arises the problem of saving information and urgent need for management IT risk, as a special function. The main goal of management IT risk process inside organization will be the protection of the organization and its ability for successfully realization business goals, as well as, information technology elements. That's reason why management risk process would be considered primary as a technical function that do IT experts, and at the same time, as the essential management function of the organization. Management IT risk is the process of identification risk, access and undertaking the steps for reduction IT risk on acceptable level. In this article will be presented the base of effective management IT risk development, and also the steps that are necessary for successfully realization of total process.

Key words: information technology, IT risk, management IT risk

1. UPRAVLJANJE IT RIZIKOM

Informacione tehnologije IT su finansijskim i operativnim komponentama sve šire i obuhvatnije integrisane u mnoge poslovne operacije i transakcije. Informacione tehnologije

uključuju IT rizik koji je, sam po sebi, rastuća komponenta ukupnog rizika poslovanja, a tiče se posebno područja sigurnosti, raspoloživosti, učinkovitosti i elementa povjerljivosti.

Rizik je potencijalna šteta za organizaciju, a najčešće se javlja zbog neadekvatnog menadžmenta procesa i događaja. Kako je IT rizik bitna komponenta ukupnog rizika poslovanja, on igra sve važniju ulogu u organizacijama (u nekom kompanijama sektor informacione tehnologije zauzima više od 50% ukupnog troška).

Upravljanje IT rizikom je proces identifikacije rizika, pristupa riziku i preduzimanja koraka radi smanjenja rizika na prihvatljiv nivo. Osnovni cilj procesa upravljanja IT rizikom unutar organizacije bi trebao biti zaštita same organizacije i njene sposobnosti za uspješno provođenje poslovnih ciljeva, a ne samo dijelova informacione tehnologije. Zbog toga bi proces upravljanja rizikom trebao biti tretiran primarno kao tehnička funkcija koju vrše IT eksperti, a u isto vrijeme i kao bitna funkcija menadžmenta same organizacije.

IT menadžeri moraju odrediti sigurnosne mjere koje IT sistemi moraju imati, kako bi bili u stanju dostići željeni nivo podrške misiji preduzeća u "stvarnom svijetu". Zbog toga bi proces upravljanja rizikom trebao biti tretiran primarno kao tehnička funkcija koju vrše IT eksperti, a u isto vrijeme i kao bitna funkcija menadžmenta same organizacije.

Većina organizacija ima ograničen budžet namijenjen IT sigurnosti, pa zbog toga se, u sklopu donošenja ostalih ključnih menadžerskih odluka, treba posvetiti posebna pažnja obezjeđenju tih sredstava. Dobro strukturirana metodologija upravljanja rizikom, može pomoći menadžmentu da identificira prikladne kontrole za pružanje sigurnosnih mjera bitnih za uspješno ostvarenje misije preduzeća.

2. KLASIFIKACIJA IT RIZIKA

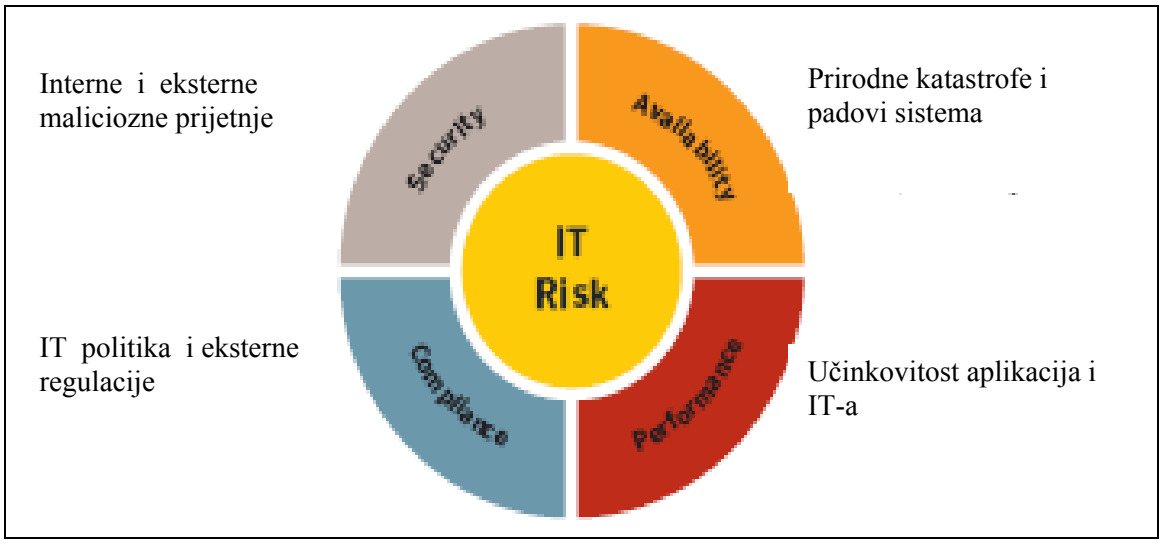
Četiri kategorije IT rizika su: sigurnosni rizici, rizici raspoloživosti, rizici učinkovitosti i rizici povjerljivosti i saglasnosti.

Sigurnosni rizici obuhvataju pojave neovlaštenog pristupa i korištenja informacija u konkurentske svrhe. Mogućnost da neovlaštene osobe mogu pristupiti ili koristiti važne poslovne informacije preduzeća predstavlja značajnu prijetnju kvalitetu poslovanja preduzeća.

Rizici raspoloživosti karakteriziraju pojave nepristupačnosti poslovnim podacima ili procesima a važne informacije ili aplikacije će biti nedostupne zbog pada sistema ili prirodnih katastrofa, što ustvari uključuje i bilo koji period oporavka elemenata IT sistema.

Rizici učinkovitosti (odgađanje pristupa poslovnim procesima ili podacima) – nedovoljna učinkovitost sistema, aplikacija ili osoblja (ili čak IT-a kao cijeline) će znatno umanjiti produktivnost i vrijednost poslovnih procesa.
Rizici povjerljivosti i saglasnosti (povreda pravne regulacije) – korištenje ili procesuiranje informacija neće ispunjavati norme i zahtjeve IT-a i poslovne politike.

Ove četiri kategorije obuhvataju sve elemente IT rizika, koji se mogu naći u organizaciji (Slika 1). Treba napomenuti da svaka organizacija ima svoj vlastiti profil IT rizika, pa je odredjivanje prioriteta elemenata rizika važan rani korak ka uspostavljanju efikasnog programa upravljanja IT rizikom.



Slika 1: Klasifikacija IT rizika

3. INTEGRACIJA PROCESA UPRAVLJANJA RIZIKOM U ŽIVOTNI CIKLUS RAZVOJA SISTEMA

Razvoj informacionog sistema se vrši prema okviru aktivnosti i zadataka poznatom kao životni ciklus razvoja sistema (System Development Life Cycle – SDLC), definisanjem svih glavnih specifikaciju čitavog procesa.
SDLC može biti korišten da osigura da se svi traženi zadaci završavaju – kompletiraju u određenom redoslijedu. Koristeći ovaj detaljan plan tj. okvir rada (framework), vrijeme i novac potrebno za svaki zadatak može biti izračunato i raspoređeno za sve formulisane zadatke, aktivnosti i individualne zadatke potrebne za razvoj IS-a.
Cijelim razvojnim procesom lako se može upravljavati da bi se projekat uspješno završio unutar ograničenog budžeta (novca) i rasporeda vremena. Kada je već jednom redoslijed zadataka poznat, efekat bilo kog kašnjenja u individualnom – pojedinom zadatku može biti prepoznat. Ako je to moguće, akcije treba preduzeti da bi se minimizirale posljedice (efekti) takvih kašnjenja.

Ne postoji jedinstven životni ciklus razvoja sistema koji je standardan za sve organizacije. Stvarni životni ciklus koji će se slijediti zavisi od organizacionog standarda, tj. izabranog okvira za SDLC. Svaki životni ciklus nudi različite olakšice i ističe određene aspekte razvojnog procesa. Uprkos ovih razlika, svaki životni ciklus razvoja sistema sadrži iste bazne olakšice, moguće samo različito nazvane i prezentirane u jednoj različitoj strukturi – okviru ili redoslijedu izvršavanja.
Minimiziranje negativnog uticaja na organizaciju i potreba za jednostavnošću u okviru donošenja odluka su osnovni razlozi zbog kojih preduzeća implementiraju proces upravljanja rizikom u okviru IT sistema.

Efektivno upravljanje rizikom mora biti potpuno integrisano u životni ciklus razvoja sistema SDLC, koji ima svojih 5 faza: inicijativu, razvoj, implementaciju, operaciju ili održavanje i stavljanje na raspolaganje. U nekim slučajevima razvoj IT sistema može zauzimati više faza u isto vrijeme. Kako god, metodologija upravljanja rizikom je ista, bez obzira na to u kojoj se fazi razvoj sistema nalazi.

3.1. Ključne uloge menadžmenta

Upravljanje rizikom je u odgovornosti menadžmenta. Ukratko ćemo objasniti ključne uloge osoblja koje treba podržavati i učestvovati u procesu upravljanja rizikom.

Top menadžment mora osigurati efikasnu primjenu potrebnih resursa u razvoju svih dijelova potrebnih za uspješno ispunjenje misije preduzeća. Oni su također zaduženi i za uključivanje rezultata aktivnosti pristupa riziku u proces donošenja odluka.

Menadžeri sistema i informacija su odgovorni za adekvatne kontrole koje su neophodne za očuvanje integriteta, povjerljivosti i raspoloživosti IT sistema i podataka sa kojima raspolažu. Oni su odgovorni sa sve promjene nastale u okviru IT sistema. Zbog toga, moraju odobravati svaku promjenu IT sistema (npr. proširenje sistema, veće promjene softvera i hardvera i sl.). Menadžeri sistema i informacija moraju razumjeti svoju ulogu u procesu upravljanja rizikom i u potpunosti ga podržavati.
Menadžeri poslovanja i funkcionalnosti su odgovorni za poslovne operacije i moraju igrati aktivnu ulogu u procesu upravljanja rizikom. Takvi menadžeri su pojedinci sa autoritetom i odgovornošću za donošenje odluka esencijalnih za ostvarenje misije. Njihovo učešće u procesu upravljanja rizikom omogućuje postizanje neophodne sigurnosti IT sistema, koja će, ukoliko se bude adekvatno postavila, omogućiti efikasnost ostvarenja misije uz minimalni utrošak resursa.
Menadžeri programa IT sigurnosti i uposlenici nadležni za kompjutersku sigurnost su odgovorni za program sigurnosti njihovog preduzeća, koji uključuje proces upravljanja rizikom. Oni igraju vodeću ulogu prilikom predstavljanja adekvatne, strukturirane metodologije za pružanje pomoći identificiranju, evaluaciji i minimiziranju rizika vezanih za IT sistem.

4. PROCES UPRAVLJANJA IT RIZIKOM

Pristup riziku je prvi proces u metodologiji upravljanja rizikom. On karakteriše odredjivanje obima potencijalnih prijetnji i rizika te njihov mogući uticaj na IT sistem, kroz njegov SDLC. Output ovog procesa pomaže identifikaciji odgovarajućih kontrola za smanjenje ili eliminaciju rizika tokom procesa njegovog ograničenja i smanjenja.

4.1. Karakterizacija sistema

U procesu pristupa riziku za IT sistem, prvi korak jeste definisanje obima aktivnosti. U okviru ovog koraka identificiraju se granice IT sistema zajedno sa resursima i informacijama koje grade taj sistem. Karakteriziranje IT sistema utvrđuje obim aktivnosti pristupa riziku i pruža informacije (npr. Informacije o hardveru, softveru, odgovornom dijelu organizacije te osoblju podrške) koje su od bitnog značaja za definisanje rizika.

Slijedeće tehnike, u pojedinačnom ili kombinovanom obliku, mogu se koristiti za sakupljanje informacija relevantnih za IT sistem u okviru njegovih operacionih granica: upitnici, intervjui „na licu mjesta” i pregledi dokumenata.

4.2. Identifikacija prijetnje

Cilj ovog koraka jeste identifikacija potencijalnih izvora prijetnje i sastavljanje liste potencijalnih izvora prijetnje koji mogu uticati na IT sistem koji se evaluira. Izvor prijetnje se definiše kao bilo koja situacija ili događaj koji u sebi nosi potencijalnu prijetnju da nanese štetu IT sistemu. Uobičajeni izvori prijetnje su prirodni faktori, ljudski faktori i faktori okruženja.

Kod pristupa izvoru prijetnje važno je uzeti u obzir sve potencijalne izvore koji bi mogli nanijeti štetu IT sistemu i njegovim dijelovima. Ljudi mogu biti izvor prijetnje kroz namjerno (kao npr. smišljeni napadi nezadovoljnih uposlenika) ili nenamjerno djelovanje (greške pri rukovanju). Jedan od primjera namjernih napada je kada programer koji radi u okviru IT sistema napiše ”Trojanca” radi zaobilaženja sistemske sigurnosti da bi došao do povjerljivih informacija.

4.3. Identifikacija ranjivosti

Analiza prijetnje IT sistemu mora uključiti analizu ranjivosti vezanih za sistemsko okruženje. Cilj ovog koraka jeste da se razvije lista sistemskih ranjivosti (slabosti) koje bi mogle biti eksploatisane od strane potencijalnih izvora prijetnji.
Preporučene metode za identificiranje sistemskih ranjivosti su: korištenje izvora ranjivosti, učinkovitost testiranja sigurnosti sistema i razvoj liste sigurnosnih potreba. Treba napomenuti da će tipovi ranjivosti koji će postojati, kao i metodologija koja je potrebna za određivanje i postojanje ranjivosti, varirati u zavisnosti od prirode IT sistema i slijedećih faza u kojim se, u svom SDLC-u nalazi.
Ukoliko IT sistem još uvijek nije dizajniran, potraga za ranjivostima se treba fokusirati na sigurnosne politike organizacije, planirane sigurnosne procedure i definisanje sistemskih potreba.
Ukoliko se IT sistem implementira, identifikacija ranjivosti bi trebala biti proširena do te mjere da uključuje više specifičnih informacija. Ukoliko je IT sistem operacionalan, proces identificiranja ranjivosti bi trebao uključiti analizu dijelova sigurnosti IT sistema i sigurnosnih kontrola, tehničkih i proceduralnih, koje se koriste za zaštitu samog sistema.

4.4. Analiza kontrole i određivanje vjerovatnoće

Cilj ovog koraka jeste analiziranje kontrola (koje su implementirane ili planirane za implementaciju) od strane organizacije radi minimiziranja ili eliminisanja vjerovatnoće da potencijalna prijetnja izazove ranjivost sistema.
Sigurnosne kontrole uključuju korištenje tehničkih i drugih metoda. Tehničke kontrole su zaštitari koji su utjelovljeni u kompjuterski hardware, software ili firmware (npr. mehanizmi kontrole pristupa, mehanizmi identifikacije, metode enkripcije, software za otkrivanje “uljeza”). Ostale kontrole su upravljačke i operacione kontrole, kao što su sigurnosne politike, operacionalne procedure te sigurnost osoblja, fizička sigurnost i sigurnost okruženja. Implementacija ovakvih kontrola tokom procesa minimiziranja rizika je direktan rezultat identifikacije nedostataka u trenutnim ili planiranim kontrolama tokom procesa pristupa riziku (npr. kontrole nisu tamo gdje bi trebale biti ili nisu adekvatno implementirane).

4.5. Analiza potencijalnog udara

Sljedeći značajan korak u mjerenju nivoa rizika jeste određivanje veličine udara kao rezultata uspješno provedene prijetnje, odnosno uspješnog iskorištavanja potencijalne ranjivosti. Prije nego što se počne sa analizom udara, neophodno je pribaviti sljedeće informacije, kao što je to već ranije opisano: sistemska misija (npr. procesi koje obavlja IT sistem), kritičnost sistema i podataka (npr. vrijednost ili važnost sistema za organizaciju) i osjetljivost sistema i podataka.
Integritet sistema i podataka se odnosi na potrebu da informacija bude zaštićena od neovlaštene modifikacije. Integritet je izgubljen ukoliko dođe do promjene podataka ili IT sistema putem namjernog ili slučajnog djelovanja. Ukoliko se gubitak integriteta sistema ili podataka ne ispravi, kontinuirano korištenje zaraženog sistema ili korumpiranih podataka može dovesti do neželjenih posljedica u vidu nepreciznih odluka, kriminalnih prevara itd. Također, povreda integriteta može biti prvi korak uspješnog napada na povjerljivost ili raspoloživost IT sistema.

4.6. Određivanje rizika

Svrha ovog koraka jeste pristup određivanju nivoa rizika za IT sistem. Određivanje rizika određenog para prijetnja/ranjivost može biti izraženo kao funkcija: vjerovatnoće da će dati izvor prijetnje pokušati iskoristi datu ranjivost, posljedica udara ukoliko dati izvor uspješno iskoristi ranjivost i adekvatnosti planiranih ili postojećih sigurnosnih kontrola za smanjenje rizika.

Sljedeća tabela pokazuje stepen ili nivo rizika kojem bi IT sistem bio izložen ukolikose iskoristi data ranjivost. U tabeli su također navedene i akcije koje top menadžment treba poduzeti za svaki nivo rizika.

Tabela 1. Nivo rizika i neophodne akcije

Nivo rizika	Opis rizika i neophodne akcije
VISOKI	Ukoliko se ustanovi da postoji visoki nivo rizika postoji snažna potreba za korektivnim mjerama. Postojeći sistem može nastaviti sa operacijama ali korektivne akcije se trebaju poduzeti što je prije moguće.
SREDNJI	Ukoliko se ustanovi da postoji srednji nivo rizika, korektivne akcije su potrebne. Plan za uključivanje ovih akcija se treba razviti u nekom razumnom periodu.
NIZAK	Ukoliko se ustanovi da postoji nizak nivo rizika treba se utvrditi da li postoji potreba za korektivnim akcijama ili će se ići na prihvatanje rizika

5. ZAKLJUČAK

Jasno je da poslovanje preduzeća može biti ugroženo unutrašnjim ili vanjskim prijetnjama koje iskorištavaju postojeće slabosti unutar IT mreža i sistema. Uspješno upravljanje IT rizikom je odlika najboljih organizacija, koje, iako se svakodnevno susreću sa višim nivoima IT rizika, imaju veoma nizak nivo incidenata, zbog pažljivih investicija koje održavaju visok nivo efikasnosti cijele tehnologije i procesnih kontrola IT sistema.

Uspješan program upravljanja rizikom će se oslanjati na podršku i zalaganje top-menadžmenta te punu podršku i učešće IT tima, koji mora biti dovoljno stručan da primjeni metodologiju pristupa riziku, da identificira rizike za misiju preduzeća i da primjeni troškovno opravdane kontrole i trajnu evaluaciju i pristup rizicima, koji se odnose na IT misiju. Samo uz aktivnu uključenost i razvijenu svijest o postojećim rizicima za IT sistem, moguće je govoriti o uspješnom procesu upravljanja IT rizikom za preduzeće.

6. LITERATURA

[1] Muratović H., Habul A.,: Analiza informacionih sistema, Ekonomski fakultet, Sarajevo, 2004.,
[2] Lagumdžija Z.,: Informatika za korisnike presonalnih kompjutera, Ekonomski fakultet, Sarajevo, 1999.,
[3] Bajgorić N.,: Menadžment informacijskih tehnologija, Ekonomski fakultet, Sarajevo, 2007.,
[4] Turban R., Potter R.,: Introduction to Information Technology, Wiley, 2005.,
[5] Stonebumer G., Goguen A., Feringa A.,: Risk Menagement Guide for Information Technology Systems, National Institute of Standards and Technology, July 2002