

1 Uvod

Porast konkurencije u oblasti proizvodnje softvera i insistiranje na brzom razvoju doveli su do mnogo neuspešnih projekata u poslednjih 20 godina. Godišnje se od neuspešnih softverskih projekata gube milijarde dolara. Neki od neuspeha su doveli do bankrota firmi, kao što je slučaj sa firmom FoxMeyer Dug Co. koja se bavila distribucijom lekova. Jedan od najvećih gubitaka imala je Federalna uprava letenja u SAD na projektu za unapređenje kontrole leta od kog se odustalo nakon 13 godina i 3 puta većih troškova nego što je planirano [2]. U tabeli 1 su prikazani još neki veći projekti koji su bili neuspešni. Po reputaciji kompanija na spisku možemo da zaključimo da je neobrađen rizik u razvoju projekata ozbiljan problem i u velikim kompanijama. Stendiš Grupa (eng. *Standish Group*) je sprovela istraživanje 1995. godine koje je obuhvatilo 8380 softverskih projekata. Projekti koji su završeni, ali je došlo do prekoračenja rokova i budžeta i kod kojih nisu sve funkcionalnosti implementirane činili su 53%, a otkazani projekti 31%. Samo 16% projekata je završeno na vreme i po planu. Istraživanje je pokazalo da je većina projekata bila neuspešna zbog lošeg vođenja projekta i da su se mnogi problemi mogli izbeći ili značajno umanjiti mogućnost za njihovo javljanje da je primenjen neki od metoda za upravljanje rizikom [3].

Tabela 1: Primeri velikih gubitaka usled grešaka u razvoju softvera [2]

Go-dina	Kompanija	Problem	Troškovi (u milionima dolara)
2004-2005	Poreska uprava VB	Softverske greške	3450
1994	Federalna uprava letenja u SAD	Odustajanje od projekta	2600
2004	J Sainsbury PLC	Odustajanje od projekta snabdevanja prodavnica	527
2004	Ford Motor	Odustajanje od projekta sistema kupovine	400
2002	McDonald's Corp.	Odustajanje od projekta sistema kupovine i informisanja	170
2001	Nike Inc	Odustajanje od projekta snabdevanja prodavnica	100

Ne postoji opšteprihvaćen metod za upravljanje rizikom. Neki od najpoznatijih metoda za upravljanje rizikom su: Boehm-ov, Riskit, SEI-SRE (eng. *Software Engineering Institute, Software Risk Evaluation*), SERUM

(eng. *Software Engineering Risk: Understanding and Management*). Ni za jedan od navedenih metoda ne može se reći da je najbolji jer svi imaju prednosti i mane. Za različite projekte različite osobine su poželjne i na osnovu toga se pravi izbor. Ukoliko postoji potreba za rešavanje eksplicitnih rizika, najčešće se bira SERUM koji modeluje proces razvoja softvera tako da se smanje rizici. Za organizovanje razvoja softverskog projekta uz detaljan model za upravljanje rizikom preporučuje se SEI-SRE metod. Riskit metod je najfleksibilniji od navedenih i može se primeniti ne samo za razvoj softvera već i u oblastima kao što su menadžment i poslovno planiranje [4]. Najstariji metod za upravljanje rizikom među navedenima je Boehm-ov metod, a njegov tvorac, Barry Boehm, smatra se “ocem procesa za upravljanje rizikom” [5]. Osnovne prednosti ovog metoda su njegova jednostavna primena, to što pokriva sve faze razvoja i može da se primeni na bilo koji tip razvoja softvera. Iako se smatra prvim formalno definisanim metodom za upravljanje rizikom u razvoju softvera, on se i danas koristi i daje podjednako dobre rezultate kao i metodi nastali posle njega. Tema ovog rada biće upravo Boehm-ov metod.

2 Upravljanje rizikom

Ne postoji razvoj softvera bez rizika. Procenjuje se da se 40-50% novca uloženog u projekat troši na naknadno ispravljanje grešaka nastalih kao posledica neobrađenih rizika [6]. U razvoju softvera rizik predstavlja sve ono što može da krene naopako i postane pretnja uspešnom dovršavanju projekta ili implementaciji softverskog sistema. Najbolji način da se smanji opasnost od rizika je njegovo prepoznavanje, praćenje i kontrola, tj. upravljanje rizikom. Najvažniji zadaci u upravljanju rizikom su: konstantno procenjivanje šta može da ugrozi projekat, odlučivanje koji rizici su dovoljno važni da bi se obrađivali i implementacija strategije koja će otkloniti te rizike. Na ovaj način se izbegava neuspeh, koji uključuje prekoračenje rokova, budžeta, dobijanje neupotrebljivog rezultata ili odustajanje od projekta.

Cilj Boehm-ovog pristupa je da smanji izloženost riziku pridruženu projektu. Izloženost riziku se računa za svaki posao, porede se rezultati za različite rizike i oni sa najvišim vrednostima se dalje obrađuju. Osnovni koraci ovog pristupa su procena rizika i kontrola rizika. Svaki od njih se sastoji od tri koraka, kao što je prikazano na slici 1.

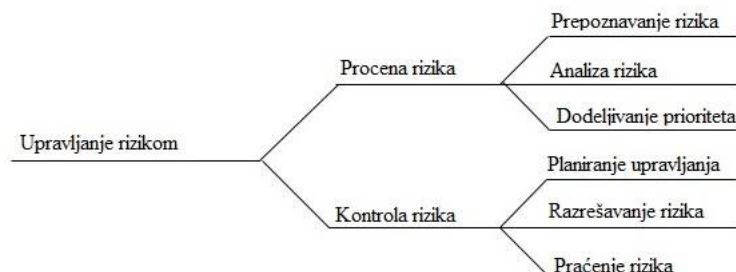
2.1 Procena rizika

Da bi razvojni tim mogao da obradi rizike, pre svega, neophodno je njihovo prepoznavanje. Kako se uvek može naći novi rizik koji nosi neka akcija projekta, treba spoznati rizike vredne obrade i one koji se mogu zanemariti. Zato prvi korak samog upravljanja rizicima jeste njihova procena. Osnovna podela akcija koje spadaju u procenu rizika je:

1. prepoznavanje rizika
2. analiza rizika
3. dodeljivanje prioriteta rizicima

Sve akcije procene rizika se obavezno rade na samom početku i predstavljaju osnovu svih narednih koraka. Ponovne procene rizika u toku rada na projektu su moguće i biće detaljnije opisane u odeljku 2.2.3.

Proces Upravljanja Rizikom



Slika 1: Koraci u upravljanju rizikom

2.1.1 Prepoznavanje rizika

Prepoznavanje rizika predstavlja najbitniji korak upravljanja rizicima. Bilo kakav propust u ovom koraku može dovesti do posledica koje bi dovele u pitanje ceo projekat. Zato se ovom koraku mora ozbiljno i sistematično pristupiti. U ovom koraku se kreira lista problema specifičnih za dati projekat.

Prema Boehm-u [1], 10 najčešćih uzroka pojave problema pri razvoju i tehnike koje se primenjuju za njihovo sprečavanje su:

1. Nedostatak kadrova
Potreban je dovoljan broj kadrova sa odgovarajućim iskustvom i znanjem u potrebnim oblastima.
2. Nerealni rokovi i budžet
Detaljno istraživanje i određivanje rokova i budžeta, inkrementalni razvoj, ponovna upotrebljivost softvera...
3. Razvoj pogrešnih funkcija
Organizaciona analiza, analiza cilja, formulacija operacija i koncepta, uključivanje klijenata u proces razvoja, analize kvaliteta...
4. Razvoj pogrešnih interfejsa
Pravljenje prototipa, različitih scenarija, uključivanje klijenata u proces razvoja...
5. Preterivanje (pozlaćivanje)
Dorađivanje zahteva, pravljenje prototipa, analize troškova i dobiti...
6. Nprekidni niz izmena u zahtevima
Ograničavanje broja dozvoljenih izmena u zahtevim, skrivanje informacija, inkrementalni razvoj (odlaganje izmena za kasnije faze)...
7. Slabosti u eksterno nabavljenim komponentama
Benčmark (eng. *Benchmark*) testovi, inspekcije, analiza kompatibilnosti, provera referenci...
8. Slabosti eksterno realizovanih poslova
Provera referenci, ugovori o nagradama, konkurentski dizajn ili prototipi (najbolji dobija posao), izgradnja timskog duha...

9. Slabe performanse u realnom radu
Simulacije, benčmark testovi, pravljenje modela, pravljenje prototipova...
10. Rad na granicama računarskih nauka
Tehničke analize, analize troškova i dobiti, pravljenje prototipova, provera referenci...

Postoje mnoge tehnike prepoznavanja rizika, neke od njih su:

Intervjuisanje

Jedna od tehnika je intervjuisanje učesnika u projektu, klijenata, prodavaca, itd. Neka od pitanja koja su karakteristična za ovu tehniku su:

- Koje su to nove ili unapređene tehnologije koje donosi ovaj projekat?
- Koji zahtevi postoje, a za koje nismo sigurni kako da ih implementiramo?
- Kakve zabrinutosti imamo oko toga da li imamo neophodne sposobnosti da zadovoljimo traženi kvalitet i performanse?

Volontersko prijavljivanje problema

Druga tehnika za prepoznavanje rizika bi bila volontersko prijavljivanje problema. Radi se o tome da se svaki pojedinac nagrađuje ukoliko skrene pažnju na neki problem. Time se ljudi koji nisu uključeni u sam projekat ohrabruju u pronalaženju potencijalnih problema.

Taksonomija rizika

Još jedna tehnika koja se koristi kod prepoznavanja rizika je taksonomija rizika. Ova tehnika uključuje provere lista problema koji su se pojavljivali na drugim projektima, čime se isključuje mogućnost pojave problema koji su već ranije rešeni.

2.1.2 Analiza rizika

Kada su uspešno pronađeni svi potencijalni problemi, potrebno je analizirati svaki od njih. Analiza rizika procenjuje verovatnoću i cenu za svaki element kreirane liste. Analiza rizika se zasniva na konceptu izloženosti riziku:

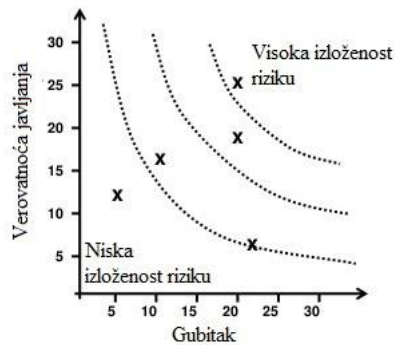
$$RE = P(UO) \cdot L(UO) \quad (1)$$

gde je:

- RE izloženost riziku (eng. *risk exposure*)
- P(UO) verovatnoća da dođe do nezadovoljavajućeg ishoda (eng. *probability of unsatisfactory outcome*)
- L(UO) gubitak do kog tada dolazi (eng. *loss due to unsatisfactory outcome*)

Zavisnost izloženosti riziku od verovatnoće nezadovoljavajućeg ishoda i gubitka usled javljanja ishoda prikazana je na slici 2. Tu se mogu uočiti dve oblasti: Oblast niske i oblast visoke izloženosti riziku. Kod niske izloženosti riziku, vrednosti verovatnoće javljanja nezadovoljavajućeg ishoda i gubitka kojeg do tada dolazi su male ili je barem jedna od njih

Izloženost riziku



Park, Port & Boehm (1999)

Slika 2: Izloženost riziku zavisno od verovatnoće nezadovoljavajućeg ishoda i gubitka

manja od jedan. Kod visoke izloženosti riziku, rizici sa velikom verovatnoćom javljanja imaju veliku cenu.

U razvoju softvera "nezadovoljavajući ishod" ima više značenja, zavisno od toga na kog učesnika u razvoju se odnosi. Za naručioce i razvijaoce nezadovoljavajući ishod je prekoračenje budžeta ili vremenskih rokova, za korisnike nefunkcionalan softver, loš korisnički interfejs, slabe performanse ili nepouzdan softver, a za održavaoce loš kvalitet softvera. Ove komponente omogućavaju identifikovanje i procenu rizika svake stavke [1]. Tehnike analize uključuju i pravljenje modela performansi, modela troškova, mrežne analize, statističke analize odlučivanja, analize faktora odlučivanja (poput pouzdanosti, dostupnosti i bezbednosti) itd.

2.1.3 Dodeljivanje prioriteta rizicima

Nakon korišćenja različitih tehnika prepoznavanja rizika, javlja se novi, veliki problem, a to je da će se u projektu identifikovati toliko rizika, da bi bile potrebne godine samo za njihovo istraživanje. To je trenutak kada dodeljivanje prioriteta rizicima dobija na velikom značaju.

Najefektivnije tehnike dodeljivanja prioriteta rizicima uključuju:

- analizu izloženosti riziku
- analizu uticaja
- redukciju povezanosti rizika.

U tabeli 2 prikazano je računanje faktora izloženosti riziku na primeru satelitskog eksperimenta [1]. Primećujemo da se i rizici koji su manje verovatni, zbog svoje velike cene, često svrstavaju u visoke rizike.

2.2 Kontrola rizika

Nakon procene, sledeća celina jeste kontrola rizika. Ona koristi podatke izračunate prethodnim koracima, tako da se verovatnoća pojave

Tabela 2: Računanje faktora izloženosti riziku na primeru satelitskog eksperimenta

Nezadovoljavajući ishod	Verovatnoća nezadovoljavajućeg ishoda $P(UO)$	Gubitak izazvan nezadovoljavajućim ishodom $L(UO)$	Izloženost riziku RE
Obustavljanje eksperimenta zbog softverske greške	3-5	10	30-50
Softverska greška, gubljenje ključnih podataka	3-5	8	24-40
Delovi aplikacije kod kojih su dozvoljene greške dovode do neprihvatljivih performansi	4-8	7	28-56
Softver za praćenje izveštava o nesigurnim uslovima kao sigurnim	5	9	45
Softver za praćenje izveštava o sigurnim uslovima kao nesigurnim	5	3	15
Greške softvera za redukciju podataka koji se čuvaju donose dodatni posao	8	1	8
Loš korisnički interfejs uzrokuje neefikasne operacije	6	5	30
Nedovoljno procesorske memorije	1	7	7
Softver za upravljanjem bazama podataka gubi dostavljene podatke	2	2	4

nekog od procenjenih rizika svede na minimum. Kontrola rizika se sastoji iz tri celine:

1. planiranje upravljanja rizicima

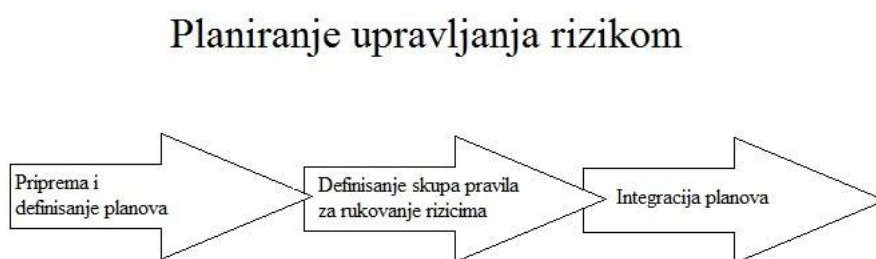
2. razrešavanje rizika

3. praćenje rizika

Svaka od ove tri celine je podjednako bitna i biće razmotrena u daljem tekstu.

2.2.1 Planiranje upravljanja rizicima

Informacije o veličinama i cenama rizika nemaju nikakvog značaja ako se one ne iskoriste kako bi se rizici smanjili ili potpuno eliminisali. Planiranje je zato potrebno odraditi sistematično i efikasno (slika 3). Započinje se pripremanjem planova koji će pokriti sve radnje potrebne da bi se suočili sa rizicima. Zatim je potrebno definisati skup pravila rukovanja svakim od rizika koji je procenjen. Na kraju se sagledava kompletna slika projekta, a planovi pojedinačnih rukovanja rizicima se integrišu.



Slika 3: Koraci u upravljanju rizikom

2.2.2 Razrešavanje rizika

Razrešavanje rizika predstavlja izvršavanje planova koji su navedeni i pripremljeni u prethodnom koraku. U ovom koraku se verovatnoća da do nekog rizika dođe eliminiše ili svodi na minimum. Razrešavanje rizika se sastoji od skupa prototipa, simulacija, testova, anketa ili bilo koje metode koja je navedena u planiranju.

Razrešavanje rizika možemo podeliti u kategorije:

- Izbegavanja
- Redukcije
- Deljenja
- Zadržavanja

Izbegavanje predstavlja promene plana u projektu, kako bi se izbegao rizik zbog prevelike cene ili nemogućnosti njegovog smanjenja. **Redukcija** predstavlja zadržavanje plana, ali promene alata kojim se stiže do željenog cilja, čime se rizik smanjuje na minimum. **Deljenje** rizika se koristi kada su u projektu 2 ili više kompanija, tj. razvojnih timova. Tada se rizik deli među kompanijama tako da njihovi delovi budu ispod praga dozvoljenih prekoračenja firme. **Zadržavanje** je najgori slučaj razrešavanja rizika, jer se tada rizik samo ignoriše (npr. određene funkcije programa ne rade ukoliko je miš postavljen na određenu tačku ekrana kada se u procesoru

izvršava određena instrukcija). Ova tehnika se koristi kada je rizik nebitan ili je cena njegovog izbegavanja veća od cene njegovog ignorisanja.

2.2.3 Praćenje rizika

Praćenjem razvoja projekta, neophodno je pratiti i rizike i izvršavati potrebne akcije kada je potrebno. Iako se procena rizika radi na samom početku, cena nekog rizika će se najčešće promeniti tokom napretka projekta. Zato se tokom razvoja projekta rade nove procene rizika. Tokom vremena, takođe se mogu pojaviti novi rizici. Nove rizike, kao i one koji su dobijeni inicijalnom procenom, potrebno je često osvežiti i sortirati po prioritetima koje rizike treba ukloniti što pre. Najčešća tehnika jeste lista od 10 (ili bilo koji drugi broj) najvećih trenutnih rizika. Nakon unapred određenog vremenskog perioda, ili u određenim trenucima vremena, vrši se nova procena rizika i pravi nova tabela na kojoj se vidi koji rizici su postali manje a koji više bitni. U tabeli 3 je dat primer praćenja rizika tokom projekta izrade grupnog seminarskog rada. Kao što možemo primetiti, moguće je da se pronađu i dopišu novi rizici, kao i da se neki rizici obrišu pošto su rešeni ili više ne predstavljaju pretnju.

3 Zaključak

Boehm-ov metod predstavlja osnovu bilo kakve ozbiljnije kontrole rizika u projektima, kao i najbolje rešenje za neiskusne timove koji obraćaju pažnju na opasnost od rizika u razvoju softvera. Lista od 10 najvećih rizika koja se prvi put javlja u ovom metodu je koristan princip koji se može primeniti u mnogim fazama razvoja. Pored toga, ona se jednostavno implementira i štedi vreme i napor jer se ne obrađuju svi rizici već samo oni najvažniji. Drugi koristan pristup je procena izloženosti riziku. Ovim se rizici mogu objektivnije oceniti i klasifikovati. Ipak, Boehm-ov metod ima i nedostatke koji se ne mogu ignorisati. Lista 10 najvećih rizika se mora konstantno pratiti i menjati. Pored toga, procena verovatnoće javljanja određenog rizika i gubitka u tom slučaju ne mogu biti 100% tačne. Međutim, pored svih nedostataka, Boehm-ov metod za upravljanje rizikom ima reputaciju jednog od najboljih metoda iz ove oblasti.

Tabela 3: Lista 10 najvećih rizika tokom izrade seminarskog rada

Rizik	Pret- hodni piori- tet	Tre- nutni piori- tet	Broj meseci na listi	Predloženo rešenje
Postoji previše grešaka u radu	4	1	3	Pregledati rad nakon kratkih intervala
Projekat nije moguće završiti na vreme	3	2	4	Unajmiti novog člana tima
Projekat je obrisao	/	3	2	Napraviti 3 odvojena backup-a
Članovi tima su odustali od projekta	2	4	4	Svaki član ima zamenu
Promašena je tema	8	5	4	Poslati mentoru dosadašnji rad radi provere da li se prati tema
Napisana je prevelika količina teksta	5	6	7	Izvršiti selekciju teksta ili reorganizovati temu
Napisana je premala količina teksta	7	7	3	Pronaći dodatne izvore i istražiti više o pojedinačnim tačkama teme
Neusklađenost teksta među članovima tima	6	8	2	Izabrati člana tima koji će modifikovati tekst tako da izgleda kao da ga je jedna osoba pisala
Nijedan računar članova tima nema mogućnost pokretanja svih izabranih biblioteka Latex-a	9	9	4	Potražiti računar od kolega kod kojih je moguć rad
Nije pronađena potrebna literatura	1	/	1	Konsultovati se sa mentorom radi dodatne literature

Literatura

- [1] Barry W. Boehm. *Software Risk Management: Principles and Practices*. IEEE Software 8(1), 1991.
- [2] Robert N. Charette. Why Software Fails. *IEEE Spectrum*, 2005.
- [3] John McManus. *Risk Management in Software Development Projects*. Butterworth-Heinemann, 2004.
- [4] Jose Carlos Arias Robert Stern. Review of risk management methods. *Business Intelligence journal*, 4(1), 2011.
- [5] Dr. E. Wallmüller. Risk Management for IT and Software Projects, 2013-2014. Qualität und Informatik, on-line at: <http://www.itq.ch/>.
- [6] Linda Westfall. Software risk management, 2002. The Westfall Team, on-line at: <http://www.westfallteam.com/>.