Implementacija procesa upravljanja rizicima u skladu sa CMMI standardom

Mr Jovan M. Popović, Gowi doo

***Abstrakt* — U ovom radu su predstavljeni problemi koji pogađaju organizacije koje imaju implementirane procese upravljanja rizicima. Pored toga je opisan jedan pristup upravljanju rizicima koji je usaglašen sa CMMI standardom kvaliteta. Na ovaj način je predstavljen proces upravljanja rizicima koji je dovoljno dobar da omogući organizacijama da se uspešno izbore sa rizicima u poslovanju.**

***Ključne reči* — CMMI, Management, Maturity, Process, Risks.**

I. UVOD

UPRAVLJANJE rizicima je danas nesumnjivo jedna od veoma važnih aktivnosti u svim kompanijama. U okruženju koje se stalno menja i gde se može očekivati da se dogode neočekivne stvari neophodno je imati nekakav proces kojim bi se predvidelo šta može da se desi na projektima, kako bi se ublažile posledice negativnih neočekivanih događaja.

Kao odgovor na sve prisutniju potrebu da se nepredviđeni događaji identifikuju i da se ublaži njihov negativan uticaj na projekat javila se potreba za implementacijom procesa upravljanja rizicima kojim bi se definisala metodologija kontrole rizika na projektima. Kao primer u softverskoj industriji ovi procesi su integrisani u sve moderne procese razvoja softvera kao što su *Rational Unified Process*(RUP)[1] ili *Microsoft Solution Framework*(MSF)[2].

Iako je upravljanje rizicima bitna aktivnost, u velikom broju kompanija se ona samo okvirno primenjuje. Veoma često rizici se identifikuju na osnovu ranijih iskustava jednostavnim kopiranjem skupa rizika iz projekta u projekat i služe samo kao formalna opomena o problemima koji mogu da se dogode. Reakcije na rizike su veoma često identične u slučaju kada se vrši „upravljanje rizicima“ kao i u slučaju kada se uopšte i ne vrši.

Kao primer može se posmatrati jedan od standardnih rizika koji se često dešava u svim projektima „Kašnjenje u isporuci“. Često se u listi rizika ovaj rizik dodaje kao opomena da će možda neko u procesu rada kasniti – bilo tim koji radi, dobavljač ili čak i klijent i služi kao opomena projektnom timu. Međutim kada se posmatra reakcija na ovaj događaj može se primetiti da se iste aktivnosti često vrše i sa i bez procesa upravljanja rizicima. Ako dođe do kašnjenja i ako je rok isporuke fiksan, projektni tim će morati da radi brže ili prekovremeno kako bi se dostigli rokovi uprkos kašnjenju. U slučaju da postoji identifikovan rizik kašnjenja, projektni tim će unapred biti svestan da će morati da radi prekovremeno dok u slučaju da nije identifikovan taj rizik moraće da rade prekovremeno tek kada shvate da je došlo do kašnjenja. Kao krajnji rezultat, u slučaju da se dogodi rizik doći će do prekovremenog rada bez obzira da li su na početku svi bili svesni toga ili ne, to jest bez obzira da li je bilo „upravljanja rizicima“ ili ne. U principu to nije proces upravljanja rizicima zato što se u kompanijama koje pravilno vrše upravljanje rizicima može jasno videti razlika u procesu razrešavanja rizika u slučaju da se primenjuje proces upravljanja rizicima ili ne. U konkretnom slučaju mogućeg kašnjenja umesto formalnog dodavanja rizika u listu bez saznanja zašto je taj rizik uopšte dodat, izvršila bi se analiza zašto taj rizik uopšte postoji. Ako je kašnjenje moguće zbog nove tehnologije u budžet projekta se može dodati vreme za analizu nove tehnologije. Ako je kašnjenje moguće zbog previše članova tima sa slabijim kvalitetima neki od njih se mogu zameniti kvalitetnijim ljudima. Ako to nije dovoljno, zaposleni koji rade na drugim projektima mogu delimično da rade i na rizičnom projektu kako bi se upoznali sa projektom i uključili u periodima kada se na projektu kasni sa radom kako bi se dodavanjem ljudi smanjila potreba za prekovremenim radom. Kao što se vidi ispravnim procesom upravljanja rizicima se može videti razlika u procesu razrešavanja rizika kada se upravljanje rizicima ispravno izvodi i kada se samo formalno identifikuju rizici. U nastavku je prikazan proces upravljanja rizicima koji je u skladu sa jednim od najbitnijih svetskih standarda ocene kvaliteta organizacionih procesa – CMMI.

II. CMMI STANDARD

Po *Capability Maturity Model Integration* (CMMI) [4-7] standardu ocenjuje se zrelost procesa u organizaciji na osnovu skupa uobičajenih procesa koji se primenjuju u praksi. Svakoj organizaciji se može dodeliti ocena od 1 do 5 u zavisnosti od procesa koji se primenjuju. Veoma često ocena zrelosti organizacije po CMMI kriterijumu je preduslov za dobijanje poslova a i bez toga svedoči o kvalitetu organizacije. Procesi mogu biti iz različitih grupa kao što je upravljanje projektom (gde spadaju planiranje, nadgledanje projekta, upravljanje rizicima), inženjering (upravljanje zahtevima, specifikacija zahteva, tehnička rešenja, integracija proizvoda, verifikacija), upravljanje procesima (definisanje standardnih organizacionih procesa, organizacione inovacije) i podrške (merenje i analiza,

Mr Jovan Milan Popović, Gowi doo, Maksima Gorkog 2, Pančevo, Srbija, (tel: +381-13-332-212; e-mail:jovan.popovic@gowi.rs). .

analiza uzroka, upravljanje konfiguracijom). U trenutnoj verziji postoji ukupno 22 procesa koji se ocenjuju.

Upravljanje rizicima predstavlja jedan od procesa koji se moraju implementirati u organizaciji kako bi se dobila ocena 3 po CMMI skali. Organizacije sa ocenom 3 imaju stabilne i definisane organizacione procese koji se na isti način primenjuju na svim projektima.

III. Primer procesa upravljanja rizicima

Proces upravljanja rizicima je proces kojim se svi negativni događaji koji mogu ugroziti projekat identifikuju i izbegavaju koliko je to moguće. Iako se ovaj proces vrši na pojedinim projektima njegova osnova leži u generalnim organizacionim procesima pošto je potrebno imati istorijske informacije o rizicima i načinima njihovog razrešavanja. Ovo je opšti organizacioni proces koji se primenjuje na pojedinim projektima ali je jedinstven za celu organizaciju.

Kao primer procesa upravljanja rizicima može se posmatrati proces definisan u MSF [3] modelu – ovaj proces je prikazana na slici 1.

Slika. 1. Upravljanje rizicima u organizaciji po MSF modelu.

Osnova za proces upravljanja rizicima je baza znanja o rizicima koja predstavlja skup svih istorijskih podataka o rizicima koji su se desili u prošlosti, njihov uticaj kao i načine na koji su oni ublažavani u prošlosti. Bez ove baze je nemoguće upravljati rizicima pošto nema dovoljno podataka o mogućim rizicima. Naravno čak i ako se adhoc napravi lista rizika na novom projektu oni se mogu koristiti ali bez ostalih informacija kao što je uticaj pojedinih rizika i pod kojim uslovima se mogu dogoditi, upravljanje rizicima nije efikasno kao u slučaju kada postoje istorijski podaci. Baza rizika je potrebna kako bi se na osnovu nje identifikovali rizici koji se mogu desiti na projektu čime se definiše dokument rizika.

Pošto se definiše dokument rizika oni se analiziraju, dodeljuju im se prioriteti i verovatnoće pojave kako bi se kreirala lista svih mogućih projektnih rizika i fokusiralo prvo na najkritičnije. Planovi se kreiraju u skladu sa rizicima tako da se maksimalno moguće izbegnu ili ublaže. U procesima razvoja kao što je RUP postoji i koncept planiranja zasnovanog na rizicima gde se kompletno planiranje razvoja bazira ne samo na zahtevima koji će se realizovati nego i na rizicima koje treba izbeći.

Kao deo kontrole aktivnosti na projektu vrši se i nadgledanje rizika kao i ažuriranje liste rizika kako bi se eventualno promenio raspored prioriteta rizika u listi. Pored toga, za sve rizike koji se ostvare unose se informacije u glavnu bazu znanja o rizicima kako bi se te informacije koristile dalje u novim projektima.

Na ovaj način je prikazan jedan iterativni proces koji nastaje iz organizacionih informacija i iskustvima o rizicima i koji se iterativno vrši tokom pojedinih projekata i ažurira bazu znanja kako bi se informacije koristile u daljem radu. U nastavku rada je detaljnije opisan ovaj proces u skladu sa zahtevima koje mora da ispuni kako bi bio validan po CMMI standardu.

IV. Upravljanje rizicima po CMMI standardu

Proces upravljanja rizicima je proces iz grupe procesa upravljanja projektom koji se mora koristiti u organizacijama na nivou zrelosti tri. Prema CMMI kriterijumima da bi se proces upravljanja rizicima koji se koristi u organizaciji prihvatio potrebno je ostvariti tri cilja u okviru ovog procesa. Ciljevi su:

1. Priprema za upravljanje rizicima,
2. Identifikacija i analiza rizika,
3. Kreiranje planova za prevenciju i ublažavanje rizika.

Metode kojima se mogu dostići navedeni ciljevi su objašnjene u nastavku rada.

A. Priprema za upravljanja rizicima

Priprema za upravljanje rizicima predstavlja skup aktivnosti koje se moraju sprovesti kako bi se rizici mogli kontrolisati. Uglavnom se ove aktivnosti fokusiraju na definisanje procesa upravljanja rizicima i strukture baze rizika. Aktivnosti koje se moraju sprovoditi su:

1. Utvrđivanje izvora i kategorija rizika,
2. Definisanje parametara rizika,
3. Uspostavljanje strategije za upravljanje rizicima.

Utvrđivanje izvora i kategorija rizika služi za definisanje strukture baze znanja o rizicima. Izvori rizika predstavljaju kanale odakle dolaze rizici – oni mogu biti ili interni ili eksterni. Primeri internih izvora rizika mogu biti tim koji radi na projektu, infrastruktura koja se koristi u organizaciji, organizacioni procesi koji se primenjuju, znanje koje je nedovoljno, dizajn koji je neadekvatan i slično. Eksterni rizici mogu biti zahtevi, klijenti, zakonske regulative, tehnologija koju treba koristiti, dobavljači i slično. Kategorije rizika predstavljaju grupe u koje se mogu staviti poznati rizici kako bi se lakše sa njima radilo. Primeri kategorija rizika mogu biti rokovi, budžet, resursi, testiranje i slično.

Definisanje parametara rizika predstavlja identifikaciju svih informacija koje opisuju rizike i koje se moraju sakupljati iz realnih projekata kada se novi rizici dodaju u bazu rizika. Parametri rizika mogu biti verovatnoća pojavljivanja rizika, njihov uticaj i kriterijumi kojima se definiše kada treba obratiti veću pažnju na rizik u projektima. Pored parametara rizika kao statičkih podataka potrebno je definisati i kriterijume kojima se ocenjuje stvarna verovatnoća rizika. Ovi kriterijumi se koriste kako bi se odredilo kolika je konkretna verovatnoća pojave rizika na pojedinim projektima.

Strategija predstavlja metodologiju koja će se koristiti u pojedinim projektima radi upravljanja rizicima.

Strategijom se definišu metode i alati koji će se koristiti, načini za kategorizaciju, poređenje i konsolidaciju rizika, mere i vremenski trenuci koji će se koristiti prilikom nadgledanja statusa rizika, granične vrednosti parametara rizika koje treba da se dostignu kako bi se preduzimale aktivnosti za ublažavanje rizika, planovi za ublažavanje i otklanjanje rizika i slično.

B. *Identifikacija i analiza rizika*

Kada se počne proces upravljanja rizicima na konkretnim projektima na osnovu podataka iz baze rizika se identifikuju i analiziraju svi rizici koji se mogu desiti na konkretnom projektu. U okviru identifikacije i analize rizika se vrše sledeće aktivnosti:

1. Identifikacija rizika,
2. Evaluacija, kategorizacija i prioritizacija rizika.

Identifikacija rizika predstavlja proces kojim se pronalaze oni rizici iz baze koji se mogu desiti na projektu. Ovi rizici se identifikuju tako što se posmatraju svi neuobičajeni aspekti u projektu i utvrđuje da li su oni izvori nekih rizika u bazi. Kao primer, ako se radi sa novom tehnologijom u bazi rizika se može nalaziti informacija da nova tehnologija može biti izvor rizika kašnjenja usled nerazumevanja ili stabilnosti aplikacije, ili usled činjenice da nove tehnologije nisu ispitane. Na ovaj način se formalno identifikuju oni rizici za koje postoji objektivni razlog zašto ih treba pratiti u projektu.

Postoje i formalniji procesi identifikacije rizika kao na primer identifikacija rizika primenom taksonomija [8-9], gde se na osnovu predefinisane taksonomije potencijalni problemi klasifikuju kako bi se identifikovali rizici koji se mogu desiti na projektu. U ovom pristupu postoje standardni upitnici koje treba popuniti kako bi se na osnovu njih identifikovali rizici koji se mogu desiti na projektu.

Kategorizacija rizika predstavlja proces grupisanja rizika na osnovu organizacionih pravila za kaegorizaciju. Evaluacija predstavlja proces analize kojim se utvrđuje verovatnoća događanja identifikovanih rizika kao i njihov uticaj na projekat kako bi se pronašao skup od nekoliko najkritičnijih rizika. Uticaj se određuje na osnovu podataka iz baze rizika tako što se pronalazi kako su identifikovani rizici uticali na prethodne projekte gde su se desili (npr. kašnjenje od 20 dana, povećan broj grešaka za 10%). S obzirom da se uticaji pojedinih rizika izražavaju u različitim merama potrebno ih je uniformisati u zajedničku meru koja predstavlja uticaj rizika na projekat. U praksi se pokazalo da je korisno da se kao zajednička mera uzme novac pošto se najviše pažnje obraća na rizik kada se zna koliko će kompanija morati da plati ako se on ostvari.

Pored uticaja, za svaki rizik se određuje i verovatnoća da će se rizik ostvariti. Verovatnoća rizika se može dodeliti opisno (malo verovatan, moguć, siguran) a može mu se dodeliti i konkretna numerička vrednost u obliku verovatnoće koja se kreće od 0 do 100%. Formalno, verovatnoća rizika se može odrediti statistički tako što se u bazi rizika utvrdi na koliko projekata u prošlosti je bio identifikovan pojedini rizik i na koliko od tih projekata se taj rizik stvarno i dogodio. Ovo je još jedan način koji pokazuje kolika je važnost istorijskih podataka. Cilj određivanja uticaja i verovatnoće je određivanje prioriteta rizika. Pojedinačno gledano uticaj i važnost ne mogu izolovano dati korisnu informaciju o važnosti rizika pošto postoje rizici koji mogu izazvati ogromne finansijske gubitke ali je mala verovatnoća da će se desiti, dok sa druge strane postoje rizici koji će se vrlo verovatno dogoditi ali je šteta koju će napraviti zanemarljiva. Pravi prioritet rizika se može dobiti množenjem verovatnoće rizika i njegovog uticaja čime se dobija validna mera važnosti pojedinih rizika. Na osnovu ovako definisanog prioriteta, može se dobiti lista rizika u kojoj se najviše pažnje obraća na najprioritetnije.

C. *Prevencija i ublažavanje rizika*

Najvažniji deo procesa upravljanja rizicima je prevencija rizika (*risk mitigation*). Prevencija rizika predstavlja skup akcija koje je potrebno preduzeti kako bi se rizici ili sprečili ili smanjila verovatnoća da se dese, kao i skup aktivnosti koje je potrebno preduzeti kako bi se ublažio negativan uticaj na projekat u slučaju da se rizik stvarno desi. Bez aktivnosti prevencije i ublažavanja rizika organizacije samo mogu da konstatuju da su predvidele rizike i da posmatraju da li rizici upropaštavaju projekte ili ne. Metode prevencije rizika prave razliku između nemih posmatrača i aktivnih „boraca protiv rizika“. Kako bi se ostvarila efikasna prevencija rizika potrebno je uraditi sledeće aktivnosti:

1. Razvoj plana prevencije rizika
2. Implementacija plana ublažavanja

Razvoj plana prevencije rizika (*develop risk mitigation plans*) predstavlja skup aktivnosti kojima se definiše šta će se raditi sa rizicima koji su identifikovani na projektu. Plan prevencije uključuje sve tehnike i metode koje se koriste kako bi se rizici izbegli, redukovali i kontrolisali tokom trajanja projekta. Ovaj plan definiše na koji način se rizici nadgledaju i koje aktivnosti je potrebno sprovesti kada verovatnoća pojave rizika dođe do granice kada se mora reagovati na njega kako bi se izbegao negativan uticaj na projekat. Opcije za obradu rizika mogu biti:

1. Izbegavanje rizika (*avoidance*) koje se vrši promenama ili uklanjanjem zahteva ili faktora koji uzrokuju rizike ukoliko je to moguće,
2. Kontrola rizika koja predstavlja preduzimanje koraka kojima se umanjuje verovatnoća pojave ili uticaj rizika na projekat,
3. Transfer rizika predstavlja prebacivanje zahteva ili tehnologije na druge strane kako bi se umanjili rizici,
4. Nadgledanje rizika koje predstavlja ubacivanje u plan projekta periodičnih aktivnosti kojima bi se rizici nadgledali kako bi se preduzela neka druga akcija u slučaju da se parametri rizika (verovatnoća ili uticaj) značajno promene,
5. Prihvatanje rizika koje predstavlja pasivnu akciju gde se prihvata činjenica da rizik postoji ali se ne radi ništa povodom toga uglavnom zato što ne postoji ni

jedan način da se na rizik utiče. Prihvatanje rizika ne bi trebalo da bude pravilo nego izuzetak i potrebno je dokumentovati zašto je odabrana ova opcija.

Veoma često se za jedan rizik odabere više od jednog navedenog metoda kako bi se rizik što je moguće više umanjio. Tokom kreiranja plana prevencije rizika bitno je odrediti granične vrednosti rizika (*thresholds*) koje određuju granične vrednosti parametara rizika kada se menja metoda prevencije rizika.

Pored navedenih planova za prevenciju kojima se proaktivno ublažavaju rizici, u procesu upravljanja rizicima se definišu i planovi za ublažavanje štete u slučaju da se rizici i ostvare (*contingency plans*). Iako postoje planovi za prevenciju rizika niko ne može da garantuje da će oni uspeti stvarno i da otklone sve rizike tako da se mora očekivati da se neki rizici i ostvare. Ako se ti rizici ostvare potrebno je imati plan koji bi reagovao na ostvareni rizik i sprečio dalji negativni uticaj na projekat.

Implementacija planova ublažavanja rizika predstavlja konkretne akcije koje se sprovode kako bi se realizovala borba protiv ostvarenog rizika. U skladu sa metodama ublažavanja rizika se ažurira projektni plan kako bi se u njega unele aktivnosti koje se moraju sprovesti tokom životnog ciklusa projekta kako bi se ublažila nastala šteta. Ove aktivnosti mogu biti primena nove tehnologije, zamena članova tima, promena specifikacije i slično. Ako se ove aktivnosti ne unesu u plan projekta pojavljuje se drugi rizik da nikada neće biti preduzete i da se proces upravljanja rizika neće ni započeti za neke rizike.

Poslednja aktivnost u implementaciji rizika je sakupljanje podataka kojima će se ažurirati baza rizika. Sakupljanje podataka je potrebno kako bi se iskustva koja se prikupe na projektu sačuvala od zaborava i iskoristila za buduće projekte. Proces upravljanja rizika je iterativni proces koji se ponavlja na projektima i veoma je bitno da se održi kontinuitet primopredaje informacija između baze znanja rizika i konkretnih projekata.

V. ZAKLJUČAK

Upravljanje rizicima je izuzetno bitna aktivnost posebno imajući u vidu današnje uslove brzih promena tehnologije i oštrih rokova usled konkurencije. Bez obzira na delatnost kojom se bave pojedine kompanije svi projekti koji se realizuju imaju dosta faktora koji im mogu naneti veliku štetu ako se na vreme ne identifikuju i otklone ili ublaže tako da danas ne postoji projekat koji se može implementirati bez ovog procesa.

Veoma često se procesu upravljanja rizicima pristupa nedovoljno sistematično razvijanjem novih strategija za borbu protiv rizika na svakom projektu. Ove strategije se zasnivaju više na iskustvu i sposobnosti pojedinaca da se izbore sa rizicima. Ovaj pristup je suviše nesiguran da bi garantovao kompanijama da će se uspešno izboriti sa rizicima i zato je potrebno standardizovati proces upravljanja rizicima koji bi se na konzistentan način primenjivao na svim projektima u organizaciji. Pored toga, korišćenjem ovakvog pristupa se ne gube dragocena znanja i iskustva stečena na pojedinim projektima bez mogućnosti da se ona iskoriste u budućnosti.

Proces upravljanja rizicima je sistematičan organizacioni proces koji se primenjuje na svim projektima u organizaciji. Ovaj proces se bazira na istorijskim podacima i znanju koje se stalno primenljuje na novim projektima. Znanje se sa druge strane se ažurira novim iskustvima stečenim na projektima čime se zatvara krug kontinualnog sazrevanja organizacionih procesa.

U ovom radu je predstavljen jedan način implementacije procesa upravljanja rizicima koji je u skladu sa CMMI standardom za ocenu kvaliteta i zrelosti organizacija. S obzirom da je CMMI standard napravljen kao kolekcija standardnih procesa koje primenjuju najuspešnije firme koje sa većom verovatnoćom od ostalih uspevaju da se izbore sa problemima koji pogađaju sve, može se smatrati da je prikazani proces upravljanja rizicima dovoljno dobar za primenu u praksi.

Ovaj rad koji se bazira na principima CMMI standarda kojim se definišu kriterijumi za ocenu kvalitetnog procesa upravljanja rizicima, predstavlja uputstvo za praktičnu primenu aktivnosti upravljanja rizicima u praksi i kao takav može pomoći organizacijama iz različitih oblasti rada da se izbore sa problemima koji ih pogađaju tako što na efikasan način vrše prevenciju rizika.

REFERENCE

[1] R. Kruchten „The Rational Unified Process – An Introduction", Addison-Wesley, Boston, USA, 2000

[2] „Microsoft Solutions Framework version 3.0 Overview", White paper, published 2003, Microsoft

[3] „Preparation Guide for Exam 70-300: Analyzing Requirements and Defining Microsoft .NET Solution Architectures, Microsoft, September 2008.

[4] CMMI Product Team, "Capability Maturity Model Integration, Version 1.1", Carnegie Mellon, Software Engineering Institute, March 2002

[5] M. Chrisis, M. Konrad, S. Shrum, "CMMI – Guidelines for Process Integration and Product Improvement", SEI Series in Software Engineering, Addison-Wesley, Boston USA, 2003

[6] CMMI-DEV standard v1.2, Carnegie Mellon Software Engineering Institute, online resources. Available on the address: http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm

[7] T. Kasse, "Practical Insight into CMMI", Artech House, Boston-London, 2004.

[8] M. Car, "Taxonomy-Based Risk Identification", Technical Report, CMU/SEI-93-TR-006, June 1993.

[9] S. Maniasi, P. Britos, R. García-Martínez. "A Taxonomy-Based Model for Identifying Risks", JIISIC'2006. pp.13~18

ABSTRACT

In this paper are presented problems and issues that that affect organizations where risk management process is implemented. Also, here is described one approach for implementation of the risk management process that is compliant with CMMI maturity standard. This way is presented risk management process that is good enough to help organizations to handle any risk that might affect their business.

Implementation of Risk Management process compliant with CMMI standard

Jovan M. Popović, Gowi doo