PD.TVZ.HR
POLYTECHNIC & DESIGN Vol. 9, No. 2, 2021.
Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995
DOI: 10.19279/TVZ.PD.2021-9-2-04

RIZICI NA PROJEKTU

PROJECT RISKS

Edmond Krusha[1,2], Alan Mahmutović[2]

[1]Tehničko veleučilište u Zagrebu, Vrbik 8, Zagreb, Hrvatska,
[2]Visoka škola za informacijske tehnologije u Zagrebu, Klaićeva 7, Zagreb, Hrvatska

SAŽETAK

U ovom radu obrađen je jedan od važnih elemenata u projektiranju. U svakodnevnom životu donose se odluke koje utječu na svakodnevnicu i kroje nam dalekosežno naše živote. Upravo te odluke koje se donose, mogu u sebi sadržavati rizike kojih nismo svjesni i koji mogu značajno utjecati u sve sfere poslovanja. U informacijskim tehnologijama najčešće se govori o operativnim rizicima. Tu se misli na vjerojatnost potencijalnih gubitaka zbog neorganiziranosti i nedovoljne informatičke podrške, organizacijskih problema, ljudskog faktora, zlouporabe i prijevare, i sl. Ovim radom se ukazuje na važnost rizika kao svakodnevne pojave u upravljanju rizicima u poslovnom odlučivanju.

Ključne riječi: *upravljanje rizicima, projekt, faktori rizika, metoda kritičnog puta*

ABSTRACT

In this paper processed is one of the important elements in the design. In everyday life, decisions are made that affect the everyday and tailor our far-reaching our lives. It is these decisions that are made, may contain the risks of which we are aware and which may have a significant impact in all areas of business. In information technologies most often talks about operational risk. This refers to the probability of potential losses due to lack of organization and lack of IT support, organizational problems, human factors, abuse and fraud, and etc. This paper emphasizes the importance of risk as everyday occurrences in risk management in business decision making.

Keywords: *risk management, project, risk factors, critical path method*

1. UVOD
1. INTRODUCTION

"Najveći je rizik ne prihvatiti nikakav rizik." (P. Drucker) [1]

U svom radu Pašić (2009) navodi da upravljanje rizikom još je jedno od područja koje voditelj projekta treba svladati. Iako će nam se često činiti da naš projekt nije rizičan, da je sve jasno i pod kontrolom, ne smijemo zaboraviti da su projekti i po definiciji rizični: ***„Jednokratni poduhvati u ograničenom vremenu i s ograničenim resursima s ciljem postizanja jedinstvenog rezultata".***

Rječnik PMI organizacije rizik definira kao „neizvjestan događaj ili stanje koje, ako se pojavi, ima pozitivan ili negativan utjecaj na ciljeve projekta." [2]. U svom radu Deković, Žaja i Smiljčić (2017) navode da rizik predstavlja vjerojatnost da se ono što se planira neće ostvariti, a izvedeno iz neizvjesnosti budućih događaja. Uz pojam rizika veže se izlaganje opasnosti - u osnovi je percipiran kao negativna pojava. „Rizik je stanje u kojem postoji mogućnost negativnog odstupanja od poželjnog ishoda koji očekujemo ili kome se nadamo. Stoga možemo reći da bi rizik postojao u financijskom poslovanju mora: biti moguć, izazivati ekonomsku štetu, biti neizvjestan i biti slučajan." [3]

2. RIZICI NA PROJEKTU
2. PROJECT RISKS

Prije razmatranja rizika na projektu, postavlja se sljedeće pitanje: "Kupiti ili izraditi vlastiti informacijski sustav?"

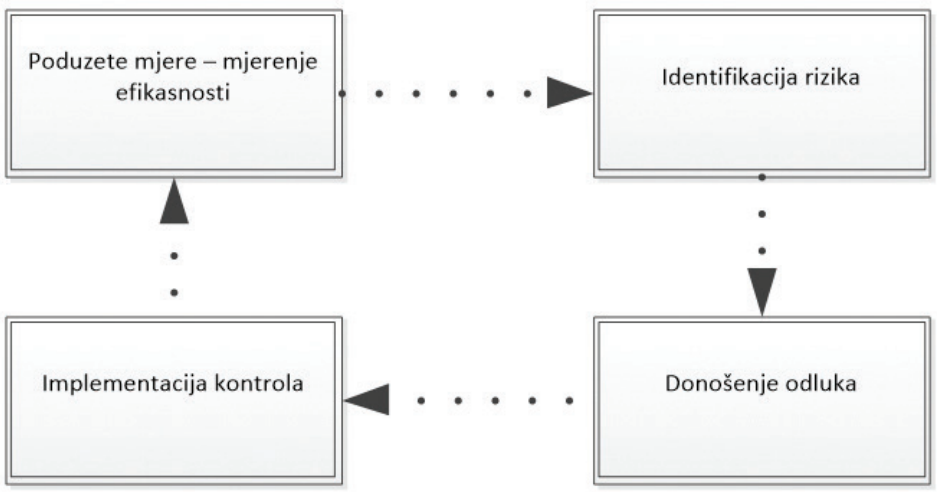
Odgovor na ovo pitanje strateška je odluka poslovodstva, s dalekosežnim posljedicama za svaku tvrtku. S obzirom da postoje više mogućnosti, napomenut ćemo neke od njih:

1. samostalno razvijanje i izrada informacijskog sustava, prema vlastitim potrebama i poslovnoj tehnologiji (tzv. "make" pristup),
2. prepuštanje kompletne realizacije posla nekom trećem, koji je vlasnik sustava (engl. "outsourcing"),
3. kupovina gotovog rješenja (tzv. "buy" pristup) ili
4. kupovina pojedinih modula sustava od raznih dobavljača najpoznatijih za pojedina poslovna područja i kombinirati ih (tzv. "best of breed" pristup).

Naravno, kao i u ostalim područjima tako i u ovom segmentu, svaka od navedenih mogućnosti ima prednosti i mane, koje moraju biti poznate svim sudionicima u odlučivanju. Kriteriji za izbor najpovoljnije varijante su povoljan odnos između:

- ekonomskih faktora (ukupna cijena),
- ocjene funkcionalnosti sustava i parametara kvalitete, pri čemu je otežavajući faktor izbor odgovarajuće tehnološke infrastrukture poput hardvera, mrežnog softvera, operativnog sustava itd., u slučaju kada tvrtka ne razvija vlastiti sustav.
- Rješenja koja razvija tvrtka ili se izrađuju na njen zahtjev, često su značajno skuplja i njihov razvoj i uvođenje dulje traje od gotovih proizvoda na tržištu.
- Ako se kupuje gotovo rješenje, u troškove treba ukalkulirati i održavanje, unapređivanje i dogradnju sustava, čime se može značajno povećati ukupna cijena.
- U tom slučaju postavlja se i pitanje vlasništva nad softverom, odnosno je li softver kupljen ili je kupljeno samo pravo korištenja (licence) ili je softver vlasništvo treće osobe koja obavlja outsourcing.
- Komercijalni paketi, ali i vanjski suradnici (eng. oursourcing) može biti pogodniji za održavanje jer su garantirana češća ažuriranja i prilagodbe softvera novim tehnološkim mogućnostima budući su tvrtke često vrlo aljkave u unapređivanju postojećih rješenja kao i usvajanju novih znanja.
- Međutim, kod kombiniranja kupnje gotovih rješenja s vlastitim razvojem ili kod kupnje rješenja od različitih dobavljača, česti su problemi s integracijom aplikacija kao i njihova ograničena fleksibilnost, pa u konačnici ukupni troškovi vlasništva (TCO – *Total Cost of Ownership)* mogu biti znatno veći.
- Izuzetno važan faktor jest postizanje neovisnosti tvrtke o jednom dobavljaču, jednom proizvođaču ili jednom manageru.

Iz Slike 1., može se iščitati da su procesi upravljanja rizikom kontinuirani i neprekidni i odvijaju se u ciklusima.



Slika 1 *Upravljanje rizikom*

Figure 1 *Risk management*

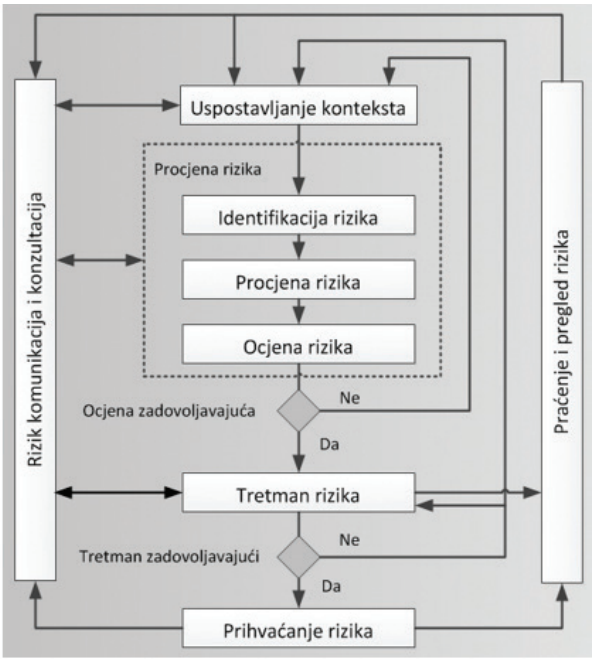
Što pokreće rizike? Neozbiljno shvaćanje rizičnih situacija, ljudi po svojoj prirodi ne vole biti kontrolirani, neznanje ili nedovoljna upućenost u problematiku, nema kontrole operativnih rizika, prihvaćanje rizika bez želje da se spriječi, i dr.

Pogledom mrežne stranicu tvrtke Span, [4] saznajemo sljedeće zanimljive podatke:

- U 8 od 10% globalnih spam poruka nalazi se zlonamjerni sadržaj
- 65% ukupne količine e-pošte čine spam poruke
- 75% Postotak organizacija s Adware infekcije (reklamni materijal (često neželjeni) kada je korisnik na mreži.)
- Postotak povreda sigurnosti na poslovne procese iznosi 36%, financije 30% i sl.

Može se reći da se gruba podjela rizika odnosi na opće i specifične rizike. Opći rizici su i mogu biti, osnovni rizici, špekulativni, pojedinačni, statistički, financijski i nefinancijski i sl.

Lakše i jednostavnije razumijevanje i shvaćanje pojma rizika, pruža primjer upisa u prvu godinu fakulteta ili neke druge visokoškolske ustanove: neočekivano velik ili mali broj prijavljenih studenata, mogu proizvesti pozitivne ili negativne učinke. Naime, prijava malog broja studenata može dovesti do ukidanja određenog studijskog programa, nestanka jednog određenog zanimanja a time i budućih radnih mjesta. Isto tako, ako interes studenata za neki studijski program naglo poraste, postavlja se pitanje treba li dozvoliti neograničeni upis ili je potrebno ciljano ograničiti kvote upisa i prilagoditi ih kapacitetu visokoškolske ustanove.



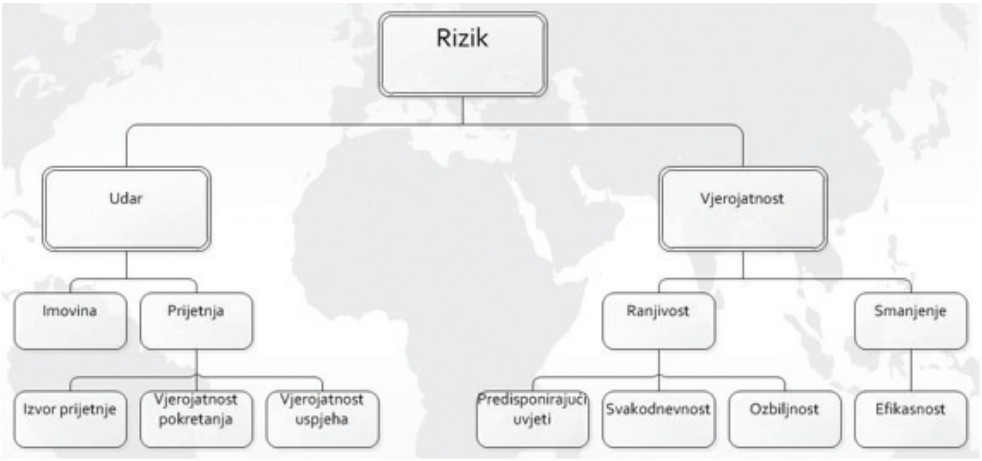
Slika 2 *Proces upravljanja rizikom IT sigurnosti; Izvor: ISO/IEC27005 - Autori*

Figure 2 *IT security risk management process Source: ISO / IEC27005 - Authors*

Dakle, sam broj prijavljenih studenata može dovesti do određenih rizika u poslovanju visokoškolske ustanove.

3. UPRAVLJANJE RIZICIMA
3. RISK MANAGEMENT

Važno je napomenuti da se rizicima, kao i svim ostalim elementima projekta, može ali i mora upravljati, nevezano za njihov pozitivan ili negativan utjecaj. Upravljanje podrazumijeva izradu plana, utvrđivanje i analizu uzroka (kvalitativnu i kvantitativnu), plan reakcije na rizike, nadzor i kontrolu.



Slika 3 *Elementi rizika Izvor: ISACA Atlanta Chapter, Geek Week, August 20, 2013/ Autori*

Figure 3 *Elements of risk Source: ISACA Atlanta Chapter, Geek Week, August 20, 2013 / Authors*

Plan upravljanja rizicima mora biti dio plana upravljanja čitavim projektom. Prilikom izrade plana upravljanja rizicima, moramo uzeti u obzir moguće pretpostavljene postupke vezane uz zakone, pravila i naputke, koji se odnose na naše poslovanje. Na primjer, koristi li se u projektu za neke radne aktivnosti prostor jedne obrazovne institucije (zgrada škole ili fakulteta), u slučaju prirodne nepogode, slijedit će se unaprijed propisana pravila za slučaj kriznih situacija (plan evakuacije i sl.). Dakle, situacije koje predstavljaju moguće rizike, moraju se uključiti u sam projekt na samom početku.

3.1. UTVRĐIVANJE RIZIKA I ODGOVORI NA RIZIKE

3.1. RISK IDENTIFICATION AND RISK RESPONSES

U svim područjima ljudske djelatnosti, u kojima se projekti obavljaju, mogu se pojaviti i rizici, ali nije nužno da se pojave i baš ta nepredvidivost čini ih rizicima. Jer, ukoliko je sigurno da će se određeni događaj i dogoditi i kada bi se imao utjecaj na ciljeve projekta (time i na trošak, vrijeme, resurse i kvalitetu), utoliko to više ne bi bili rizici, već sigurni događaji, uključeni u planiranje te bi postali ograničenje za sam projekt. Rizici koji se pojavljuju u svim projektima, a najčešće su vezani uz sam projektni tim, su tzv. opći rizici. Postoje i popisi vrsta rizika, ali prilikom utvrđivanja rizika u pojedinim projektima, potrebno je koristiti prvenstveno vlastito znanje, iskustvo i poznavanje određenog područja, kao i iskustvo i znanje kolega i članova tima i čitati različitu relevantnu literaturu, izvještaje, propise, zakone ili standarde. Za svaku vrstu rizika potrebno je utvrditi koliko je bitna za sam projekt, a promišljanje o vrstama rizika pomaže osvješćivanju procesa koji se događaju tijekom provedbe projekta kao i onih koji se događaju paralelno s projektom, ali imaju određeni utjecaj na njega. Osvješćivanje mogućih rizika vodi kontroli, boljem planiranju i u konačnici, uspješnijem projektu. Popis rizika može se nadopunjavati novim uočenim rizicima i primjerima te čuvati za korištenje u drugim projektima.

3.2. VRSTE RIZIKA

3.2. TYPES OF RISK

1. **Politički –** promjene koje utječu na projekt
2. **Zakonodavni –** promjena zakona, promjena državne politike i sl.
3. **Tržišni –** konkurencija, promjene u ponudi ili potražnji, trendovi i sl.
4. **Stručni –** nova dostignuća i spoznaje koja su povezana s prirodom svake struke.
5. **Ekonomski –** sposobnost privlačenja i zadržavanja radne snage, utjecaj promjene tečajnih lista na troškove u međunarodnim transakcijama, utjecaj globalne ekonomije na lokalnu.
6. **Socijalno-kulturološki –** demografske promjene, promjene socijalno-ekonomske strukture korisnika.
7. **Zdravlje i sigurnost –** obrazovna ustanova, adekvatna opremljenost, okolina, razina buke, vibracije, azbest, sigurnost hrane, promet, stres.
8. **Tehnološki –** promjene u tehnologiji, zastarjelost tehnologije, nabava optimalne tehnologije.
9. **Ugovorni –** povezani s neizvršenjem ugovornih obaveza dobavljača ili izvođača u dostavi robe ili usluge u dogovoreno vrijeme i unutar dogovorenog troška i specifikacija.
10. **Okoliš –** nedostatak stručnjaka po pitanju zaštite okoliša, standardi koji se mijenjaju, odlaganje otpada, lokalne zajednice.
11. **Fizički –** krađa, vandalizam, palež, oluje, poplave, druge štete vezane uz vremenske (ne) prilike;
12. **Radni –** vezani uz procese u tijeku – promjene u izvođenju nastave (prelazak na smjenski rad i obrnuto), zauzetost nastavnika drugim projektima.
13. **Pravni** – utjecaj promjene zakona i propisa na poslovanje i troškove.
14. **Planiranja** – Rizik da će doći do neuspjeha zbog pogrešaka u fazi planiranja.
15. **Informacijski rizik** – Rizik nedostatka ili nedovoljne kvalitete informacija u početnoj fazi projekta koji kasnije dovodi do problema.

	Primjer 1	Primjer 2	Primjer 3
Opis rizika	Ključni članovi razvojnog tima možda će se razboljeti u najnezgodnije vrijeme	Baza podataka koju ugrađujemo u naš produkt možda neće moći obraditi dovoljan broj transakcija u sekundi.	Financijer projekta možda će imati financijskih problema pa će htjeti smanjiti sredstva za projekt.
Kategorija rizika	vezan uz projekt	vezan uz produkt	poslovni
Vjerojatnost pojavljivanja	velika	umjerena	mala
Učinak rizika	ozbiljan	podnošljiv	katastrofalan
Plan za upravljanje	Reorganiziraj tim tako da ima više preklapanja poslova pa će ljudi lakše moći zamijeniti jedan drugog.	Nabavi odmah bolju bazu podataka za koju je manje vjerojatno da će stvarati probleme.	Napiši unaprijed dokument koji dokazuje da projekt daje važan doprinos poslovnim ciljevima financijera te da bi smanjivanje sredstava donijelo više štete nego koristi.
Strategija plana	minimizacija	izbjegavanje	priprema

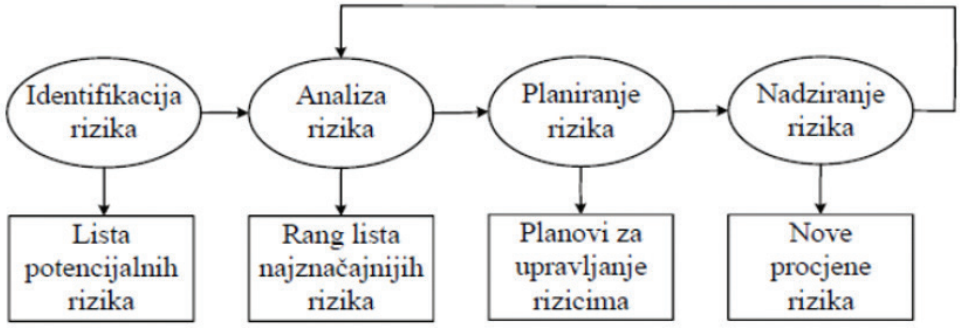
Slika 4 *Upravljanje softverskim rizikom - analiza rizika; Izvor: Projektiranje i oblikovanje IS-a, predavanja TVZ. 2017/2018*
Figure 4 *Software risk management - risk analysis; Source: IS design and design, TVZ lectures. 2017/2018*

Kad se utvrdi koji rizici prijete, za svaki od njih treba odrediti vjerojatnost i utjecaj na posao, vrijeme, resurse, trošak i kvalitetu u projektu [9]. Kao primjer, prikazana je tablica 'Upravljanje softverskim projektom i analiza rizika'.

Kod upravljanja rizicima, poznajemo sljedeće rizike:

1. Projektni rizici koji utječu na projektne resurse ili odvijanje projekta.
2. Produktni rizici. Utjecaj na kvalitetu softvera koji se razvija u sklopu projekta.
3. Poslovni rizici. Organizacija koja odrađuje projekt ili financira.

Na uočene rizike može se odgovarati različitim strategijama. Na rizike koji imaju uglavnom negativan utjecaj, može se odgovarati izbjegavanjem, prebacivanjem ili ublažavanjem: ako se utvrdi da rizik ima preveliki i prevažan negativni utjecaj na sam projekt, može se u potpunosti odustati od aktivnosti koja bi mogla dovesti do rizične situacije, može ga se prebaciti na nekog drugog (npr. na osiguravajuće društvo) ili ga ublažiti na način da se prilikom planiranja aktivnosti predvide veće vremenske rezerve ili izdašniji budžet. Svakako treba uočiti i rizike s pozitivnim utjecajem, jer to su situacije koje je dobro iskoristiti, podijeliti ili proširiti.



Slika 5 *Postupak upravljanja rizikom*
Figure 5 *Risk management process*

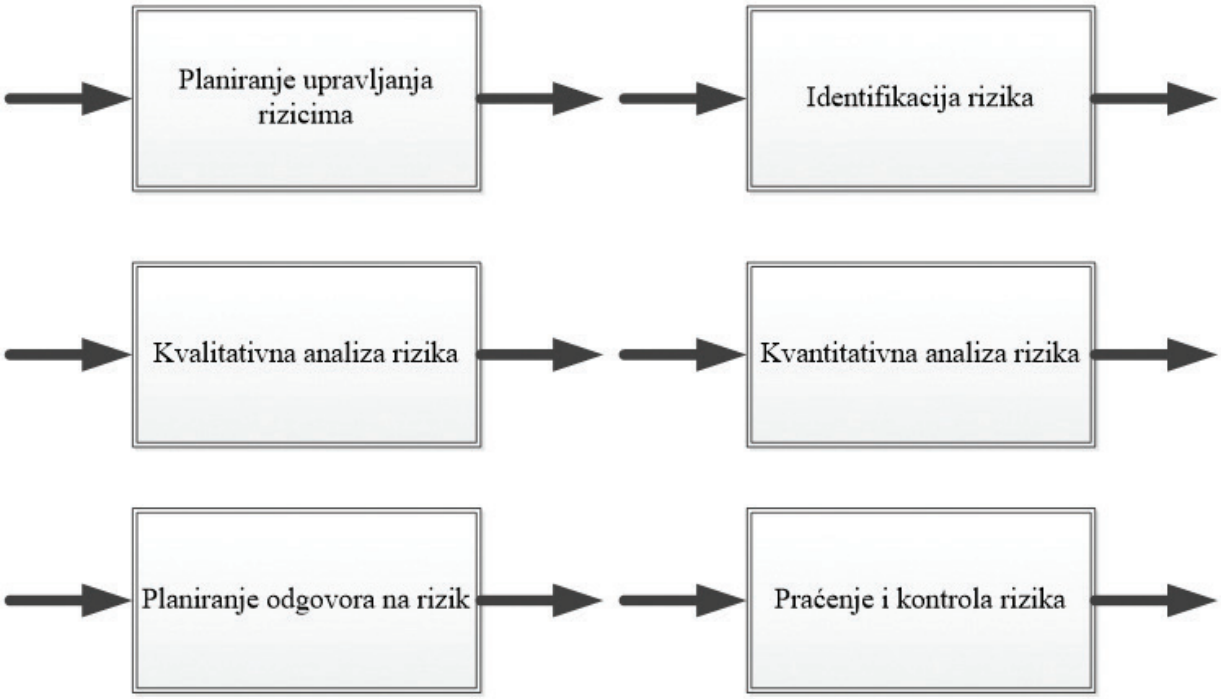
Iz primjera upisa učenika u srednju ili visokoškolsku ustanovu, kao pozitivan rizik može se ukazati situacija da preveliki broj prijavljenih učenika ili studenata može biti prilika za formiranje dodatnog razreda ili grupe i angažiranje novih nastavnika. S vremenom, novoangažirani nastavnici mogli bi se uključiti u razvoj nekih novih programa, dovesti do daljnjeg povećanja dodatnih upisa itd.

3.3. UPRAVLJANJE PROJEKTNIM RIZICIMA PREMA PMI

3.3. PROJECT RISK MANAGEMENT ACCORDING TO PMI

PMBOK (**Project Management Body of Knowledge) je skup standardnih terminologija i smjernica** [2] (PMBOK-2008) je podijelio projektne rizike u 6 procesa. Metodologija sadrži sljedeće pod- procese:

1. **Plan upravljanja rizicima**
    a. Izrađuje se plan upravljanja rizicima, definiraju se načini i mogućnosti koje se poduzimaju radi upravljanja rizicima. Tu su obuhvaćeni načini opisivanja, praćenja, definiranja i praćenja kontrole rizika.
2. **Identifikacija rizika**
    a. U ovom dijelu su obuhvaćeni aktivnosti u vezi pronalaženja i istraživanja mogućih rizika, njihovo definiranje i raspodjela u određene grupe rizika. Identifikacija rizika podrazumijeva i izradu liste mogućih rizika, koje se mogu pojaviti u budućnosti.
3. **Kvalitativna analiza rizika**
    a. Kvalitativna analiza rizika pruža podatke o mogućim vjerojatnostima pojavljivanja rizičnih događaja i njihovom utjecaju na projekt. Kod kvalitativne analize veliku važnost ima stručnost, iskustvo i kvalitativne sposobnosti osoba koje provode procjenu rizika, a naravno, kod ove metode numeričke vrijednosti su relativne, za razliku od kvantitativne metode, gdje su vrijednosti egzaktne. U ovom procesu se koriste određene metode i tehnike, kako bi se mogli identificirati rizični događaji i kakve posljedice mogu imati na ciljeve projekta.
4. **Kvantitativna analiza rizika**
    a. Ova metoda koristi različite kvantitativne metode radi određivanja vjerojatnoće pojavljivanja različitih događaja i utjecaja na projekt i temelji se na korištenju točnih numeričkih vrijednosti. Ova analiza omogućuje formiranje liste prioritetnih rizika.
5. **Planiranje reagiranja na rizike**
    a. U ovom procesu se definiraju akcije i aktivnosti kojima se trebaju izbjeći rizici, smanjuju se mogućnosti koje dovode do rizičnih događaja i reagira se u uvjetima nastanka rizičnih događaja. Planiranje u ovom procesu predstavlja kompleksan i složen proces zbog raznovrsnosti mogućih događaja.
6. **Praćenje i kontrola rizika**
    a. Ovaj proces uključuje aktiviranje odgovora na moguće rizične događaje, također se kontrolira odvijanje rizičnih događaja i reakcije na rizike. Proces treba biti stalan u praćenju i kontroli kroz cijeli životni vijek projekta, zbog mogućnosti nastajanja novih rizika ili nestajanja prethodnih rizika.



Slika 6 *Znanja o upravljanju projektima; Izvor: www.Nutek-us.com*

Figure 6 *Project Management Body of Knowledge; Source: www.Nutek-us.com*

3.4. METODOLOGIJE U PLANIRANJU
3.4. METHODOLOGIES IN PLANNING

Kako su rizici svakodnevna pojava, potrebno je naučiti nositi se s njima, a ne zanemariti mogućnost da se dogodi nešto nepredviđeno. Sposobnost suočavanja s rizicima i prihvaćanje ili pokretanje rizičnijih projekata predstavlja odraz zrelosti voditelja projekta. Primjerice, upuštanje u rizik uvođenja novih tehnologija i metoda u obrazovanju, može dovesti do mnogo novih kreativnih rješenja. Veličina projekta nije proporcionalna jačini rizika pa tako mali projekt može nositi velike rizike ali i veliku motivaciju korisnika i sudionika.

Kod projekta jedino je sigurno da se projekt neće realizirati onako kako je planirano bez obzira koje se metode procjene vremena i troškova koristile. Budući da je cilj dovršiti projekt, koristiti ćemo *CPM (Critical Path Method)* ili metodu kritičnog puta, radi se o grafičkoj metodi temeljenoj na mreži, razvila ju je 1956. tvrtka DuPont. **PERT** *(Project Evaluation and Review Technique)* ili metoda evaluacijske procjene projekata, metoda je mrežnog planiranja, nastala 1957. godine kao rezultat suradnje američke mornarice i tvrtke Booz Allen & Hamilton. [5]

Ove se metodologije najčešće koriste prilikom planiranja projekata kao najpopularniji alati. Problemi kod projektiranja nastaju zbog loših predviđanja, koja su subjektivna i jako neprecizna ili previše optimistična. U literaturi se često postavlja pitanje: Zašto su IT projekti najneuspješniji od svih projekata iako se radi o grani koja se najbrže razvija i napreduje u svim segmentima.

Samo oko 20% svih informacijskih sustava u svijetu pokazuje očekivanu učinkovitost, idućih 40 % pokazuje marginalnu dobit, a preostalih 40% čist je promašaj. O neuspješnim informacijskim sustavima nitko ne piše, tako da se često stvara pogrešan dojam da su svi drugi sustavi uspješni, a samo onaj koji koristite ili mukotrpno razvijate neuspješan. Klasić K., i Klarin K. (2003) [6] *u skripti Informacijski sustavi navode rijetke primjere koji su postali poznati zbog visokih šteta na ljudima i stvarima, kojima su uzrok bili neuspješni sustavi.*

Slijedi par primjera neuspješnosti IS-a iz spomenute skripte:

- ***Ariane 5, let 501** (1996.), koja je eksplodirala prilikom lansiranja radi niza grešaka u softveru. Nesreća je mogla imati više uzroka, od kojih se navode nedovoljno testiran softver, loše održavanje te nedostaci u oblikovanju softvera*
- ***Therac –25**, aparat za zračenje upravljan računalom, kojim je pri terapiji najmanje šest osoba ozračeno previsokim dozama radijacije, a za troje je dokazano da je umrlo od zračenja. Razlog je bio u nedovoljnoj kvaliteti sustava, odnosno neadekvatnom testiranju softvera za određivanje količine zračenja, nedovoljno jasnoj dokumentaciji i uputama za rad, te softverskim greškama u programu koji je trebao osigurati sigurnost pri primjeni stroja.*
- ***Londonski sustav hitne pomoći** (engl. The London Ambulance Service), koji je trebao upravljati prometom ambulantnih vozila na području od preko 600 kvadratnih milja, koji prevozi preko 5000 pacijenata dnevno u 750 vozila. S obzirom da se radi o preko 2000 telefonskih poziva na dan, uključujući više od 1300 hitnih intervencija, odlučeno je uvesti računalom podržan sustav. Autori softvera nisu imali dovoljno iskustva u izradi tako složenog i velikog sustava, pa su napravili čitav niz grešaka u oblikovanju i programiranju sustava, koji se tri tjedna nakon uvođenja raspao. Softver nije bio prilagođen ljudima koji su ga trebali koristiti, tako da se pretpostavlja da su neke osobe umrle jer hitna pomoć nije do njih stigla na vrijeme.*

Činjenica je da softverski projekti imaju mnogo svojih specifičnosti. Kako god, jasno je da problem nije samo loše upravljanje rizicima već upravo ponavljanje istih grešaka u svim područjima upravljanja projektom općenito, koje dovode do već poznatih rizika. Možda su uzroci u velikim količinama informacija, u porastu raznolikosti i složenosti problema koji se nastoje riješiti informatizacijom i osuvremeniti poslovanje.

Tu su i svakodnevni problemi upravljanja organizacijskim sustavima, kao i kriza razvoja programskih proizvoda i informacijskih sustava. Postoji zlatno pravilo, odnosno stara izreka u procesu upravljanja rizicima, a koja glasi: „Prepoznati rizik je napola izbjegnut.“

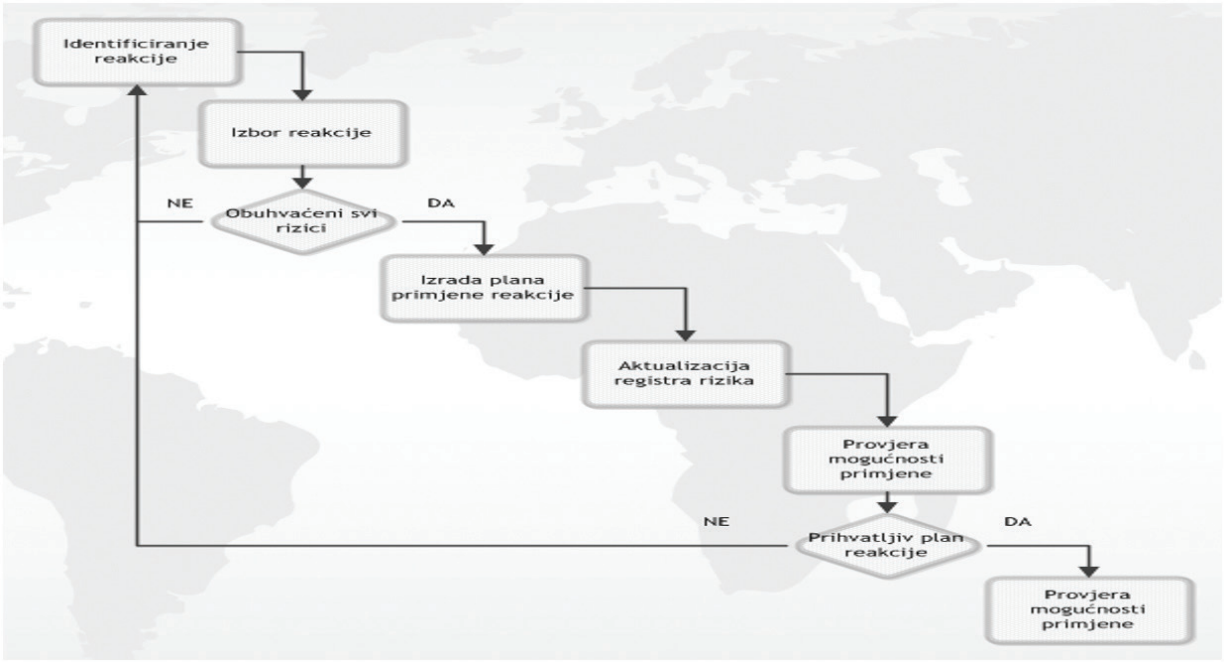
Plan reakcije na rizike dio je ukupnog plana realizacije projekta. U aktivnosti koje provodimo tijekom ostvarivanja projektnih ciljeva treba uključiti i aktivnosti planiranja rizika, koje trebaju biti na istom nivou kao i ostale aktivnosti. Kao posljednji korak, treba biti kontrola primjene reakcija na rizik.

U literaturi se spominje da je osnova za praćenje i kontrolu projektnih rizika, plan upravljanja rizicima. Praćenje i kontrola upravljanja rizicima zasniva se na povratnim informacijama o izvršenim reakcijama na rizike, ponovnoj identifikaciji i procjeni rizika koji su se pojavili, efektivnosti odaziva na te rizike i ažuriranju plana upravljanja rizicima u skladu s tim. [7]

Na stranicama Aperion Univerziteta *se navodi da* praćenje i kontrola rizika na projektu podrazumijeva poduzimanje sljedećih aktivnosti: [7]

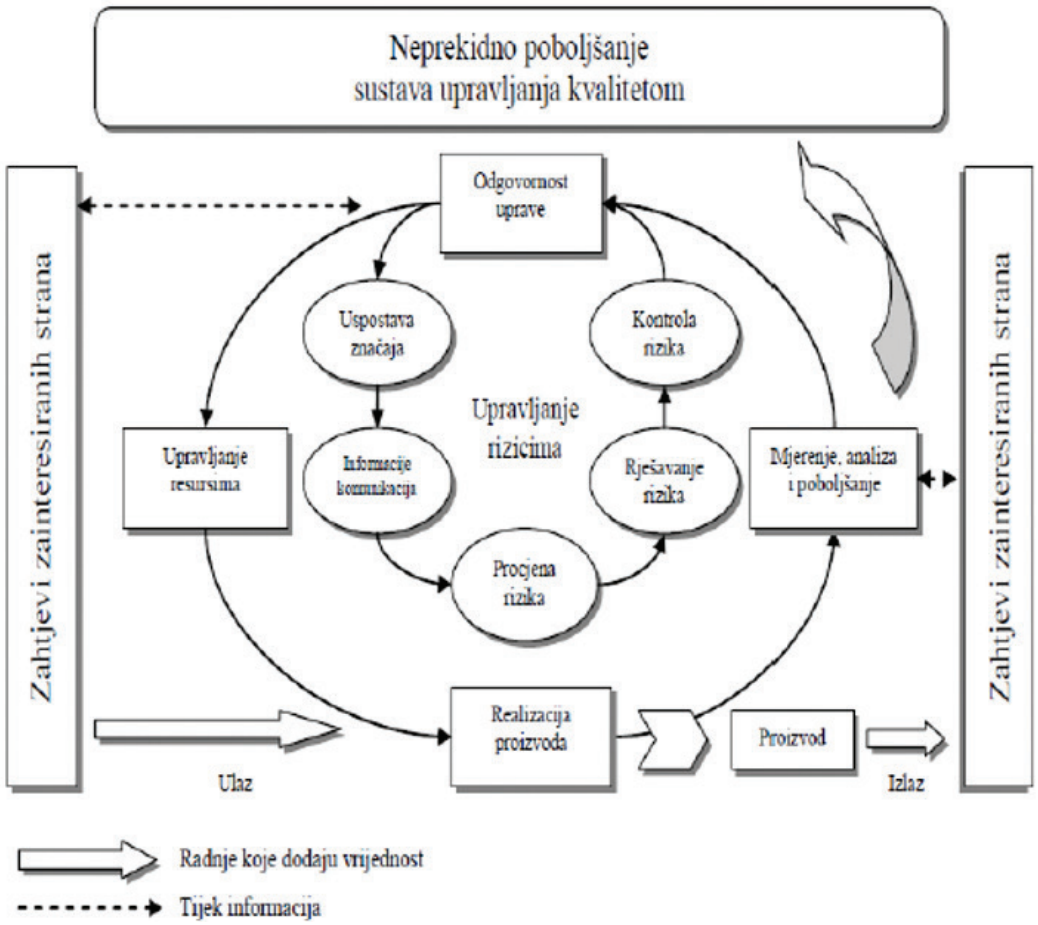
- Provođenje planiranih odgovora na rizike,
- Registriranje promjena u registar rizika,
- Nadzor nad provođenjem aktivnosti koje predstavljaju odgovor na rizike,
- Pravovrjemeno reagiranje na upozorenja,
- Izvještavanje o uspješnim ili neuspješnim upravljačkim aktivnostima,
- Ocjena efektivnosti svih procesa upravljanja projektnim rizicima.

Zbog svega prethodno navedenog, neophodno je postojanje kontinuiranog uvida u odvijanje projekta i da se neprekidno obavljaju potrebna prilagođavanja i promjene u realizaciji reakcija na rizične događaje. To znači da treba postojati organiziran sustav praćenja i kontrole, čiji je zadatak praćenje odvijanja realizacije projekta i permanentno mijenjanje i prilagođavanje planirane akcije i strategije.



Slika 7 *Algoritam planiranja reakcije na rizike (PMI – 2009); Izvor: www.apeiron-uni.eu/Autori*

Figure 7 *Risk response planning algorithm (PMI - 2009); Source: www.apeiron-uni.eu/Autors*



Slika 8 *Sustav upravljanja rizicima i sustav upravljanja kvalitetom (Drljača i Bešker, 2010)*

Figure 8 *Risk management system and quality management system (Drljača and Bešker, 2010)*

4. ISO 9001 I UPRAVLJANJE RIZICIMA
4. ISO 9001 AND RISK MANAGEMENT

Pored zahtjeva za procesnim pristupom, očito je potrebno primijeniti i proces procjene rizika, osobito na tržišne trendove, strateške odrednice, razvojne studije, operativne aktivnosti, zadovoljstvo korisnika proizvodima i uslugama. Kao rezultat ova dva pristupa, organizacija treba posvetiti više pažnje potrebama i očekivanjima kupaca i ostalih zainteresiranih strana. (Drljača i Bešker, 2010).

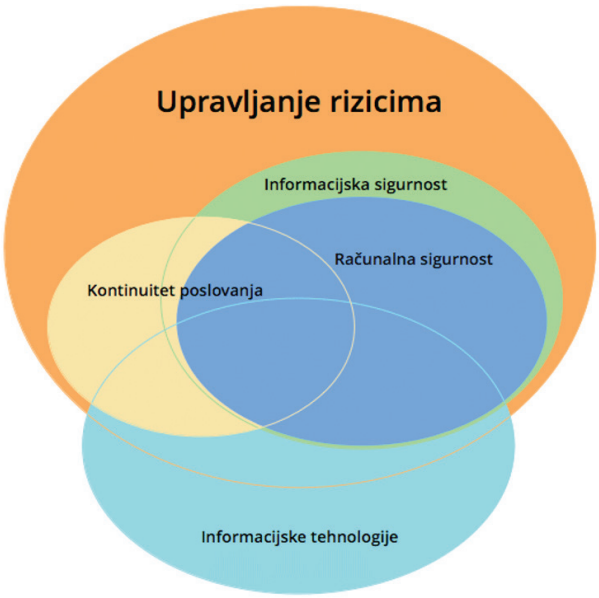
Denis Franković (2014) [8] u svom diplomskom radu navodi sljedeće. Međunarodna norma ISO 9001:2008 ističe da razvoj sustava upravljanja kvalitetom mora uzeti u obzir okruženje u kojem organizacija djeluje, promjene u okruženju, kao i rizike koji su vezani za to okruženje. Istovremeno norma ISO 9001:2008 ne sadrži zahtjeve u odnosu na ostale sustave upravljanja, osobito upravljanja okolišem, zdravljem i sigurnošću, upravljanje financijama ili upravljanje rizicima. Ta norma ne sadrži posebne napomene za upravljanje rizicima (npr. identifikaciju, analizu, ispitivanje, mjere za smanjenje ili eliminaciju rizika, itd.). Ipak, pažljiva analiza norme ISO 9001:2008 pokazuje da postoje odrednice koje se indirektno odnose na neke elemente upravljanja rizicima.

Drugim riječima to znači da čak i stupanj materijalizacije načela upravljanja kvalitetom na razini zahtjeva norme ISO 9001:2008 podrazumijeva utvrđivanje elemenata sustava upravljanja rizicima, što je nužan korak u modeliranju sustava upravljanja rizicima kao strukturnog elementa integriranog sustava upravljanja, jer sustav kvalitete uspostavljen na ovoj razini, doprinosi kvaliteti razvoja TQM-a (eng. Total Quality Management – "Potpuno upravljanje kvalitetom"). (Drljača i Bešker, 2010) Na slici 8. je prikazan odnos sustava upravljanja rizicima i sustava upravljanja kvalitetom. Može se vidjeti kako je upravljanje rizicima dio samog sustava upravljanja kvalitetom te mu ono omogućuje bolje funkcioniranje.

Od važnijih standarda, treba spomenuti i ISO 27001, s obzirom da se navedeni standard može koristiti u svim kompanijama koje koriste informacijske sustave.

Standard obuhvaća sljedeća područja kontrola sigurnosti:

1. Politika sigurnosti
2. Upravljanje imovinom
3. Fizička sigurnost
4. Kontrola pristupa
5. Organizacija informacijske sigurnosti
6. Sigurnost ljudskih resursa
7. Upravljanje komunikacijama
8. Nabava, održavanje i razvoj IS-a
9. Upravljanje sigurnosnim incidentima
10. Upravljanje kontinuitetom poslovanja i
11. Sukladnost.



Slika 9 *Upravljanje rizicima ISO 27001*
Izvor: https://advisera.com/27001academy/hr/sto-je-iso-27001/

Figure 9 *ISO 27001 risk management*
Source: https://advisera.com/27001academy/hr/sto-je-iso-27001/

Ova norma se sastoji od 11 područja, 39 kontrolnih ciljeva i ukupno 133 kontrole. Ova norma pomaže u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima su informacije svakodnevno izložene. Pomaže organizaciji kod osiguranja zaštite svoga informacijskog sustava.

ISO 27001 je međunarodni standard objavljen od strane Međunarodne Organizacije za Standardizacije (ISO) i opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Najnovija verzija ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Prva revizija standarda je objavljena 2005. godine a razvijena je na temelju britanskog standarda BS 7799-2. ISO 27001 je postao najpopularniji standard informacijske sigurnosti u svijetu, te su mnoge kompanije certificirane prema njemu – ovdje možete vidjeti broj certifikata u posljednje dvije godine.

Organizacija ISO objavila je veći broj normi vezanih uz zaštitu i sigurnost informacijskog sustava:

- ISO 27001 (2006) – Sustav upravljanja informatičkom sigurnošću,
- ISO 27002 (2007) – Kodeks postupaka za upravljanje sustava informacijske sigurnosti,
- ISO 27003 – Vodič za uvođenje sustava informacijske sigurnosti,
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti,
- ISO 27005 (2006) – Upravljanje rizicima informacijske sigurnosti,
- ISO 27006 (2007) – Zahtjevi za postupkom analize i certificiranja standarda,
- ISO 27011 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru,
- Itd.

Od gore spomenutih normi, najveću važnost imaju ISO/IEC 27002 i ISO/IEC 27001. Primjena ovih normi osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, kao i povećanje pouzdanosti sustava u slučaju katastrofe te pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja djelatnika vezanim uz informacijsku sigurnost.

Norma ISO/IEC 27001 prihvaćena je kao hrvatska norma HRN ISO/IEC 27001:2006 pod nazivom "Sustavi upravljanja informacijskom sigurnošću – Zahtjevi", a norma ISO/IEC 27002 prihvaćena je kao hrvatska norma HRN ISO/IEC 17799:2006 pod nazivom "Kodeks postupaka za upravljanje informacijskom sigurnošću".

5. ZAKLJUČAK
5. CONCLUSION

U radu su obrađene bitne situacije pri odlučivanju i načinu kako donijeti ispravne odluke i izbjeći rizike u izgradnji projekata iz bilo kojih područja rada. Ukazano je na činjenicu da su rizici svakodnevna pojava u poslovanju i odlučivanju. Svaka odluka koja nije detaljno analizirana i obuhvaćena kontinuiranim praćenjem pojavljivanja mogućih rizika, može dovesti do neuspjeha u planiranju i neefikasnosti u izradi projekta ili poslovanju općenito. Također je ukazano na činjenicu da se rizik pojavljuje ili se može pojaviti na tehničkoj ili organizacijskoj razini. Rizike nije moguće kontrolirati ali njima se može upravljati neprestanim praćenjem događaja i poduzimanjem radnji za smanjenje rizika.

6. REFERENCE
6. REFERENCES

[1.] P. F. Drucker.
[2.] P. M. Institute, A Guide to the Project Managament Body of Knoeledge, Third Edition, Project Managament Institute, 2004.
[3.] V. T. Vaughan E., Osnove osiguranja, upravljanje rizicima, Zagreb: Mate, 1995.
[4.] Spam, »znate-li-uopce-koliko-spam-moze-biti-opasan-za-vasu-tvrtku,« [Mrežno]. Available: https://span.eu/2017/05/znate-li-uopce-koliko-spam-moze-biti-opasan-za-vasu-tvrtku/ .
[5.] S. S. I. L. z. M. K. Kraus C., »Metode i alati projektnog menadžmenta,« [Mrežno]. Available: http://dfest.nsk.hr/wp-content/themes/boilerplate/2015/prezentacije/Kraus_Starcevic-Stancic.pdf. [Pokušaj pristupa 03 07 2018].

[6.] K. K. Klasić K., Projektiranje informacijskih sustava, Split: Sveučilište u Splitu, 2003.

[7.] A. Univerzitet, »Aperion Univerzitet,« [Mrežno]. Available: http://www.apeiron-uni.eu/. [Pokušaj pristupa 23 06 2018].

[8.] F. D., Upravljanje s rizicima i matrica rizika, Varaždin: FOI, 2014.

[9.] J. Gojšić, »Upravljanje projektima,« Incremedia, 2008.

[10.] R. M. Wideman, »Max's project management wisdom,« Max's, [Mrežno]. Available: http://www.maxwideman.com.

[11.] P. o. Hrvatska, »Combined Standard Glossary, verzija 1.1.,« Udruga za projekt menedžment, [Mrežno]. Available: http://pmi.cikac.com/glossary.aspx. [Pokušaj pristupa 3 6 2021].

[12.] D. J., »Upravljanje rizikom i mjerenje izloženosti rizicima,« RRiF, za računovodstvo, poreze i financije, br. 7., 2007.

[13.] Wordpress, »Pogled kroz prozor, Digitalni časopis za obrazovne stručnjake,« Wordpress, 30 4 2009. [Mrežno]. Available: https://pogledkrozprozor.wordpress.com/2009/04/30/upravljanje-projektima-rizici/ . [Pokušaj pristupa 09 02 2021].

[14.] I. International, »Isaca Croatia chapter,« Isaca, [Mrežno]. Available: https://www.isaca.hr/. [Pokušaj pristupa 09 01 2021].

[15.] Mahdi, »Mahdi.hashemitabar,« [Mrežno]. Available: http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27005-2011-english.pdf . [Pokušaj pristupa 20 05 2018].

[16.] Nutek, »Nutek,« Nutek, Inc. Quality Engineering Seminar, Software, and Consulting , [Mrežno]. Available: www.Nutek-us.com . [Pokušaj pristupa 20 05 2018].

[17.] 2. A. Advisera, »Što je ISO 27001,« Advisera, [Mrežno]. Available: https://advisera.com/27001academy/hr/sto-je-iso-27001/. [Pokušaj pristupa 24 06 2018].

AUTORI · *AUTHORS*

● Edmond Krusha
Rođen je 1955. godine., radi u Hrvatskom zavodu za mirovinsko osiguranje kao 'Viši stručni savjetnik specijalist', prije toga obnašao je dužnost 'Načelnika odjela za uredsko poslovanje i pisarnicu'. Diplomirao je na Tehničkom veleučilištu u Zagrebu, smjer informacijske tehnologije, od 2013. u Visokoj školi za informacijske tehnologije radio je kao asistent iz područja tehničkih znanosti, polje računarstvo. Trenutno radi kao predavač u spomenutoj Visokoj školi i nositelj je više kolegija. Nadalje, od 2014. nositelj je više kolegija na Tehničkom veleučilištu u Zagrebu. Također je asistent na RRiF-u, Visokoj školi za financijski menadžment. U nastavnoj djelatnosti autor je i suautor dvadesetak skripti i uputa za vježbe. Suautor je Priručnika 'Programsko inženjerstvo i informacijski sustavi', izdavač TVZ. Organizator je dvaju konferencija o kibernetičkoj sigurnosti u suradnji s Tehničkim veleučilištem u Zagrebu i Zagrebačkim inovacijskim centrom u Zagrebu (ZICER).

Korespondencija · *Correspondence*
e.krusha@gmail.com

● Alan Mahmutović
Rođen 1988. godine, radi na Visokoj školi za informacijske tehnologije (VSITE) kao asistent, prije toga radio u Elektroprojektu na poslovima financijskog planiranja i izvještavanja provedbe projekata energetike, upravljanje vodama i zaštite okoliša. Završava poslijediplomski specijalistički studij Priprema i provedba EU projekata na Sveučilištu u Zagrebu. Diplomirao na Ekonomskom fakultetu u Zagrebu, smjer Menadžerska informatika. Na VSITE-u angažiran na kolegijima Osnove računovodstva i Korištenje računala i programa, funkcijski izvršava poslove Erasmus koordinatora.

Korespondencija · *Correspondence*
al.mahmutovic@gmail.com