Razvoj programskog alata za procjenu rizika

Ivor, Gradiški-Zrinski

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Ivor Gradiški-Zrinski

RAZVOJ PROGRAMSKOG ALATA ZA PROCJENU RIZIKA

DIPLOMSKI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ivor Gradiški-Zrinski

Matični broj: 44056/15–R

Studij: Baze podataka i baze znanja

RAZVOJ PROGRAMSKOG ALATA ZA PROCJENU RIZIKA

DIPLOMSKI RAD

Mentor:

Izv. prof. dr. sc. Sandro Gerić

Varaždin, srpanj 2021.

Ivor Gradiški-Zrinski

Izjava o izvornosti

Izjavljujem da je moj diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Rad se temelji na razradi rizika i metoda za procjenu rizika. Razrađuje se rizik kao pojam i svi tipovi rizika koji mogu postojati. Rad se dotiče pojmova poput magnitude i opisa rizika. Središnji dio rada temelji se na standardima za upravljane rizicima. Pobrojani su i u grubo razrađeni svi poznatiji standardi. Detaljnije je opisan ISO 31000 standard koji pokriva općenitu procjenu rizika. Osim ISO 31000 dotaknuo sam se i ISO 27005 koji se bavi procjenom rizika i procesom upravljanja rizikom u informacijskoj sigurnosti. Alat koji sam kreirao u radu služi za procjenu rizika temeljenu na matricama rizika. Rad završava prikazom funkcioniranja alata koji je izrađen u C# programskom jeziku.

Ključne riječi:

- rizik
- procjena rizika
- vjerojatnost rizika
- ozbiljnost rizika
- matrice rizika
- ISO 31000
- ISO 27005

Sadržaj

1. Uvod

Rizik je pojam koji je zastupljen u životu svakog pojedinca, ali i organizacije. Svaki naš potez ili odluka menadžera u organizaciji za sobom povlače rizik. Svaka osoba nakon što promisli svoje poteze shvati da uvijek postoji vjerojatnost da se nešto loše dogodi, bio to put na posao, hodanje po stepenicama ili vožnja bicikla.

Procjena rizika postoji u gotovo svim granama industrije. Neke od industrija koje će biti obrađene u nastavku ovog rada su kemijska i naftna industrija jer njihovi standardi i sigurnost moraju biti na vrlo visokoj razini. Procjena rizika ne obrađuje samo rizike za koje je potencijalno kriv čovjek nego u obzir uzima prirodne katastrofe i slično.

S ciljem lakše primjene procjene rizika kreirani su razni standardi za upravljanje rizicima. Standardi za upravljanje rizicima počeli su se koristi 1995. godine i do danas se neprestano razvijaju. Vrlo su korisni jer nude mnogo informacija koje olakšavaju implementaciju organizacijama. Postojanje različitih industrija i organizacija dovelo je do postojanja raznih standarda i okvira koji su specijalizirani za određeno područje. U nastavku rada ću se također dotaknuti raznih okvira i standarda koji se danas koriste.

Jedan od glavnih standarda danas je ISO. Vrlo je kvalitetan i ima mnogo implementacija. U radu ću obraditi verziju 31000 koja služi za općenito upravljanje rizikom i verziju 27005 koja je specijalizirana za informacijsku sigurnost.

Procjena rizika ima razne metode koje se koriste. Jedna od njih su matrice rizika. Matrice imaju osi ozbiljnosti i vjerojatnosti na temelju kojih izračunavamo razinu određenog rizika. Matrice su danas vrlo zastupljene u procjeni rizika i ima ih raznih oblika. Osim razrade matrica rizika u posljednjem dijelu rada opisan je postupak izrade alata za procjenu rizika temeljenog na matricama i bit će prikazan način na koji ga je moguće koristiti.

2. Metode i tehnike rada

Odabrana tema nudi mnoštvo informacija i vrlo je široka. Kod kreiranja rada iskoristio sam mnogo vremena za prikupljanje kvalitetne literature i informacija. Nakon inicijalnog prikupljanja literature provjeravao sam kvalitetu informacija. Čitajući literaturu stvarao sam razne bilješke iz kojih sam kreirao inicijalnu strukturu rada. Tijekom teorijske razrade radio sam skice i bilježio ideje za aplikaciju, a za izradu rada koristio sam niže pobrojane alate.

2.1. Visual Studio 2019 IDE + C# programski jezik

Visual Studio je razvojno okruženje razvijeno od strane Microsoft-a. Koristi se za razvoj raznih aplikacija. Za izradu aplikacije korištena je community verzija koja je besplatna. Jezik u kojem je aplikacija izrađena je C#. Visual Studio i C# jako dobro nadopunjuju te je zato on odabran. C# je moderni objektno orijentirani programski jezik. Omogućuje programerima razvoj robusnih i sigurnih aplikacija koje se izvode u .NET virtualnom izvršnom sustavu.

2.2. Overleaf

Overleaf je startup i socijalno poduzeće koje gradi moderne alate za kolaborativno uređivanje tekstualnih radova. Primarni im je proizvod mrežni suradnički urednik teksta u stvarnom vremenu za radove, teze, tehnička izvješća i ostale dokumente napisane na jeziku oznake LaTeX. Overleaf je brzo usvojen u znanosti i istraživanju, a sada podržava zajednicu od preko sedam milijuna autora iz preko 180 zemalja svijeta koji su stvorili preko 45 milijuna dokumenata. [1]

2.3. diagrams.net

Diagrams.net je tehnološki stog otvorenog koda za izgradnju aplikacija za izradu dijagrama i najrašireniji svjetski program za izradu dijagrama temeljen na pregledniku. Ometaju industriju novim poslovnim modelom koji donosi razumnu zaradu, ali ne koristi umjetnu oskudicu za stvaranje napuhnute tvrtke usmjerene na prodaju s odgovarajućim prihodima. Misija tvrtke je pružiti besplatan visokokvalitetan program za izradu dijagrama. [2]

2.4. Github + Sourcetree

GitHub je internet hosting za razvoj softvera i kontrolu verzija pomoću Git-a. Nude distribuiranje kontrole verzija i upravljanje kodom sa svojim dodatnim značajkama. Pruža kontrolu pristupa, suradnju više ljudi i praćenje grešaka. Sourcetree je grafičko sučelje za Git. Kreiran je od strane Atlassiana. Besplatan je, jednostavan za početnike, a moćan za eksperte i nudi jako dobru vizualizaciju koda i ostalih dijelova aplikacija.

3. Definiranje rizika

U ovom poglavlju će se razraditi pojam rizika. Govorit će se o tome što je točno rizik, kako se rizik opisuje i slično. Nakon inicijalnog opisa rizika razrađene su magnitude rizika te su izdvojene neke od važnosti procjene rizika. Poglavlje završava analizom nagrade i rizika.

3.1. Što je rizik?

Rizik je gotovo sveprisutan pojam. Kao takav ima mnogo terminoloških i konceptualnih konotacija, a koristi se u vrlo raznolikim organizacijskim, disciplinskim ili metodološkim postavkama. Definicija iz Oxfordskog rječnika je sljedeća: "Rizik je šansa ili mogućnost opasnosti, gubitka, ozljede ili neke druge štetne posljedice", a definicija rizika je "izložen opasnosti". U tom kontekstu se rizik koristi za označavanje negativnih posljedica. Međutim, preuzimanje rizika također može rezultirati pozitivnim ishodom. Treća mogućnost je veza rizika s nesigurnošću mogućeg ishoda. Institut za upravljanje rizikom definira rizik kao kombinaciju vjerojatnosti događaja i njegovih posljedica. Posljedice pak mogu varirati od pozitivnih pa sve do negativnih. Međunarodni vodič za definicije povezane s rizikom je ISO vodič 73, a rizik definira kao učinak nesigurnosti u ciljevima, no za objasniti ovu definiciju treba posjedovati određenu razinu znanja o upravljanju rizicima.[3]

Tablica 1: Definicije rizika raznih organizacija

Organizacija	Defincija rizika
ISO Guide 73 ISO 31000	Učinak neizvjesnosti na ciljeve. Imajte na umu da učinak može biti pozitivan, negativan ili odstupati od očekivanog. Također, rizik se često opisuje događajem, promjenom okolnosti ili posljedica.
Institute of Risk Management (IRM)	Rizik je kombinacija vjerojatnosti događaja i njegovih posljedica. Posljedice se mogu kretati od pozitivnih do negativnih.

(Izvor: Hopkin, 2010)

Kao primjer rizika izvedenog iz gore navedenih definicija može biti posjedovanje motora. Za većinu ljudi to nudi mogućnost bržeg dolaska od točke A do točke B uz par ostalih beneficija. Naravno da motori mogu sudjelovati u raznim nesrećama te postoje očiti negativni ishodi koji se s motorom mogu dogoditi, a to je zapravo rizik.

3.2. Tipovi rizika

Rizik može imati pozitivne ili negativne ishode no može rezultirati i neizvjesnošću. Iz tog razloga rizici se mogu smatrati povezanima s mogućnošću, gubitkom ili prisutnošću neizvjesnosti za osobu ili organizaciju. Svaki rizik ima svoje osobine koje zahtijevaju određenu analizu

ili upravljanje.[3]

Tipovi rizika koji postoje su:

- opasni ili čisti rizici;
- kontrolni ili neizvjesni rizici;
- oportunitetni ili špekulirani rizici;

Važno je napomenuti da ne postoji prava ili kriva podjela rizika, no ova je vrlo učestala te ću je detaljnije interpretirati. Rizici opasnosti povezani su s izvorima potencijalne štete ili situacija s potencijalnim negativnim potkopavanjem ciljeva. Rizici opasnosti su najčešći rizici povezani s organizacijskim upravljanjem rizicima, uključujući profesionalne programe zaštite na radu. [3]

Kontrolni rizici povezani su s nepoznatim i neočekivanim događajima. Ponekad ih se naziva neizvjesnim rizicima jer ih je izuzetno teško kvantificirati. Takvi rizici često nastaju kod upravljanja projektima jer je u tim okolnostima poznato da će se događaji dogoditi, ali precizne posljedice tih događaja su vrlo teško predvidive te ih je vrlo teško kontrolirati. Pristup otklanjanju takvih rizika se temelji na principu smanjenja mogućih posljedica.[3]

Dva su glavna aspekta povezana s oportunitetnim rizicima. Postoje rizici vezani uz iskorištavanje prilike, ali postoje i rizici vezani uz neiskorištavanje prilike. Ti rizici možda neće biti fizički vidljivi no često su financijske prirode. Iako se rizici od prilika preuzimaju s namjerom da imaju pozitivan ishod, ovo nije zajamčeno.[3]

3.3. Opis rizika

Da bi se rizik u potpunosti razumio, potreban je detaljan opis kako bi se postiglo zajedničko razumijevanje rizika. S ciljem prikupljanja točnog raspona informacija o svakom riziku razlika između rizika opasnosti, kontrole i oportuniteta mora se jasno razumjeti. Jedan od primjera opisa rizika slijedi u nastavku.[3]

- ime ili naslov rizika;
- izjava o riziku, uključujući opseg rizika i detalje mogućih događaja i ovisnosti;
- priroda rizika, uključujući detalje o klasifikaciji rizika i vremenski okvir potencijalnog događaja;
- dionici u riziku, kako unutarnji tako i vanjski;
- stav prema riziku, apetit, tolerancija ili ograničenja za rizik;
- vjerojatnost, veličina i posljedica događaja ako se rizik ostvari;
- kontrolni standard ili ciljana razina rizika;

- incident koji se može dogoditi i gubitak iskustva;
- postojeći kontrolni mehanizmi i aktivnosti za sprječavanje rizika;
- odgovornost za razvoj strategije i politike rizika;
- potencijal za poboljšanje kontrole rizika i razinu povjerenja u postojeće kontrole;
- preporuke za poboljšanje kontrole rizika i rokovi za provedbu;
- odgovornost za provedbu poboljšanja;
- odgovornost za reviziju usklađenosti s rizikom;

Kao primjer za identifikaciju rizika možemo uzeti zaražavanje neke osobe virusom. Virusna infekcija je rizik opasnosti jer od zaražavanja osobe virusom nema nikakve koristi već se samo može prouzročiti šteta. Sprječavanje zaraze virusom može biti cijepljenje. Cijepljenje je pak oportunitetni rizik jer je namjera odabrati što kvalitetnije cjepivo. Kada se osoba jednom cijepi tada nastupaju kontrolni rizici, a mogu se interpretirati u vidu da se osoba nakon cijepljenja može opet zaraziti zbog slabe učinkovitosti cjepiva.[3]

3.4. Magnituda rizika

Učestalost i ozbiljnost rizika najbolje se pokazuju pomoću karte rizika koja se ponekad navodi kao matrica rizika. Mape rizika mogu se izraditi u mnogim formatima. Pretpostavimo da smo identificirali moguće neželjene ishode u organizaciji, a sljedeći korak u procesu je dodjela reda veličine ozbiljnosti svakog neželjenog ishoda. [4]

3.4.1. Magnituda ozbiljnosti rizika

Najjednostavniji način za opisati magnitudu ozbiljnosti rizika je pomoću Richterove skale za potrese. Jačina potresa je određena pomoću logaritama amplitude valova koji se mjere seizmografima. Zbog logaritamske osnove te tablice svaki cijeli porast broja predstavlja desetorostruko povećanje amplitude. Ista vrsta logaritamske tablice će se koristiti ovdje, ali se sastoji od 9 stupnjeva. Skala će izražavati ozbiljnost posljedica raznih neželjenih ishoda. Budući da potres magnitude 7 smatramo kao katastrofalni događaj tako i neki naš događaj koji ima tu magnitudu smatramo katastrofalnim. Tablica u nastavku daje primjer skale za mjerenje težine posljedica neželjenih ishoda povezanih s objektima za rukovanje opasnim materijalima. [4]

3.4.2. Magnituda učestalosti rizika

Učestalost pojave svakog neželjenog ishoda se može smatrati razlikom između opasnosti i rizika. Ishod će imati veći rizik ako je veća učestalost da će se dogoditi ili pak manji rizik ako je manja njegova učestalost. Tablica u nastavku prikazuje magnitude učestalosti rizika. Magnituda je zapravo logaritam broja 10.

Tablica 2: Tablica magnituda ozbiljnosti događaja

Tablica magnituda ozbiljnosti događaja				
Magnituda	Trošak	Učinci na zaposlenika	Učinci na javnost	Učinci na prirodu
7	10000000 USD	Trajni učinci na zdravlje	Trajni učinci na zdravlje	Raširena i dugoročna ili trajna šteta
6	1000000 USD		Višestruke ozljede	Rašireno i kratkoročno ili
5	100000 USD	Teške ozljede	Hospitalizacija	lokalizirano dugoročno zagađenje
4	10000 USD	Bolovanje i mirovanje	Predugo izlaganje	Kratkoročno i lokalizirano zagađenje
3	1000 USD	Medicinska pomoć	Kratko izlaganje	Slabo zagađenje
2	100 USD	Ukazivanje prve pomoći	Buka	Nikakvi učinci

(Izvor: Johnson, 1998)

Tablica 3: Tablica magnituda učestalosti rizika

Magnituda vjerojatnosti rizika		
Magnituda	Broj godišnjih pojava	Opis
+2	100	Dva puta tjedno
+1	10	Jednom mjesečno
0	1	Jednom godišnje
-1	0.1	Jednom u 10 godina
-2	0.01	1% šanse u godini
-3	0.001	Jedva moguće u životnom vijeku organizacije
-4	0.0001	Skoro nemoguće da se dogodi

(Izvor: Johnson, 1998)

3.4.3. Primjena magnituda ozbiljnosti i učestalosti rizika

Korištenje tablica za procjenu magnitude rizika je vrlo jednostavna metoda jer se dobiva zbrajanjem magnitude ozbiljnosti i učestalosti rizika. Tablica u nastavku prikazuje primjere ozbiljnosti i procjene učestalosti za neželjene ishode. Važno je napomenuti da su ovo samo primjeri i ne opisuju realnu situaciju.

Tablica 4: Tablica magnituda rizika

Primjer tablice magnituda rizika				
Opasne stvari: aceton, kopresirani zrak, argon, zapaljive kiseline				
#	Neželjeni ishod	Opasnost	Vjerojatnost	Rizik
1A-1	Požar uzrokovan acetonom	4	-1	3
1A-2	Opekotina uzrokovana dodirom vruće površine	3	-1	2
1A-3	Izlijevanje octene kiseline u količinama za koje je potrebno objaviti izvještaj	2	0	2

(Izvor: Johnson, 1998)

Ovo je bio jedan od načina identifikacije rizika, a nakon toga započinje upravljanje rizikom i svi procesi vezani uz upravljanje rizikom.

3.5. Važnosti rizika i procjene rizika

Nakon događaja u svjetskom financijskom sustavu tijekom 2008. godine, sve organizacije zauzimaju veći interes za rizik i upravljanje rizikom. Sve se više razumijeva da izričito upravljanje rizicima donosi razne benefite. Poduzimanjem proaktivnog pristupa riziku i upravljanju rizicima, organizacije će moći postići poboljšanja u sljedeća tri područja:

- operacije će postati učinkovitije jer će događaji koji mogu uzrokovati poremećaje biti unaprijed identificirani te će se poduzeti radnje s ciljem smanjenja vjerojatnosti da će se taj događaj dogoditi;
- procesi će biti učinkovitiji, jer će se razmotriti odabir procesa i rizika koji su uključeni u dostupne alternative. Također, promjene procesa koje se isporučuju putem projekata biti će učinkovitije i pouzdanije;
- strategija će biti učinkovitija jer se rizici povezani s različitim strateškim ciljevima bolje analiziraju i moguće je donijeti bolje strateške odluke; [3]

Danas više nije prihvatljivo da se organizacije nađu u položaju u kojem neočekivani događaji uzrokuju financijski gubitak, poremećaj u normalnom poslovanju, štetu ugledu i gubitak prisutnosti na tržištu. Dionici sada očekuju da će organizacije u potpunosti uzeti u obzir rizike koji mogu prouzročiti poremećaj u poslovanju, kasnu isporuku projekata ili neuspjeh. [3]

3.6. Rizici i nagrade

Analiza nagrade i rizika vrlo je jednostavan alat koji vam može pomoći da procijenite profil rizika i nagrade. Ovakav alat se može primjeniti na raznim razinama, a neke od njih su :

- primjena od strane izvršnog direktora za usporedbu različitih strateških pravaca za tvrtku;
- razina kada voditelj programa odlučuje koje će projekte zadržati u programu, a koje odbaciti;
- razina kada voditelj projekta odlučuje kako rasporediti zadatke;
- razina kada člana tima odlučuje kako najbolje provesti dan; [5]

U nastavku slijedi predložak za analizu rizika i nagrada koji se sastoji od 4 kategorije :

- niska jednakost- rizik i nagrada su proporcionalno niski;
- visoka jednakost- rizik i nagrada su proporcionalno visoki;
- pozitivno - predstavlja pozitivan omjer rizika i nagrade, gdje se veći povrat može postići s ograničenim rizikom;

- negativno - predstavlja negativnu ravnotežu rizika i nagrade, pri čemu je nizak povrat nagrada za preuzimanje relativno visokog rizika; [5]

Provedba analize rizika i nagrada radi se na način da stvaramo popis različitih opcija i njihovih nagrada. Nakon kreiranja popisa opcija one se ucrtavaju u predložak analize rizika i nagrada. Neke od opcija mogu biti: prijenos poslova na vanjske suradnike, prestanak ulaganja u proizvodne pogone, ulaganje u nove proizvode. Nakon analize može se činiti da neke opcije imaju povoljniji profil nagrađivanja i manji rizik od drugih. Također treba istražiti mogu li se nekim opcijama smanjiti rizici ili eventualno povećati nagrade. U navedenom primjeru, ako bi se rizik od razvoja novih proizvoda nekako mogao ublažiti, ta bi opcija postala povoljnija od prijenosa poslova na vanjske suradnike. Osim kompromisa između dviju opciju treba izbaciti opcije koje donose slabu nagradu, a primjer toga je prestanak proizvodnje proizvoda koji imaju vrlo malu vrijednost za poduzeće. [5]

Slika 1: Primjer analize rizika i nagrada (Izvor: [5])

4. Standardi u upravljanju rizicima

Poglavlje sadrži razradu nekih od standarda za upravljanje rizicima. Bit će govora o opsegu različitih standarda za upravljanje rizicima. Nakon toga slijedi detaljna razrada svakog od okvira za upravljanje rizikom.

4.1. Opseg standarda za upravljanje rizikom

Postoji niz uspostavljenih standarda i okvira za upravljanje rizikom. Prvi takav standard razvilo je organizacijsko tijelo za standarde u Australiji 1995. godine, a nedugo nakon toga slični standardi su razvijeni u Kanadi, Japanu, Velikoj Britaniji i Sjedinjenim Američkim Državama. Pristup kod svih standarda je vrlo sličan te je iz njih nastao standard ISO 31000:2019.[3]

Jednostavno rečeno, standard upravljanja rizikom kombinacija je opisa rizika u procesu upravljanja, zajedno s preporučenim okvirom. Ključne značajke upravljanja rizikom su opisane u tablici koja nudi sažetak standarda u upravljanju rizicima.

Tablica 5: Tablica standarda za upravljanje rizicima

Standard	***Opis***
ISO 31000	Standard objavljen od strane Svjetske organizacije za standarde
BS 31100	Standard objavljen od strane Britanske institucije za standarde
Institute of Risk Management (IRM)	Standard proizveden suradnjom kompanija AIRMIC, Alarm i Instituta za upravljanje rizikom
COSO ERM	Okvir razvijen od strane 5 COSO organizacija
Turnbull Report	Okvir razvijen od strane Financijskog Izvještajnog Vijeća
Orange Book	Standard proizveden od strane Britanske vlade i Ministarstva Financija

(Izvor: Hopkin, 2010)

Jedan od najbolje uspostavljenih i najčešće korištenih standarda upravljanja rizikom je IRM. IRM je standard visokog nivoa usmjeren prema osobama koje nisu nužno stručnjaci u upravljanju rizicima. Australski standard COSO namijenjen je stručnjacima za upravljanje rizikom. Osim ISO i COSO standarda ostali su također u širokoj uporabi. Neke od dostupnih standarda su razvili profesionalci za upravljanje rizikom dok su druge razvili revizori pa čak i računovođe. U nastavku slijede tri glavna pristupa u raznim standardima:

- pristup "upravljanjem rizika" temeljen na ISO 31000, Britanskom BS 3 i IRM standardu;
- pristup "unutarnje kontrole" razvijen od strane COSO okvira i Turnbull izvještaja;
- pristup "kulture svjesne rizika" razvijen od strane Kanadskog instituta za računovođe; [3]

4.2. Opseg okvira za upravljanje rizicima

Kao što je već ranije navedeno postoje mnogi standardi i okviri za upravljanje rizicima. Općenito se priznaje da je standard dokument koji daje informacije o procesu upravljanja rizikom i okviru za upravljanje rizikom. Unutar mnogih standarda upravljanja rizikom, aktivnosti upravljanja rizikom trebaju se odvijati unutar poslovnog konteksta organizacije i rizika s kojima se organizacija može susresti. Da bi se kontekst mogao opisati potreban nam je određeni okvir koji nudi podršku u tom procesu. Jedan od takvih okvira je ISO 31000. On stavlja poseban naglasak na kontekst i navodi da se razmatranje mora vršiti na vanjskom i unutarnjem kontekstu. Osim razmatranja unutarnjeg i vanjskog konteksta potrebno je uzeti u obzir kontekst upravljanja rizicima.

Svi uspostavljeni standardi upravljanja rizicima odnose se na okvire za upravljanje rizicima, iako se to predstavlja na različite načine. Kako bi se pružilo jednostavno objašnjenje opsega okvira za upravljanje rizicima razvijena je kratica Risk Arhitecture, Structure and Protocols (RASP).[3]

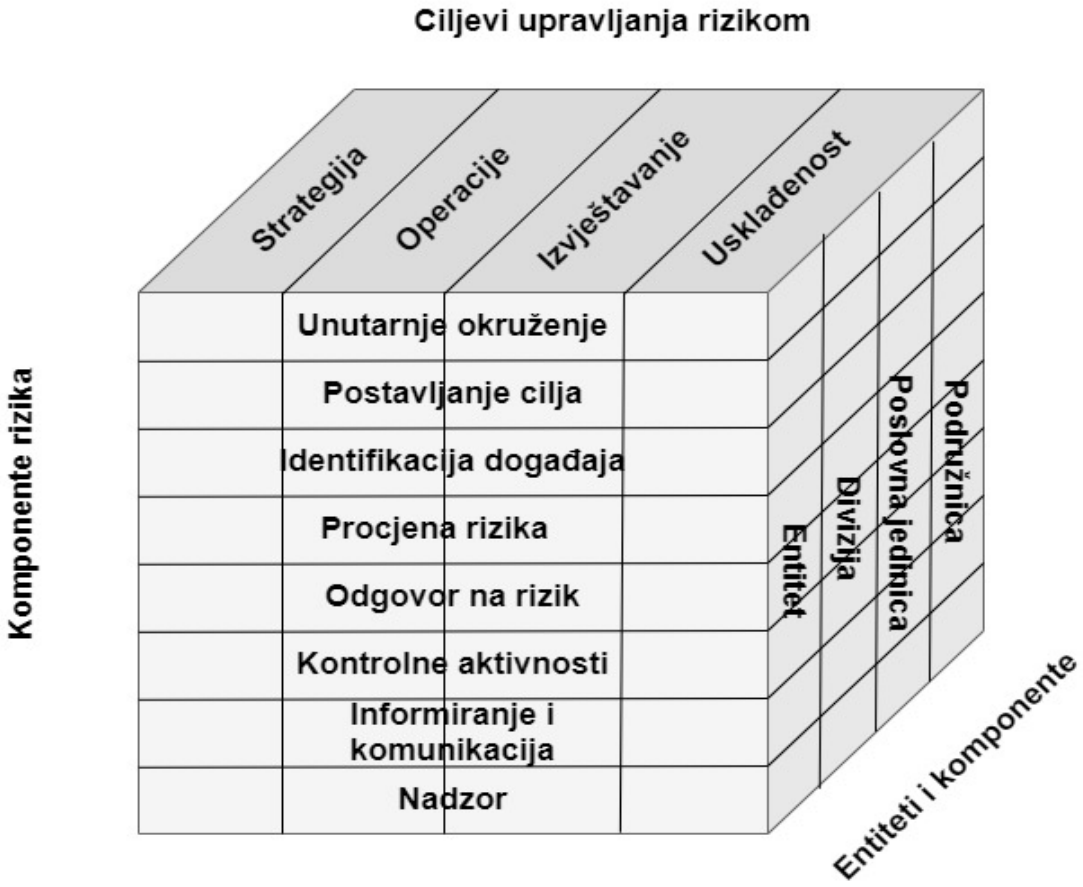
Slika 2: RASP (Izvor: [6])

4.3. COSO ERM okvir

S ciljem razumijevanja nastanka ovog standarda interne kontrole potrebno se vratiti u 1970. godine. U tom periodu nastalo je mnogo velikih organizacijskih neuspjeha te je bila potrebna neka promjena, a upravo ju je taj okvir nudio. Interna ili unutarnja kontrola se kao izraz koristi već mnogo godina, a jedna od njenih pravih definicija je: Unutarnja kontrola je proces koji utječe na upravni odbor, upravu, entitete i drugo osoblje, osmišljen da pruži razumno jamstvo u vezi postizanja ciljeva u sljedećim kategorijama:

- učinkovitost operacija;
- pouzdanost financijskog izvještavanja;
- pridržavanje važećih zakona i propisa; [7]

COSO okvir je učinio vrlo dobar posao u opisivanju i definiranju interne kontrole i postao je svjetski model. Okvir COSO ERM prikazan je na slici u nastavku:



Slika 3: COSO okvir (Izvor: [7])

Na slici vidimo 4 okomita stupca koji prikazuju strateške ciljeve poduzeća. U vodoravnom položaju vidimo 8 komponenti rizika, dok su s desne strane entiteti i komponente organizacija. Sada slijedi detaljniji opis svih osam komponenti rizika:

- unutarnje okruženje - obuhvaća ton organizacije i postavlja osnovu načina na koji se rizik promatra i rješava;
- postavljanje cilja - ciljevi moraju postojati prije nego što uprava može prepoznati potencijalni događaj koji može utjecati na njihova postignuća;
- identifikacija događaja - unutarnji i vanjski događaji koji utječu na postizanje ciljeva moraju se utvrditi jesu li rizici ili prilike;
- procjena rizika - analiza rizika uzima u obzir vjerojatnost i utjecaj rizika kao osnovu za određivanje načina na koji se njima treba upravljati;
- odgovor na rizik- odabir načina upravljanja određenim rizikom;
- kontrolne aktivnosti- uspostavljaju se i provode politike i postupci kojima je cilj osigurati učinkovito provođenje odgovora na rizik;
- informiranje i komunikacija - analiziraju se relevantne informacije i potiče se komunikacija između ljudi s ciljem ispunjenja svih njihovih obaveza;
- Nadzor - cjelokupno upravljanje rizikom poduzeća prati se i modificira prema potrebi. [7]

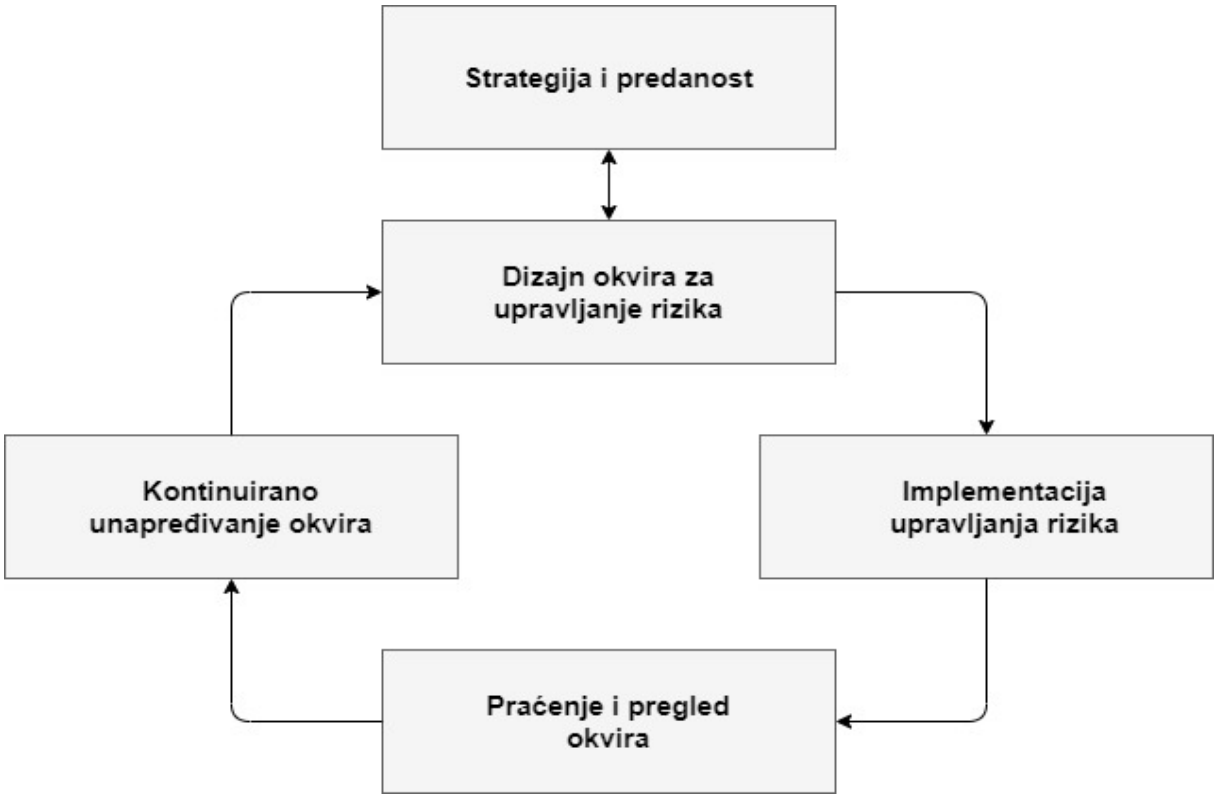
4.4. Britanski standard BS 31100

Britanski standard BS 31100 opisuje okvir upravljanja rizikom kao skup komponenti koje pružaju temelje i organizacijske aranžmane za dizajniranje, provedbu, nadzor, pregled i kontinuirano poboljšavanje procesa upravljanja rizicima u cijeloj organizaciji.[8]

BS 31100 također nastoji riješiti rizike prije nego što se oni uopće pojave po principu traženja rizika. Britanski standard objašnjava da rizici s potencijalno poželjnim posljedicama mogu učiniti aktivnost privlačnijom i navesti organizaciju na traženje te aktivnosti, baš kao što rizici s neželjenim potencijalnim posljedicama mogu motivirati izbjegavanje. Pojašnjenje komponenti od kojih je okvir sastavljen slijedi u nastavku:

- strategija i predanost - odbor ili neko drugo upravljačko tijelo bi trebalo zahtijevati razvoj politika upravljanja rizicima i nuditi politiku podrške upravljanju rizicima;
- dizajn okvira za upravljanje rizika - organizacija treba steći razumijevanje vanjskog i unutarnjeg konteksta upravljanja rizikom i imati za cilj oblikovanje upravljanja rizikom;
- implementacija upravljanja rizika - priprema i provedba plana za upravljanje rizikom;
- praćenje i pregled okvira - cilj je identificirati gdje postoje slučajevi upravljanja rizikom koji trenutno nisu u skladu s okvirom;

- kontinuirano unapređivanje okvira - organizacija mora nastaviti poboljšavati svoj okvir za upravljanje rizikom; [8]



Slika 4: Komponente okvira BS 31100 (Izvor: [8])

4.5. Standard za upravljanje rizikom (engl. *A Risk Management Standard - ARMS*)

Standard za upravljanje rizikom je rezultat rada tima izvučenog iz glavne organizacije za upravljanje rizikom u Ujedinjenom Kraljevstvu, uključujući Institut za upravljanje rizikom (engl. *Institute of Risk management- IRM*). Osim toga, tim je tražio stavove i mišljenja širokog spektra drugih profesionalnih tijela s interesima u polju rizika tijekom dugog razdoblja. Standard koristi terminologiju rizika definiranu od strane ISO. [9]

4.6. Turnbull Report

Objavljen je od strane Radne skupine za unutarnju kontrolu Instituta ovlaštenih računovođa u Engleskoj i Walesu 1999.godine. Izvještaj primarno nudi implementaciju smjernica za unutarnju kontrolu, unutarnju reviziju i upravljanje rizikom. Uspješna implementacija smjernica pripomogla je kod kreiranja novih standarda u britanskom korporativnom upravljanju. [10]

4.7. Orange Book

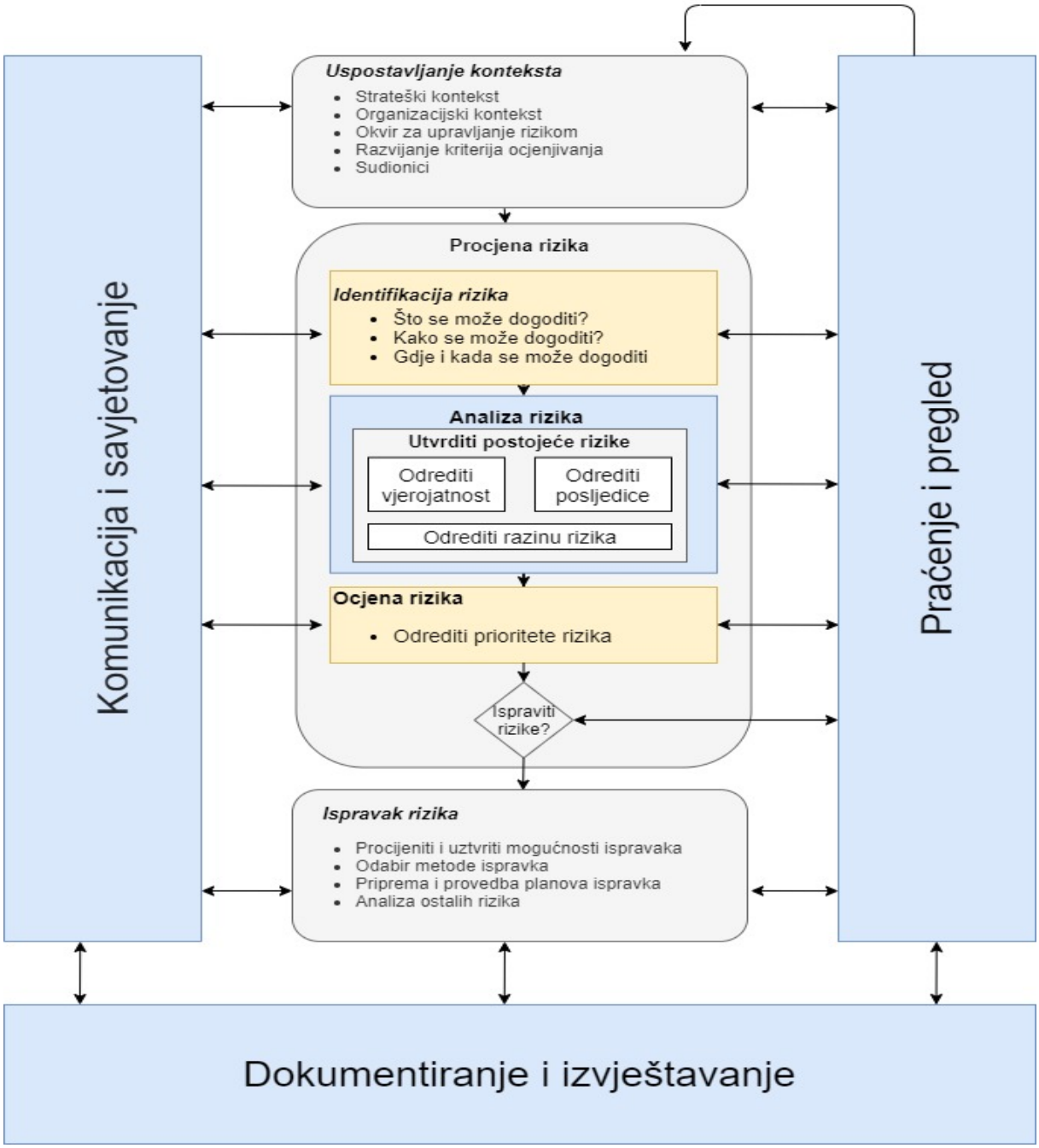
Dokument je kreiran od strane britanske vlade. Iznosi glavne principe na kojima se temelji učinkovito upravljanje rizicima u svim vladinim odjelima. Ovaj dokument je namijenjen svima uključenim u dizajn, rad i isporuku učinkovitih javnih usluga. Njegova primarna publika će vjerojatno biti:

- članovi odbora za reviziju i osiguranje rizika;
- osobe koje se bave rizikom;
- članovi odbora u organizacijama; [11]

Ovaj dokument ne utvrđuje postupak kojim bi organizacija trebala raditi kod upravljanja rizicima nego postavlja načela i definira pristup koji pruža fleksibilnost u dizajniranju i provedbi upravljanja rizikom. Taj pristup upravljanju rizicima mora odgovarati svima jer su javne organizacije različitih veličina, različito strukturirane i imaju različite potrebe. [11]

5. Procjena rizika i proces upravljanja rizikom prema ISO 31000

U poglavlju slijedi jednostavan prikaz postupka upravljanja rizikom prikazan na slici ispod. Od njega se sastoje svi utvrđeni standardi za upravljanje rizikom. Nakon slike nastavlja se s dijelovima procesa upravljanja te će svaki dio biti detaljno opisan u nastavku.



Slika 5: Proces upravljanja rizikom (Izvor: [12])

5.1. Općenito o procesu upravljanja rizikom

Proces upravljanja rizicima uključuje sustavnu primjenu politika, postupaka i raznih praksi na aktivnosti komuniciranja i savjetovanja, uspostavljanja konteksta i procjene, liječenja, praćenja, pregleda, bilježenja i izvještavanja o riziku. Proces upravljanja rizicima trebao bi biti sastavni dio upravljanja i donošenja odluka. Osim toga mora biti integriran u strukturu, operacije i procese organizacije. Može se primijeniti na strateškoj, operativnoj, programskoj ili projektnoj razini. U organizaciji može postojati mnogo aplikacija procesa upravljanja rizikom, prilagođenih postizanju ciljeva i prilagođavanju vanjskom i unutarnjem kontekstu u kojem se primjenjuju. Dinamičnu i promjenjivu prirodu ljudskog ponašanja i kulture treba uzimati u obzir tijekom cijelog postupka upravljanja rizicima. Iako se postupak upravljanja rizikom često predstavlja kao sekvencijalni, u praksi je najčešće iterativni.[13]

Također ovaj proces obuhvaća ključne elemente procesa upravljanja rizicima koji su:

- uspostavljanje konteksta;
- komunikacija i savjetovanje;
- procjena rizika;
- ispravak rizika;
- nadzor i pregled; [13]

5.2. Komunikacija i savjetovanje

Svrha komunikacije i savjetovanja je pomoći relevantnim dionicima u razumijevanju rizika, osnovi na kojoj se donose odluke i razlozima zbog kojih su potrebne određene radnje. Komunikacija nastoji promicati svijest i razumijevanje rizika, dok savjetovanje uključuje dobivanje povratnih informacija i informacija koje podržavaju donošenje odluka. Uska koordinacija između njih dvoje trebala bi olakšati činjeničnu, pravodobnu, relevantnu, točnu i razumljivu razmjenu informacija, uzimajući u obzir povjerljivost i integritet informacija, kao i prava na privatnost pojedinaca. Komunikacija i savjetovanje s odgovarajućim vanjskim i unutarnjim dionicima se treba odvijati unutar i tijekom svih koraka procesa upravljanja rizicima. [13]

Uspješna procjena rizika ovisi o učinkovitoj komunikaciji i savjetovanju s sudionicima. Uključivanje dionika u proces upravljanja rizicima pomoći će u:

- izradi komunikacijskog plana;
- definiranju konteksta;
- objedinjavanju različitih područja stručnosti za prepoznavanje i analizu rizika;
- osiguranju da se različita gledišta prikladno uzimaju u obzir pri procjeni rizika;

- osiguranju adekvatne identifikacije rizika;
- osiguranju odobrenja i podrške kod ispravka rizika;

Dionici bi trebali pridonijeti povezivanju postupka procjene rizika s drugima disciplinama upravljanja, uključujući upravljanje promjenama, upravljanje projektima i financijsko upravljanje.[13]

5.3. Uspostavljanje konteksta

Svrha uspostavljanja opsega, konteksta i kriterija je prilagodba postupka upravljanja rizikom, omogućujući učinkovitu procjenu rizika i odgovarajući tretman rizika. Opseg, kontekst i kriteriji uključuju definiranje opsega procesa i razumijevanje vanjskog i unutarnjeg konteksta.[13]

5.3.1. Utvrđivanje konteksta

Organizacija bi trebala definirati opseg svojih aktivnosti upravljanja rizikom. Budući da se postupak upravljanja rizikom može primijeniti na različitim razinama (npr. strateška, operativna, programska, projektna ili druge aktivnosti), važno je biti jasan o opsegu koji se razmatra, relevantnim ciljevima koje treba razmotriti i njihovom usklađivanju s organizacijskim ciljevima. Pri planiranju treba uključiti sljedeće stvari:

- ciljeve i odluke koje treba donijeti;
- ishode koje očekujemo od koraka poduzetih u procesu;
- odgovarajuće alate i tehnike procjene rizika;
- potrebne resurse, odgovornosti i evidencije koje treba voditi;
- odnose s drugim projektima, procesima i aktivnostima; [13]

5.3.2. Vanjski i unutarnji kontekst

Vanjski i unutarnji kontekst je okruženje u kojem organizacija nastoji definirati i postići svoje ciljeve. Kontekst procesa upravljanja rizicima trebao bi se uspostaviti iz razumijevanja vanjskog i unutarnjeg okruženja u kojem organizacija djeluje i trebao bi odražavati specifično okruženje aktivnosti na koje se postupak upravljanja rizikom treba primijeniti. [13]

Utvrđivanje i razumijevanje konteksta važno je jer:

- se upravljanje rizikom odvija u kontekstu ciljeva i aktivnosti organizacije;
- organizacijski čimbenici mogu biti izvor rizika;
- se svrha i opseg postupka upravljanja rizikom mogu međusobno povezati s ciljevima organizacije u cjelini. [13]

5.3.3. Utvrđivanje kriterija rizika

Organizacija treba odrediti iznos i vrstu rizika koji se može ili ne mora utvrditi u odnosu na ciljeve. Također bi se trebali definirati kriteriji za procjenu značaja rizika i potporu procesima donošenja odluka. Kriteriji rizika trebaju se uskladiti s okvirom upravljanja rizicima i prilagoditi specifičnoj svrsi i opsegu aktivnosti koja se razmatra. Kriteriji rizika trebali bi odražavati vrijednosti, ciljeve i resurse organizacije te biti u skladu s politikama i izjavama o upravljanju rizicima. Kriteriji bi se trebali definirati uzimajući u obzir obveze organizacije i stavove dionika. [13]

Iako bi se kriteriji rizika trebali uspostaviti na početku postupka procjene rizika, oni su dinamični i po potrebi ih treba neprestano pregledavati i mijenjati. Da bi se postavili kriteriji rizika, treba uzeti u obzir sljedeće:

- prirodu i vrstu neizvjesnosti koje mogu utjecati na ishode i ciljeve (materijalne i nematerijalne);
- kako će se definirati i mjeriti posljedice (pozitivne i negativne) te vjerojatnost;
- dosljednost u mjerenju;
- način utvrđivanja razine rizika;
- kako će se uzeti i obraditi kombinacije i sljedovi višestrukih rizika;
- sposobnost organizacije;
- čimbenike povezane s vremenom; [13]

5.4. Procjena rizika

Procjena rizika je cjelokupni postupak utvrđivanja rizika, analize rizika i procjene rizika. Procjenu rizika treba provoditi sustavno, iterativno i u suradnji, oslanjajući se na znanje i stavove dionika. Treba koristiti najbolje dostupne informacije, po potrebi nadopunjene daljnjim ispitivanjem.

5.4.1. Identifikacija rizika

Svrha identifikacije rizika je pronaći, prepoznati i opisati rizike koji bi mogli pomoći ili spriječiti organizaciju da postigne svoje ciljeve. Relevantne, prikladne i ažurne informacije od velike su važnosti za prepoznavanje rizika. Organizacija može koristiti niz tehnika za utvrđivanje nesigurnosti koje mogu utjecati na jedan ili više ciljeva. Treba uzeti u obzir sljedeće čimbenike:

- uzroke i događaje;
- prijetnje i mogućnosti;
- ranjivosti;

- promjene u vanjskom i unutarnjem kontekstu;
- pokazatelje novih rizika;
- prirodu i vrijednost imovine i resursa;
- posljedice i njihov utjecaj na ciljeve;
- ograničenja znanja i pouzdanosti informacija;
- čimbenike povezane s vremenom;
- pristranosti, pretpostavke i uvjerenja uključenih; [13]

Organizacija bi trebala identificirati rizike, bez obzira jesu li njihovi izvori pod njezinom kontrolom ili ne. Treba razmotriti da može postojati više vrsta ishoda, što može rezultirati raznim opipljivim ili nematerijalnim posljedicama. [13]

5.4.2. Analiza rizika

Svrha analize rizika je shvatiti prirodu rizika i njegove karakteristike, uključujući prema potrebi razinu rizika. Analiza rizika uključuje detaljno razmatranje neizvjesnosti, izvora rizika, posljedica, vjerojatnosti, događaja, scenarija, kontrola i njihove učinkovitosti. Događaj može imati više uzroka i posljedica te može utjecati na više ciljeva. Analiza rizika može se izvoditi s različitim stupnjevima detalja i složenosti, ovisno o svrsi analize, dostupnosti i pouzdanosti informacija i raspoloživosti resursa. Tehnike analize mogu biti kvalitativne, kvantitativne ili kombinacija istih, ovisno o okolnostima i namjeni. Analiza rizika treba uzeti u obzir sljedeće čimbenike:

- vjerojatnost događaja i posljedica;
- prirodu i veličinu posljedica;
- složenost i povezanost posljedica;
- vremenski povezane čimbenike i volatilnost;
- učinkovitost postojećih kontrola;
- razinu osjetljivosti i pouzdanosti. [13]

Na analizu rizika može utjecati svako razilaženje mišljenja, pristranosti, percepcije rizika i prosudbi. Dodatni utjecaji su kvaliteta korištenih informacija, pretpostavke i izuzeća, sva ograničenja tehnika i načina na koji se izvršavaju. Te utjecaje treba razmotriti, dokumentirati i priopćiti donositeljima odluka. Jako neizvjesne događaje može biti teško kvantificirati. To može predstavljati problem prilikom analize događaja s teškim posljedicama. U takvim slučajevima upotreba kombinacije tehnika obično daje bolji uvid. Analiza rizika daje ulaz u procjenu rizika, odluke o tome treba li rizik tretirati i kako, te daje informacije o najprikladnijoj strategiji i metodama liječenja rizika. Rezultati pružaju uvid u odluke i opcije koje uključuju različite vrste i razine rizika. [13]

5.4.3. Ocjenjivanje rizika

Svrha ocjenjivanja rizika je podržati odluke. Ocjenjivanje rizika uključuje usporedbu rezultata analize rizika s utvrđenim kriterijima rizika kako bi se utvrdilo gdje su potrebne dodatne radnje. To može dovesti do odluke da se:

- ništa ne poduzima;
- razmotri mogućnost liječenja rizika;
- poduzme daljnja analiza s ciljem boljeg razumijevanja rizika;
- održavaju postojeće kontrole;
- preispitaju ciljevi; [13]

Odluke bi trebale uzeti u obzir širi kontekst te stvarne i uočene posljedice za vanjske i unutarnje dionike. Ishod procjene rizika treba zabilježiti, priopćiti, a zatim i potvrditi na odgovarajućim razinama organizacije. [13]

5.5. Liječenje rizika

Svrha liječenja rizika je odabrati i primijeniti mogućnosti za rješavanje rizika. Liječenje rizika je iterativni postupak koji uključuje:

- formuliranje i odabir mogućnosti liječenja rizika;
- planiranje i provođenje liječenja rizika;
- procjene učinkovitosti tog liječenja;
- odlučivanje je li preostali rizik prihvatljiv;
- poduzimanje daljnjeg liječenja, ako rizik nije prihvatljivo izliječen; [13]

5.5.1. Izbor mogućnosti liječenja rizika

Odabir najprikladnijih opcija liječenja rizika uključuje balansiranje potencijalnih koristi ostvarenih u vezi s postizanjem ciljeva naspram troškova, napora ili nedostataka provedbe. Opcije liječenja rizika nisu nužno međusobno isključive ili prikladne u svim okolnostima. Opcije za liječenje rizika mogu uključivati jedno od sljedećih:

- izbjegavanje rizika odlukom da se ne započne ili nastavi s aktivnošću koja dovodi do rizika;
- preuzimanje ili povećanje rizika kako bi se iskoristila prilika;
- uklanjanje izvora rizika;

- promjena vjerojatnosti;
- promjena posljedica;
- dijeljenje rizika (npr. putem ugovora, kupnje osiguranja);
- zadržavanje rizika informiranom odlukom; [13]

Opravdanje za liječenje rizika šire je od isključivo ekonomskih razloga i trebalo bi uzeti u obzir sve obveze organizacije, dobrovoljne obveze i stavove dionika. Odabir mogućnosti liječenja rizika trebao bi se izvršiti u skladu s ciljevima organizacije, kriterijima rizika i raspoloživim resursima. [13]

Pri odabiru mogućnosti liječenja rizika, organizacija bi trebala razmotriti vrijednosti, percepcije i potencijalno sudjelovanje dionika te najprikladnije načine komuniciranja i savjetovanja s njima. Iako su podjednako učinkoviti, neki tretmani rizika mogu biti prihvatljiviji za neke dionike nego za druge. Liječenje rizika, čak i ako se pažljivo osmisli i primijeni, možda neće donijeti očekivane ishode i može proizvesti neželjene posljedice. Praćenje i preispitivanje moraju biti sastavni dio provedbe liječenja rizika kako bi se osiguralo da različiti oblici liječenja postaju i ostaju učinkoviti. Liječenje rizika također može uvesti nove rizike kojima treba upravljati. Ako ne postoje dostupne mogućnosti liječenja ili ako mogućnosti liječenja ne mijenjaju dovoljno rizik, rizik treba evidentirati i održavati u tijeku pregleda. [13]

Donositelji odluka i drugi dionici trebali bi biti svjesni prirode i opsega preostalog rizika nakon tretmana rizika. Preostali rizik treba dokumentirati i podvrgnuti praćenju, pregledu i prema potrebi, daljnjem liječenju. [13]

5.5.2. Priprema i provedba planova liječenja rizika

Svrha planova liječenja rizika je odrediti kako će se provesti odabrane mogućnosti liječenja, tako da uključeni razumiju dogovore i da se može pratiti napredak u odnosu na plan. Plan liječenja trebao bi jasno odrediti redoslijed kojim se treba provoditi liječenje rizika. Planove liječenja treba integrirati u planove upravljanja i procese organizacije, uz savjetovanje s odgovarajućim dionicima. Podaci navedeni u planu liječenja trebaju sadržavati:

- obrazloženje za odabir mogućnosti liječenja, uključujući očekivane koristi;
- one koji su odgovorni za odobravanje i provedbu plana;
- predložene akcije;
- potrebne resurse, uključujući nepredviđene slučajeve;
- mjere učinka;
- ograničenja;
- potrebno izvještavanje i praćenje;
- vrijeme kada se očekuje da će se poduzeti i dovršiti radnje; [13]

5.6. Nadzor i pregled

Svrha praćenja i pregleda je osigurati te poboljšati kvalitetu i djelotvornost dizajna, provedbe i ishoda procesa. Stalno praćenje, povremeni pregled procesa upravljanja rizikom i njegovih ishoda trebali bi biti planirani dio procesa upravljanja rizikom, s jasno definiranim odgovornostima. Nadzor i pregled trebali bi se odvijati u svim fazama procesa. Praćenje i pregled uključuje planiranje, prikupljanje i analizu podataka, bilježenje rezultata i pružanje povratnih informacija. Rezultati praćenja i pregleda trebali bi biti uključeni u aktivnosti upravljanja učinkom mjerenja i izvještavanja organizacije. [13]

Kao dio procesa upravljanja rizicima, rizici i kontrole trebaju se nadzirati i pregledavati, a redovito treba provjeravati sljedeće stvari:

- ostaju li pretpostavke o rizicima valjane?;
- postižu li se očekivani rezultati?;
- jesu li rezultati u skladu sa stvarnim iskustvom?;
- jesu li tretmani ispravka rizika učinkoviti?; [13]

5.7. Dokumentiranje i izvještavanje

Proces upravljanja rizikom i njegovi ishodi trebali bi se dokumentirati i izvještavati putem odgovarajućih mehanizama. Dokumentiranje i izvještavanje ima za cilj:

- izvijestiti o aktivnostima i ishodima upravljanja rizikom u cijeloj organizaciji;
- pružiti informacije za donošenje odluka;
- poboljšati aktivnosti upravljanja rizikom;
- pomoći u interakciji s dionicima, uključujući one koji su odgovorni za aktivnosti upravljanja rizikom; [13]

Odluke o stvaranju, zadržavanju i rukovanju dokumentiranim informacijama trebale bi se uzeti u obzir, ali bez ograničavanja na: njihovu upotrebu, osjetljivost informacija te vanjski i unutarnji kontekst. Izvještavanje je sastavni dio upravljanja organizacijom i trebalo bi poboljšati kvalitetu dijaloga sa dionicima i podržati najviše rukovodstvo i nadzorna tijela u ispunjavanju njihovih odgovornosti. Čimbenici koje treba uzeti u obzir za izvještavanje uključuju, ali nisu ograničeni na:

- različite dionike, njihove specifične potrebe i zahtjeve za informacijama;
- trošak, učestalost i pravodobnost izvještavanja;
- način izvještavanja;
- relevantnost informacija za organizacijske ciljeve i donošenje odluka; [13]

6. Procjena rizika i proces upravljanja rizikom u informacijskoj sigurnosti prema ISO 27005

U poglavlju će biti razrađena procjena rizika prema ISO 27005 standardu. Obradit će se analiza mogućih rizika te njihova procjena. Nakon procjene rizika slijedi opis liječenja rizika s kojim poglavlje završava.

6.1. Uvod u procjenu rizika u informacijskoj sigurnosti

Procjena rizika određuje vrijednost informacijske imovine, identificira primjenjive prijetnje i ranjivosti koje postoje (ili bi mogle postojati), identificira postojeće kontrole i njihov učinak na utvrđeni rizik, utvrđuje potencijalne posljedice i konačno daje prioritet izvedenim rizicima. Na posljetku rizike rangira prema kriteriju u uspostavljenom kontekstu. [14]

Procjena rizika često se vrši u dvije ili više iteracija. Prvo se provodi procjena na visokoj razini s ciljem prepoznavanja rizika visokog nivoa koji zahtijevaju daljnju procjenu. Sljedeća iteracija može uključivati dublje razmatranje ranije identificiranih rizika. U situacijama gdje procjena ne nudi dovoljno informacija moguće je provoditi dodatne analize pa čak i druge metode. Na organizaciji je da odabere vlastiti pristup procjeni rizika na temelju svojih ciljeva i cilja procjene rizika. [14]

6.2. Uspostavljanje konteksta i kriterija

Bitno je odrediti svrhu upravljanja rizikom informacijske sigurnosti jer to utječe na cjelokupni rezultat procesa i uspostavljanja konteksta. Svrha može biti za:

- podršku sustavu za upravljanje informacijskom sigurnošću;
- usklađenost sa zakonskim propisima;
- opis zahtjeva za informacijskom sigurnošću proizvoda, usluge ili mehanizma;
- pripremu plana odgovora na incident; [14]

6.2.1. Osnovni kriteriji

Ovisno o opsegu i ciljevima upravljanja rizikom, mogu se primijeniti različiti pristupi. Pristup se također može razlikovati za svaku iteraciju. Treba odabrati ili razviti odgovarajući pristup upravljanju rizicima koji se bavi osnovnim kriterijima poput: kriterija za procjenu rizika, kriterija utjecaja i kriterija prihvaćanja. Uz to, organizacija bi trebala procijeniti jesu li dostupni potrebni resursi za:

- izvršavanje procjene i uspostavljanje plana liječenja rizika;

- definiranje i provođenje politike i postupaka uključujući provedbu odabranih kontrola;
- nadgledanje kontrola i postupaka upravljanja rizikom informacijske sigurnosti; [14]

Kod razvoja kriterija za procjenu rizika informacijske sigurnosti u organizaciji potrebno je u obzir uzeti sljedeće:

- stratešku vrijednost poslovnih informacija;
- kritičnost uključene informacijske imovine;
- zakonske i regulatorne zahtjeve te ugovorne obveze;
- operativnu i poslovnu važnost dostupnosti, povjerljivosti i integriteta informacija;
- očekivanja i percepciju dionika te negativne posljedice na dobru volju i ugled organizacije; [14]

Kod razvoja kriterija utjecaja treba ih navesti u smislu oštećenja ili troškova za organizaciju nakon nekog kritičnog događaja vezanog uz informacijsku sigurnost. U obzir treba uzeti sljedeće:

- razinu klasifikacije informacijske imovine;
- kršenja informacijske sigurnosti (npr. gubitak povjerljivosti, integriteta i dostupnosti);
- oštećene dijelove poslovanja;
- gubitak poslovne i financijske vrijednosti;
- ometanje planova i rokova;
- štetu ugleda i kršenje zakonskih, regulatornih ili ugovornih zahtjeva; [14]

Također je važno razviti i navesti kriterije prihvaćanja rizika. Oni često ovise o politici, ciljevima i interesima dionika organizacije. Organizacija bi trebala definirati vlastite ljestvice za razine prihvaćanja rizika, a u obzir treba uzeti sljedeće:

- da kriteriji za prihvaćanje rizika mogu uključivati više pragova s ciljanom razinom rizika;
- da se kriteriji mogu izraziti kao omjer procijenjene dobiti i procijenjenog rizika;
- da se na različite klase rizika mogu primjenjivati različiti kriteriji prihvaćanja rizika npr. rizici koji bi mogli rezultirati neusklađenošću s propisima ili zakonima možda neće biti prihvaćeni, dok se prihvaćanje opasnijih rizika može dopustiti ako je to određeno kao ugovorni zahtjev;
- da kriteriji prihvaćanja rizika mogu uključivati zahtjeve za budući dodatni tretman; [14]

Kriteriji prihvaćanja rizika mogu se razlikovati ovisno o tome koliko dugo se očekuje postojanje rizika, jer rizik može biti povezan s privremenom ili kratkoročnom aktivnošću. Kriteriji prihvaćanja rizika trebaju se postaviti s obzirom na sljedeće:

- poslovne kriterije;
- pravne i regulatorne aspekte;
- operacije;
- tehnologije;
- financije;
- socijalne i humanitarne čimbenike; [14]

6.2.2. Opseg i granice

Potrebno je definirati opseg postupka upravljanja rizikom informacijske sigurnosti kako bi se osiguralo da se sva relevantna imovina uzima u obzir kod procjene rizika. Informacije o organizaciji treba prikupljati kako bi se utvrdilo okruženje u kojem djeluje i relevantnost za postupak upravljanja rizikom informacijske sigurnosti. Pri definiranju opsega i granica, organizacija bi trebala uzeti u obzir sljedeće stvari:

- strateške i poslovne ciljeve te politiku organizacije;
- poslovne procese;
- zakonske, regulatorne i ugovorne zahtjeve koji se primjenjuju na organizaciji;
- politiku informacijske sigurnosti organizacije i cjelokupni pristup upravljanju rizicima;
- informacijsku imovinu;
- ograničenja koja utječu na organizaciju;
- očekivanja dionika; [14]

Uz to, organizacija bi trebala pružiti opravdanje za svako izuzeće iz područja primjene. Primjeri opsega upravljanja rizicima mogu biti aplikacija, informacijska infrastruktura ili poslovni proces.

6.2.3. Organizacija za upravljanje rizikom informacijske sigurnosti

Potrebno je uspostaviti organizaciju i odgovornosti za postupak upravljanja rizikom informacijske sigurnosti i održavati istu. Slijede glavne uloge i odgovornosti organizacije:

- razvoj procesa upravljanja rizikom informacijske sigurnosti pogodnog za organizaciju;
- identifikacija i analiza dionika;

- definiranje uloga i odgovornosti svih strana kako unutarnjih tako i vanjskih;
- uspostavljanje potrebnih odnosa između organizacije i dionika, sučelja s funkcijama upravljanja rizikom na visokoj razini u organizaciji te sučelja s drugim relevantnim projektima ili aktivnostima;
- specifikacija evidencije koju treba voditi; [14]

6.3. Procjena rizika

6.3.1. Identifikacija rizika

Svrha identifikacije rizika je utvrditi što bi moglo prouzročiti potencijalni gubitak i dobiti uvid u to kako, gdje i zašto bi se gubitak mogao dogoditi. Cilj identifikacije rizika je prikupiti ulazne podatke potrebne kod aktivnosti procjene rizika, a to su informacije o imovini, prijetnjama, trenutnim kontrolama, ranjivostima i posljedicama. [14]

Imovina je sve što ima vrijednost za organizaciju i stoga zahtijeva zaštitu. Za identifikaciju imovine treba imati na umu da se informacijski sustav sastoji od više hardvera i softvera. Identifikacija imovine trebala bi se provesti na odgovarajućoj razini detalja koja pruža dovoljno podataka za procjenu rizika. Ovisno o razini detalja koja se koristi u identifikaciji imovine ovisit će i kvaliteta te količina informacija prikupljenih tijekom procjene rizika. Razina se može unaprijediti u daljnjim iteracijama procjene rizika. Za svaku imovinu treba identificirati vlasnika kako bi se osigurala odgovornost za istu. [14]

Prijetnja je sve što može naštetiti imovini kao što su informacije, procesi, sustavi. Samim time našteti i samoj organizaciji. Prijetnje mogu biti prirodnog ili ljudskog podrijetla, te mogu biti slučajne ili namjerne. Prijetnje treba identificirati generički i prema vrsti (npr. neovlaštene radnje, fizička oštećenja, tehnički kvarovi). Zatim se prema potrebi identificirane pojedinačne prijetnje dodatno identificiraju unutar generičke klase. To dovodi do zaključka da se nikakve prijetnje ne zanemaruju. Neke prijetnje mogu utjecati na više elemenata. U takvim slučajevima mogu uzrokovati različite probleme ovisno o tome koja imovina je pogođena. Interno iskustvo iz incidenata i prošlih procjena prijetnji trebalo bi se uzeti u obzir kod trenutne procjene. Bilo bi također korisno pogledati druge kataloge prijetnji (možda specifične za organizaciju ili posao) da se upotpuni popis generičkih prijetnji tamo gdje je to potrebno. [14]

Treba utvrditi postojeće kontrole kako bi se izbjegao nepotreban rad ili trošak, npr. u dupliciranju kontrole. Uz to, tijekom identificiranja postojećih kontrola, treba izvršiti provjeru kako bi se osiguralo da kontrole rade ispravno. Postoje situacije kada odabrana kontrola (ili strategija) ne uspije u radu, no to je praćeno mjerenjem učinkovitosti kontrole. Pregledi uprave i izvješća o reviziji također pružaju informacije o učinkovitosti postojećih kontrola. Važno je napomenuti da kontrole koje se planiraju provesti treba uzeti u obzir na isti način kao i one već provedene. [14]

Prisutnost ranjivosti sama po sebi ne nanosi štetu jer za njezino iskorištavanje mora postojati prijetnja. Ranjivost koja nema odgovarajuću prijetnju možda neće zahtijevati provedbu

kontrole, ali bi trebala biti prepoznata. Treba imati na umu da je i neispravno implementirana kontrola ranjivost. Kontrola može biti učinkovita ili neučinkovita ovisno o okruženju u kojem djeluje. [14]

Posljedice mogu biti gubitak učinkovitosti, loše poslovanje i gubitak reputacije. Ova aktivnost identificira štetu ili posljedice za organizaciju koje bi mogle biti uzrokovane raznim incidentima. Scenarij incidenta je opis prijetnje koja iskorištava određenu ranjivost ili skup ranjivosti u incidentu s informacijskom sigurnošću. Utjecaj scenarija incidenta treba utvrditi uzimajući u obzir kriterije utjecaja definirane tijekom aktivnosti uspostavljanja konteksta. To pak može utjecati na jedno ili više sredstava ili na dio imovine. [14]

6.3.2. Analiza rizika

Analiza rizika može se poduzeti u različitim razinama detalja, ovisno o kritičnosti imovine, opsegu poznatih ranjivosti i prethodnim incidentima koji su se dogodili u organizaciji. U praksi se kvalitativna procjena često koristi prvo da bi se dobila opća naznaka razine rizika s ciljem otkrivanja glavnih rizika. Kasnije će možda biti potrebno poduzeti konkretniju ili kvantitativnu analizu glavnih rizika jer je obično manje složeno i jeftinije za izvoditi kvalitativne od kvantitativne analize. [14]

Način na koji se iskazuju posljedice i vjerojatnost te načini na koji se kombiniraju osigurat će da razina rizika varira ovisno o vrsti rizika i svrsi za koju se procjenjuje rizik. Vjerojatnost i ozbiljnost bi morale biti vrlo dobro razmotrene i razrađene. [14]

Nakon identifikacije sve imovine koja se pregledava, vrijednosti dodijeljene toj imovini trebaju se uzeti u obzir tokom procjene posljedica. Vrijednost poslovnog učinka može se izraziti u kvalitativnim i kvantitativnim oblicima, ali bilo kojom metodom dodjeljivanja novčane vrijednosti. Time se može pružiti više informacija za donošenje odluka i olakšati postupak donošenja odluka. Vrednovanje imovine započinje klasifikacijom prema njenoj kritičnosti u smislu važnosti za ispunjavanje poslovnih ciljeva organizacije. [14]

Procjena imovine ključni je čimbenik u procjeni scenarija incidenta jer incident može utjecati na više raznih sredstava ili dijelova imovine. Različite prijetnje i ranjivosti će imati različite učinke na imovinu, poput gubitka povjerljivosti, integriteta ili dostupnosti. Procjena posljedica stoga je povezana s procjenom imovine na temelju analize poslovnog učinka. Posljedice se mogu utvrditi modeliranjem ishoda događaja ili skupa događaja, ekstrapolacijom iz eksperimentalnih studija ili iz prošlih podataka. Posljedice u vremenu i financijama treba mjeriti istim pristupom koji se koristi za vjerojatnost prijetnje i ranjivost. Potrebno je održavati dosljednost kvantitativnog ili kvalitativnog pristupa. [14]

Nakon identificiranja scenarija incidenta, potrebno je procijeniti vjerojatnost svakog scenarija i utjecaja koji se javljaju, koristeći tehnike kvalitativne ili kvantitativne procjene. To bi trebalo uzeti u obzir koliko često se prijetnje pojavljuju i koliko se lako ranjivosti mogu iskoristiti. Za to u obzir treba uzeti:

- iskustvo i primjenjive statistike vjerojatnosti prijetnje;

- motivaciju i resurse dostupne napadačima kod namjernih izvora prijetnje;
- razne zemljopisne čimbenike, mogućnost ekstremnih vremenskih uvjeta i čimbenika koji mogu utjecati na ljudske pogreške kod slučajnih izvora;
- ranjivosti, kako pojedinačno, tako i agregirano;
- postojeće kontrole i koliko učinkovito smanjuju ranjivosti; [14]

Na primjer, informacijski sustav može imati ranjivost na prijetnje maskiranjem korisničkog identiteta zlouporabom resursa. Ranjivost maskiranja korisničkog identiteta može biti velika zbog nedostatka autentifikacije korisnika. S druge strane, vjerojatnost zlouporabe resursa može biti mala, unatoč nedostatku autentifikacije, jer su načini zlouporabe resursa ograničeni. [14]

6.3.3. Ocjenjivanje rizika

Odluke koje se odnose na procjenu rizika i na kriterije za procjenu rizika treba donositi prilikom uspostavljanja konteksta. Te odluke i kontekst trebalo bi detaljnije pregledati u ovoj fazi kada se sazna više o utvrđenim rizicima. Za procjenu rizika, organizacije bi trebale usporediti procijenjene rizike s kriterijima za procjenu rizika definiranim tijekom uspostavljanja konteksta. [14]

Kriteriji procjene rizika koji se koriste za donošenje odluka trebaju biti u skladu s definiranim vanjskim i unutarnjim kontekstom upravljanja rizikom informacijske sigurnosti i uzimati u obzir ciljeve organizacije te stavove dionika. Također bi trebali uključivati:

- svojstva informacijske sigurnosti - ako jedan kriterij nije relevantan za organizaciju (npr. gubitak povjerljivost), tada svi rizici koji utječu na ovaj kriterij možda nisu relevantni;
- važnost poslovnog procesa ili aktivnosti podržane određenom imovinom ili skupom imovine - ako je utvrđeno je da je postupak od male važnosti, rizici povezani s njim trebaju biti manje razmatrani od rizika koji utječu na važnije procese ili aktivnosti; [14]

Procjena rizika koristi razumijevanje rizika dobiveno analizom rizika za donošenje odluka o budućnosti radnje. Odluke trebaju uključivati:

- odgovor na pitanje treba li poduzeti neku aktivnost;
- prioritete za liječenje rizika uzimajući u obzir procijenjene razine rizika;
- zakonske i regulatorne čimbenike; [14]

6.4. Liječenje rizika

6.4.1. Opći opis liječenja rizika

Opcije liječenja rizika treba odabrati na temelju ishoda procjene rizika i očekivanog troška za provedbu ovih opcija i očekivane koristi od njih. Cilj je postići i provoditi velika smanjenja

rizika s relativno niskim izdacima. Daljnje mogućnosti za poboljšanja mogu biti neekonomične i treba provoditi prosudbu ovisno o tome jesu li poboljšanja opravdana. Općenito, štetne posljedice rizika trebaju biti što lakše izvedive bez obzira na apsolutne kriterije. Menadžeri bi trebali uzeti u obzir rijetke, ali ozbiljne rizike. U takvim slučajevima će se možda morati provesti kontrole koje nisu opravdane unutar strogih ekonomskih razloga. [14]

Četiri mogućnosti za liječenje rizika se međusobno ne isključuju. Ponekad organizacija može imati koristi kombinacijom nekih od njih. Neki tretmani rizika mogu učinkovito riješiti više od jednog rizika (npr. Obuka o informacijskoj sigurnosti i svijesti). Potrebno je definirati plan liječenja rizika koji jasno identificira redoslijed prioriteta u kojem se trebaju provoditi pojedinačni tretmani rizika i njihovi rokovi. Prioriteti se mogu utvrditi pomoću raznih tehnika uključujući rangiranje rizika i analizu troškova i koristi. Odgovornost menadžera u organizaciji je odlučiti o ravnoteži između troškova provedbe kontrola i dodjele proračuna. [14]

Identifikacija postojećih kontrola može odrediti da postojeće kontrole premašuju trenutne potrebe, u smislu usporedbe troškova i uključujući održavanje. Ako se razmatra uklanjanje suvišnih ili nepotrebnih kontrola treba uzeti u obzir sigurnost podataka i čimbenike troškova. Budući da kontrole mogu utjecati jedna na drugu, uklanjanje suvišnih kontrola može smanjiti ukupnu sigurnost. Osim toga, možda je jeftinije ostaviti suvišne ili nepotrebne kontrole na mjestu nego što je to potrebno ukloni ih. [14]

Treba razmotriti mogućnosti liječenja rizika uzimajući u obzir:

- kako pogođene strane percipiraju rizik;
- najprikladnije načine komuniciranja s tim stranama; [14]

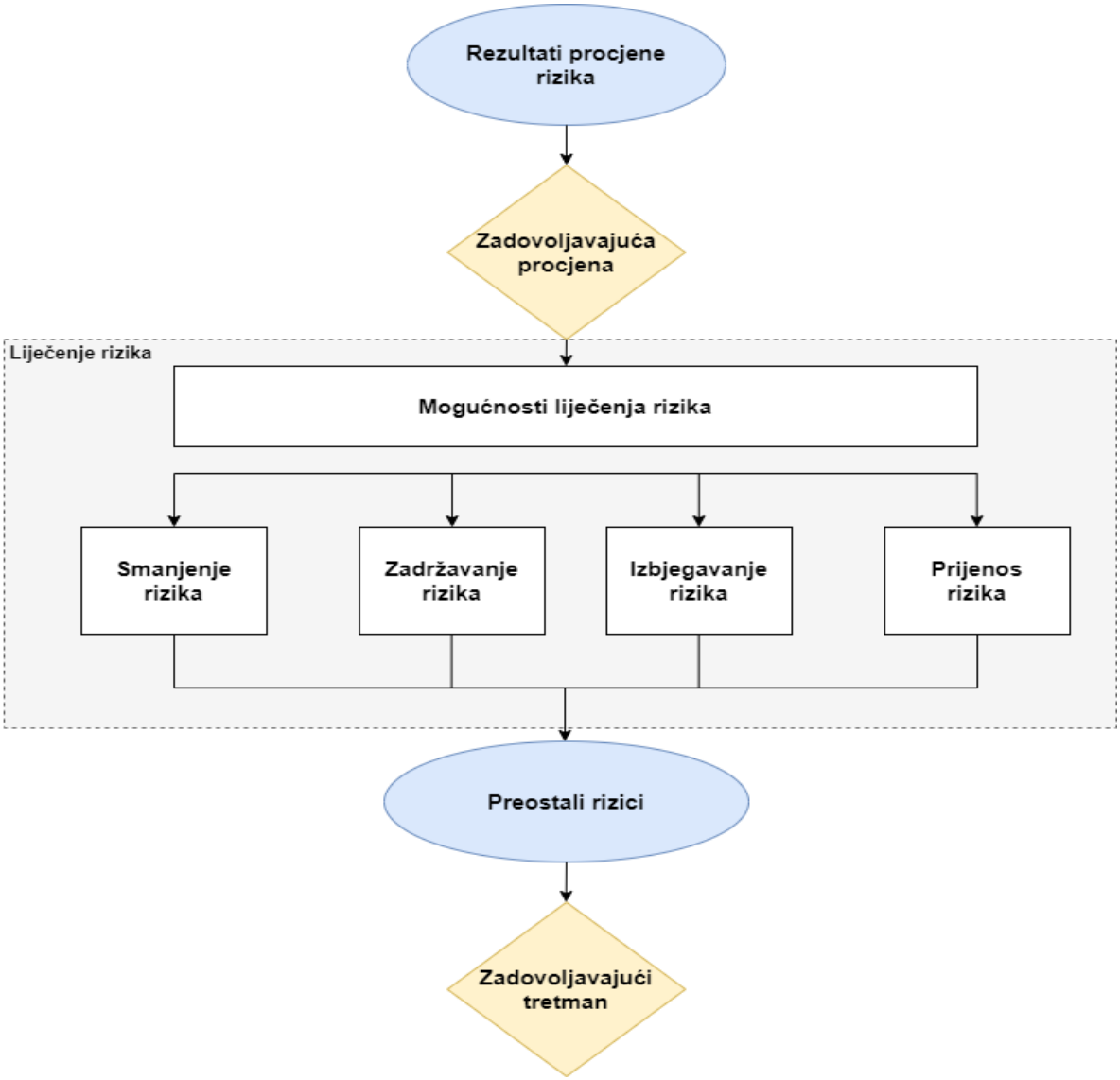
6.4.2. Smanjenje rizika

Treba odabrati odgovarajuće i opravdane kontrole kako bi se udovoljilo zahtjevima utvrđenim procjenom i liječenjem rizika. Odabir treba uzeti u obzir kriterije prihvaćanja rizika uz sve zakonske, regulatorne i ugovorne zahtjeve. Osim kriterija i zahtjeva odabir mora voditi računa o troškovima i vremenskom okviru za provedbu kontrola. Dobrim kontrolama moguće je lako spustiti ukupni trošak vlasništva nad sustavom. [14]

Općenito, kontrole mogu pružiti jednu ili više sljedećih vrsta zaštite: ispravak, uklanjanje, prevenciju, minimiziranje utjecaja, odvraćanje, otkrivanje, oporavak, nadzor i svijest. Tijekom odabira kontrole važno je izvagati troškove nabave, implementacije, administracije, rada, praćenja, i održavanje kontrola vrijednosti imovine koja se štiti. U obzir treba uzeti i povratak investicije u smislu smanjenja rizika i otkrivanja novih poslovnih prilika. [14]

Mnogo je ograničenja koja mogu utjecati na odabir kontrola. Tehnička ograničenja kao što su zahtjevi izvedbe, upravljivost i kompatibilnost mogu ometati upotrebu određenih kontrola te izazvati ljudsku pogrešku i poništiti kontrolu što može dovesti i do povećanja rizika. Pri odabiru kontrola i tijekom provedbe treba uzeti u obzir različita ograničenja, a najčešće se u obzir uzimaju :

- vremenska ograničenja;
- financijska ograničenja;
- tehnička ograničenja;
- operativna ograničenja;
- kulturna i etička ograničenja;
- zakonska ograničenja;
- kadrovska ograničenja;
- ograničenja za integriranje novih i postojećih kontrola; [14]



Slika 6: Aktivnost liječenja rizika (Izvor: [14])

6.4.3. Zadržavanje, izbjegavanje i prijenos rizika

Kada razina rizika zadovoljava kriterije prihvaćanja rizika, nema potrebe za provođenjem dodatnih kontrola i rizik se može zadržati. [14]

U slučaju da se utvrđeni rizici smatraju previsokima ili troškovi primjene drugih mogućnosti liječenja rizika premašuju koristi može se donijeti odluka da se rizik u potpunosti izbjegne povlačenjem postojeće aktivnosti ili skupa aktivnosti. Za rizike uzrokovane prirodom možda je najisplativija alternativa u fizičkom premještanju postrojenja za obradu informacija do mjesta na kojem rizik ne postoji ili je pod nadzorom. [14]

Prijenos rizika uključuje odluku da se određeni rizici podijele s vanjskim stranama. Prijenos rizika može stvoriti nove rizike ili modificirati postojeće već identificirane rizike što nekad dovodi do potrebe za dodatnim liječenjem rizika. Prijenos se može izvršiti osiguranjem koje će podržati posljedice ili ugovaranjem partnera čija će uloga biti nadgledanje informacijskog sustava i poduzimanje neposrednih radnji za zaustavljanje napada prije nego što napad dogodi. Treba napomenuti da je moguće prenijeti odgovornost za upravljanje rizikom, ali nije moguće prenijeti odgovornost za štetu. [14]

7. Izazovi u procjeni rizika

Danas su izazovi za učinkovito provođenje procjena rizika slični u gotovo svim organizacijama, ali strategije provedene za prepoznavanje i sprječavanje tih izazova jedinstvene su za svaku organizaciju. Iskrena, promišljena i autentična procjena rizika s kojima se suočava cijelo poduzeće ili poslovni segment omogućuje odgovarajuću identifikaciju nadolazećih prijetnji. Efikasna implementacija i provedba strategije procjene rizika stvara konkurentsku prednost koja donosi vrhunski povrat. S druge strane, procjena rizika vođena lošim načelima izlaže poduzeće potencijalno pogubnim ishodima. [15]

S druge strane, iako svaka neuspješna priča u proteklom desetljeću uvijek upućuje na nepostojanje preciznih modela upravljanja rizicima u poduzećima, jednako je točno da postoje određeni izazovi za učinkovitu procjenu rizika. Ti su izazovi uobičajeni u svim industrijama, s varijacijama u njihovom intenzitetu, ovisno o vrstama poslovanja, veličini poduzeća i kulturi unutar organizacije. Ti izazovi uključuju sljedeće:

- promatranje procjene rizika kao prepreke u provođenju svakodnevnih aktivnosti - iako poduzeća prepoznaju procjenu rizika kao kritičnu disciplinu, nažalost, prihvaćanje je još uvijek uglavnom akademsko. Veliki broj poduzeća abdicira ili odgađa procjenu rizika u korist uobičajenih poslovnih zadataka i smatra da povezane prakse donose ograničenu ili nikakvu vrijednost. Ovaj manjkavi pristup potječe iz nesposobnosti organizacija da stvore solidan poslovni slučaj za procjenu rizika;
- borbu organizacije sa samim procesom - među poduzećima koja su spremna izvršiti procjenu rizika strahovito se velik broj njih zapetlja u sam postupak i rijetko kad dođe do plodnog završetka. To je često rezultat žurbe s dovršenjem procjene rizika u regulatorne svrhe;
- interpretaciju podataka za dobivanje kvalitetnog uvida u situaciju - informacije postoje i generiraju se u velikim količinama brzini. Iako je organiziranje i obrada dostupnih velikih količina podataka radi predviđanja rizika teška, ona donosi veliku pomoć, no nisu sve organizacije spremne odraditi tako veliki zadatak;
- ignoriranje provedbe procjene rizika - slaba provedba gore navedenih koraka u kombinaciji s nedostatkom odgovornosti dovodi do slabe ili nikakve provedbe procjene rizika; [15]

7.1. Izazovi vezani uz ljudski faktor

Osim organizacijskih izazova u procjeni rizika postoji i problem s ljudskim faktorom, a takav problem se manifestira u situacijama kada čelnici upravljanja rizicima trebaju govoriti jezik poslovanja. Poput mnogih profesija, oni koji vode napore u upravljanju rizicima u organizaciji često razvijaju vlastiti jezik koji koriste za komunikaciju s drugima. Razgovori o vjerojatnosti, utjecaju, inherentnim i rezidualnim rizicima, apetitu za rizikom i tolerancijama na rizik postaju

uobičajeni među vođama upravljanja rizicima, ali ih drugi možda ne razumiju dobro. Neki vođe upravljanja rizikom zaboravljaju važnost govora jezikom kojim se služe oni iz njihove publike. Poslovni vođe usredotočeni su na povećanje marži, postizanje ciljeva i unapređenje poslovanja, a to obično utječe na njihovo razmišljanje i jezik koji koriste. Kao rezultat toga, ključni poslovni lideri možda ne razumiju ili ne cijene stručnjake koji se bave upravljanjem rizikom. Da bi se pozabavili tim problemom, neki vođe upravljanja rizikom preispituju jezik i žargon koji zaposlenici koriste kako bi osigurali da ih se čuje i razumije. Učenje, a zatim i korištenje poslovnog jezika koji se koristi u organizaciji može uvelike utjecati na angažiranje vođa poslovanja. [16]

7.2. Izazovi vezani uz poslovnu kulturu

Jedan od često zanemarenih problema je previd etičke i poslovne kulture. Poslovna kultura razlikuje se među organizacijama i važno je razumjeti kako kultura organizacije može utjecati na napore upravljanja rizikom. Razumijevanje što je važno među vođama organizacije može dati uvid u spremnost vođa organizacije da moraju poduzeti određene rizike. [16]

8. Procjena rizika

U ovom poglavlju će biti razrađena tema procjene rizika. Odgovorit će se na pitanje zašto je procjena rizika važna i u kojim se sve sferama života može pronaći. Osim potrebe za procjenom rizika razradit će se i pristupi procjeni rizika.

8.1. Potreba i važnost procjene rizika

Prepoznavanje rizika i procjena rizika zajedno čine komponentu procjene rizika u upravljanju rizicima. Budući da je procjena rizika jedan od glavnih faktora planiranja strategije bez nje se ne mogu postići kvalitetni rezultati. Rizici mogu biti povezani s korporativnim ciljevima, očekivanjima dionika i temeljnim procesima. Koju god od ovih polaznih točaka odaberemo na njoj se može vršiti procjena rizika. Svrha procjene rizika je identificirati značajne rizike koji bi mogli utjecati na odabranu značajku. Iako je procjena rizika od vitalne važnosti, korisna je samo ako se zaključci procjene koriste za donošenje odgovarajućih odgovora na rizik.[3]

Važna značajka poduzimanja procjene rizika je odluka hoće li se identificirani rizik ocjenjivati na svojstvenoj ili trenutnoj razini. Svojstvena procjena se vrši tako da se ne uzimaju u obzir kontrole koje su trenutno na snazi. Taj pristup preporučuju unutarnji revizori, dok ISO 31000 navodi da procjenu rizika treba vršiti na trenutnoj razini. Prednost poduzimanja procjene svojstvenog rizika je u tome što možemo identificirati razliku između trenutne i svojstvene razine rizika što pak daje naznaku važnosti postojećih kontrolnih mjera. [3]

Potreba za procjenom rizika postoji u raznim dijelovima države, a neke od njih su:

- zakonodavstvo;
- politika;
- ekonomija i ekonomska razmatranja;
- industrija; [17]

Kao primjer potrebe za promjenom rizika može biti političar na visokoj funkciji. Ako je političar ignorirao potrebu za procjenom rizika to može potencijalno utjecati na veće nesreće u raznim granama. Nesreća će ga dovesti u vrlo tešku situaciju koja stvara rizik da će političar biti odgovoran. Ta odgovornost ga može primorati da preda ostavku. [17]

8.2. Pristupi procjeni rizika

Danas je dostupan širok spektar tehnika procjene rizika. Objavljen je i "*Final Draft International Standard*" koji nudi informacije za cijeli niz tehnika procjene rizika koje se smiju koristiti. U nastavku će biti pobrojani najčešće korišteni pristupi procjeni rizika. [3]

Razmjena ideja temelji se na slobodnom protoku informacija i razgovoru između ljudi. Ljudi bi trebali biti upućeni u organizaciju i biti stručni u svom području. Cilj razgovora je lakše otkrivanje potencijalnog rizika i opasnosti. Međutim, istinska ideja ove metode uključuje posebne tehnike kojima se pokušava osigurati da mašta svakog člana pokrene misli i izjave drugih članova grupe. Ova metoda se može koristiti zajedno s ostalim niže opisanim metodama procjene rizika. Također se može koristiti i na visokoj razini rasprave gdje su problemi već identificirani. [18]

Delphi tehnika je postupak za postizanje pouzdanog konsenzusa mišljenja grupe eksperata. Ovaj postupak se ponekad poistovjećuje s razmjenom ideja no originalno je zamišljen tako da eksperti svoja mišljenja daju pojedinačno i anonimno, ali s mogućnošću pristupa stajalištima drugog stručnjaka. Delphi tehnika može se primijeniti u bilo kojoj fazi procesa procjene rizika. [18]

Kontrolne liste su najčešće stvorene iz prethodnih iskustava ili prošlih neuspjeha. Mogu se koristiti kod popisa opasnosti, ali i kod procjene učinkovitosti kontrola. Također imaju svoju korist u svakoj od faza životnog ciklusa procesa ili sustava. Često se koriste kao dio ostalih tehnika procjene rizika. Kontrolne liste su najkorisnije kod provjere pokrivenosti svih slučajeva nakon neke jače metode. [18]

Preliminarna analiza opasnosti (engl. *Preliminary hazard analysis - PHA*) je jednostavna induktivna metoda analize čiji je cilj prepoznati opasne situacije i događaje koji mogu naštetiti nekoj aktivnosti, objektu ili sustavu. Najčešće se provodi početkom razvoja projekta kada je malo podataka o detaljima dizajna ili operativnim postupcima. Analiza može biti korisna kod postojećih sustava za određivanje prioriteta kod opasnosti i rizika. [18]

HAZOP je akronim za studiju opasnosti i operativnosti (engl. *Hazard and Operability study*). HAZOP je strukturirano i sustavno ispitivanje planiranog ili postojećeg procesa, procedure ili sustava. To je je tehnika za identificiranje rizika po ljude, opremu ili organizacijske ciljeve. HAZOP identificira načine neuspjeha, njihove uzroke i posljedice. Tehnika je u početku razvijena za analizu kemijskih procesa, ali je proširena i na druge vrste sustava i kompleksnih operacija. Pod njih spadaju npr. strojni, elektronski i programski sustavi. [18]

Procjena toksičnosti (engl. *Toxicity assessment - TA*) je procjena svih opasnosti vezanih uz biljke, životinje, ljude i općenito uz okoliš. Metoda uključuje analizu opasnosti ili izvora štete i kako oni utječu na ciljanu populaciju te analizira puteve kojima opasnost može dosegnuti osjetljivu populaciju. Informacije se zatim kombiniraju kako bi se dala procjena vjerojatnog opsega i prirode štete.[18]

Strukturirana "Što ako" tehnika (engl. *Structured “What-if” Technique - SWIFT*). SWIFT je izvorno razvijen kao jednostavnija alternativa HAZOP-u. To je sustavna, timska studija, koja koristi skup "brzih" riječi ili fraza koje koristi voditelj radionice kako bi potaknuo sudionike na bolju identifikaciju rizika. Voditelj i tim koriste standardne fraze tipa "što-ako" kombinirane s uputama za istraživanje vezane uz to kako će sustav ili organizacija reagirati na odstupanja od uobičajenog načina rada. SWIFT se obično primjenjuje na više razina sustava s nižom razinom detalja od HAZOP-a. Iako je SWIFT izvorno dizajniran za kemijske i petrokemijske studije opasnosti, tehnika je široko rasprostranjena i primjenjuje se u raznim organizacijama.[18]

Analiza scenarija (engl. *Scenario analysis - SA*) je naziv za razvoj opisnih modela o tome kako bi mogla izgledati budućnost. Može se koristiti za utvrđivanje rizika uzimajući u obzir mogući budući razvoj i istraživanje njihovih implikacija. Analiza scenarija ne može predvidjeti vjerojatnost promjena, ali može razmotriti posljedice i pomoći organizacijama da razviju snagu i otpornost potrebnu za prilagodbu na predvidive promjene. Analiza scenarija je korisna za pomoć u donošenju odluka i planiranju budućih strategija, kao i za razmatranje postojećih aktivnosti. [18]

Stabla odlučivanja predstavljaju alternativne odluke i ishode u sekvencijalnom načinu uzimajući u obzir neizvjesne ishode. Slična su stablima događaja u tome što počinju inicijalnom odlukom ili događajem iz kojih se dalje modeliraju različiti putevi i ishodi. U upravljanju rizicima stablo odlučivanja se koristi u raznim situacijama kada postoji neizvjesnost kod odabira najboljeg postupka. Također nude i grafički prikaz. [18]

Analiza učinaka i tipova neuspjeha (engl. *Failure modes and effects analysis - FMEA*) je tehnika koja se koristi za identifikaciju načina na koji komponente, procesi ili sustavi ne mogu ispuniti namjere za koje su dizajnirani. FMEA identificira sljedeće:

- sve potencijalne načine kvarova različitih dijelova sustava (način kvara je ono što se primijeti kao neuspjeh ili pogrešno izvođenje);
- učinke koje kvarovi mogu imati na sustav;
- mehanizme neuspjeha;
- kako izbjeći kvarove i / ili ublažiti učinke kvara na sustav. [18]

Kritička analiza učinaka i tipova neuspjeha (engl. *Failure modes and effects and criticality analysis - FMECA*) proširuje FMEA tako da se svaki identificirani način kvara rangira prema svojoj važnosti ili kritičnosti. Ova kritička analiza je obično kvalitativna ili polukvantitativna, ali se može kvantificirati koristeći stvarne stope kvarova.

Neke od metoda koje neće biti detaljnije opisane, a koriste se su :

- Analiza skrivanja (engl. *Sneak analysis - SA*);
- Analiza skrivenog kruga (engl. *Sneak circuit analysis - SCI*);
- Markovljeva analiza;
- Monte Carlo simulacija;
- Bayesove mreže;
- FN krivulje;
- Indeksi rizika;
- Analiza troškova i koristi (engl. *Cost/benefit analysis- SA*); [18]

9. Matrice rizika

U poglavlju će biti detaljno opisane matrice rizika i njihovi tipovi. Dotaknut će se i uobičajene prakse kod izrade matrica te njihove prednosti i nedostatci.

9.1. Općenito o matricama rizika

Uobičajena metoda koja se koristi za rangiranje rizika su matrice rizika. One su najčešće veličine 4x4 ili 5x5. Sastoje se od dvije osi. Na jednoj osi je ozbiljnost događaja dok na drugoj vjerojatnost događaja. Matrice rizika se često definiraju kao "mehanizam za karakterizaciju i rangiranje rizika procesa". [19]

Matrice rizika obično se koriste za procjenu rizika kako bi se definirala razina rizika za sustav ili određene događaje i kako bi se utvrdilo je li rizik dovoljno kontroliran ili ne. Matrica gotovo uvijek ima dvije kategorije za procjenu: ozbiljnost i vjerojatnost. Na slici u nastavku slijedi primjer matrice rizika. [20]

Matrica za procjenu rizika				
Ozbiljnost / Vjerojatnost	Katastrofalna	Kritična	Marginalna	Neznatna
Često	Visok rizik	Visok rizik	Ozbiljan rizik	Osrednji rizik
Vjerojatno	Visok rizik	Visok rizik	Ozbiljan rizik	Osrednji rizik
Povremeno	Visok rizik	Ozbiljan rizik	Osrednji rizik	Nizak rizik
Slabo	Ozbiljan rizik	Osrednji rizik	Osrednji rizik	Nizak rizik
Vrlo malo vjerojatno	Osrednji rizik	Osrednji rizik	Osrednji rizik	Nizak rizik
Eliminirano	Eliminiran rizik			

Slika 7: Proces upravljanja rizikom (Izvor: [20])

U kontekstu matrica rizika, rizik se obično definira kao posljedica pomnožena s vjerojatnošću što rezultira negativnom posljedicom ili gubitkom. Umjesto da se odnosi na negativne posljedice kao "rizik", može se koristiti i precizan pojam zvan očekivani gubitak (engl. *Expected Loss- EL*). [21]

9.2. Podjela matrica rizika

Regije rizika su vrlo često proizvoljno dodijeljene ili dodijeljene na osnovu simetrije. To predstavlja problem ako su blokovi matrice rizika pogrešno grupirani te se tada mogu izvući netočni zaključci o relativnom riziku koji predstavljaju razne događaje u objektu. Uobičajeno se koriste tri vrste matrica za rangiranje rizika koje su opisane u nastavku. [19]

9.2.1. Kvalitativna matrica rizika

Kvalitativnoj matrici rizika u osnovi je zadatak analiza opasnosti s nekim relativnim prosudbama donesenim kako bi se kategorizirale opasnosti. Kada se koristi matrica veličine 3x3 ozbiljnost i učestalost se procjenjuju na jednostavnoj relativnoj skali koja nudi nisku, visoku i srednju razinu. Razine su parovi posljedica i učestalosti. [19]

9.2.2. Polukvantitativna matrica rizika

Postoji par ozbiljnih procjena rizika koje zapravo koriste čisti kvalitativni pristup procjeni rizika. Razlog tome su razni limiti tog pristupa. S ciljem povećanja iskoristivosti tog pristupa počele su se koristiti polukvantitativne sheme. Često se nazivaju kvalitativnim metodama iako se na njih primjenjuje kvantitativna osnova bilo na osi učestalosti ili na osi ozbiljnosti pa čak i na obje osi. Mnogo stručnjaka tvrdi da su i polukvantitativne i kvantitativne matrice vrlo limitirane i nema smisla grupirati rizike na taj način. [19]

9.2.3. Kvantitativna matrica rizika

Ne moraju se sve opasne situacije analizirati kvalitativno. Čineći ljestvicu posljedica kvantitativnom, čak i ako se radi samo o relativno bezdimenzionalnim jedinicama, relativni rizik se može izračunati za sve regije u matrici. Koristeći kvantitativni pristup izradi matrice rizika gdje svaki scenarij ima svoju relativnu vrijednost rizika omogućava se usporedba i rangiranje svakog pojedinog scenarija. [19]

9.3. Matrice rizika - Ozbiljnost

Ozbiljnost se obično definira kao skup kategorija kao što su:

- Katastrofalne: višestruka smrt
- Kritične: smrt ili višestruke teške ozljede
- Marginalne: jedna teška ili više lakših ozljeda
- Zanemarive: jedna lakša ozljeda [20]

Naravno, ove su kategorije subjektivne i dionici ih potencijalno mogu definirati na različite načine. Na primjer, zašto jedna smrt nije katastrofalna? Što je "teška ozljeda"? Alternativno, ili uz to, novčani gubici mogu se povezati s kategorijama ozbiljnosti, iako to postavlja moralne i praktične poteškoće u određivanju novčane vrijednosti ljudskog života.

Ozbiljnost je relativno jednostavno definirati, iako ostaje problem uzima li se u obzir najgori ishod, samo vjerodostojan ishod, najvjerojatniji ishod ili unaprijed definiran događaj. [20]

Korištenje najgoreg slučaja najobuhvatniji je pristup, ali može izraziti zabrinutost da je previše pesimističan i umjesto njega treba koristiti najgori vjerodostojni ishod. Ovo posljednje postavlja problem kako definirati „vjerodostojno“ i može dovesti do zamagljivanja razlike između ozbiljnosti i vjerojatnosti, čineći ova dva čimbenika istinski neovisnim u procjeni rizika. Treći pristup je korištenje najvjerojatnijeg ishoda, koji opet miješa ozbiljnost i vjerojatnost te smanjuje njihovu neovisnost. U mnogim slučajevima ljudi možda nisu svjesni da to čine i jednostavno se obvezuju dodijeliti ozbiljnost prema onome što su smatrali najvjerojatnijim ishodima. Konačna mogućnost, uzimajući u obzir samo određene unaprijed određene događaje može rezultirati vrlo optimističnom i često nerealnom procjenom rizika zbog prevelike ograničenosti. [20]

9.4. Matrice rizika - Vjerojatnost

Kod definiranja matrice rizika mnogo problema nastaje kod definiranja vjerojatnosti. Kada se za predviđanje koristi matrica rizika, cilj je procijeniti koliko često se događaj može dogoditi u budućnosti. Te je podatke teško ili nemoguće utvrditi. Iako bi se vjerojatnost mogla definirati pomoću povijesnih događaja, većina se sustava danas značajno razlikuje od istih sustava u prošlosti zbog opsežnije uporabe softvera ili upotrebe nove tehnologije i dizajna. Zapravo je uobičajeni razlog stvaranja novog sustava taj što postojeći sustavi više nisu prihvatljivi. [20]

Povijesni podaci govore nam samo o prošlosti, ali matrica rizika obično se koristi za predviđanje budućnosti. Samo zato što se nešto još nije dogodilo, ne pruža točno predviđanje budućnosti, posebno kada se sustav ili njegovo okruženje razlikuje od prošlog sustava. Čak i ako se sam dizajn ne promijeni u budućnosti, način korištenja sustava ili okruženje u kojem se koristi s vremenom će se gotovo uvijek promijeniti. Koncept "migracije prema većem riziku tijekom vremena" argumentira protiv primjenjivosti prošlosti kao odrednice za budućnost. A procjena budućih promjena zajedno s njihovim utjecajima u osnovi je nemoguća. [20]

Prema primjeru matrice rizika iz slike 7. vjerojatnosti rizika podijeljene su na :

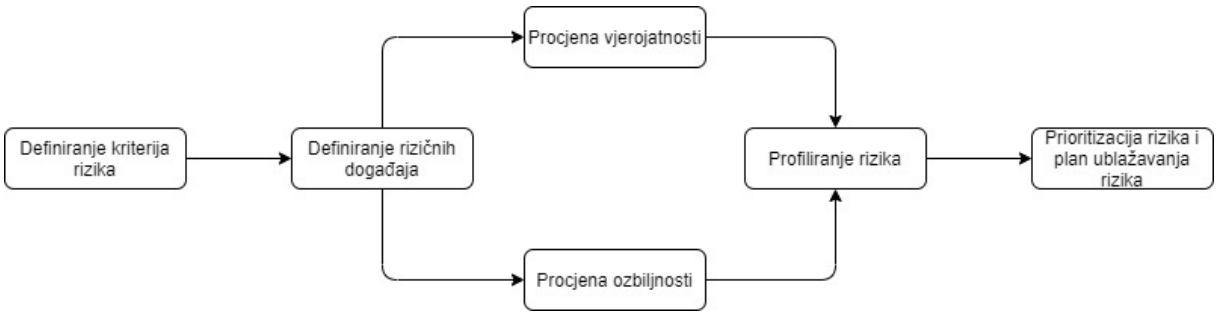
- Česte: često će se javljati u životu sustava;
- Vjerojatne: pojavit će se nekoliko puta u životu sustava;
- Povremene: vjerojatno će se dogoditi nekad u životu sustava;
- Malo vjerojatne: malo je vjerojatno da će se dogoditi u životu sustava, ali moguće;

- Vrlo malo vjerojatne: izuzetno je malo vjerojatno da će se dogoditi;
- Eliminirane: jednako vjerojatnosti nula; [20]

9.5. Uobičajene prakse kod izrade matrica

Smatra se da su matrice rizika dovoljno svestrane da se mogu koristiti za analizu i odrediti prioritete u mnogim postavkama. Niz međunarodnih standarda podržava ulogu matrica rizika u procjeni rizika i mnoge tvrtke ih smatraju "najboljom praksom".

Da bi se matrice rizika mogle koristiti za utvrđivanje prioriteta rizika potrebno je provesti nekoliko koraka. Jedan od procesa kreiranja matrice rizika kao alata za procjenu rizika može se vidjeti na slici ispod.



Slika 8: Proces upravljanja rizikom (Izvor: [20])

9.5.1. Definiranje kriterija rizika

Ovaj korak određuje veličinu i boje matrice rizika. Matrice su najčešće kvadratnog oblika no nema tehničkog objašnjenja zašto. Najčešća veličina je pet redaka s pet stupaca (tj. 5x5 matrica), ali neke tvrtke koristite matricu od 3x3, a ostali koriste matricu od 8x8. Boje koje se standardno koriste su crvena, žuta i zelena no neke tvrtke također uključuju i ostale boje. [21]

9.5.2. Definiranje rizičnih događaja

Ovaj korak identificira rizik događaja. Kao primjer događaja može se uzeti brušenje određenog metalnog dijela u tvrtki. Za taj događaj treba identificirati sve moguće nepovoljne ishode.

9.5.3. Procjena vjerojatnosti i ozbiljnosti događaja

Ovaj korak procjenjuje raspon posljedica svakog utvrđenog ishoda u koraku 2 i dodjeljuje vjerojatnosti svakom ishodu. Za primjer, registrira se ishod ozbiljnih gubitaka, a očekivane financijske posljedice procjenjuju se od 1 USD do 5 milijuna USD s vjerojatnošću događaja od 40%.Te će se podatak kao takav zapisati u matricu. [21]

9.5.4. Profiliranje rizika

Za svaki od procijenjenih koraka uzimamo rezultat iz gornjeg koraka te ga zapisujemo u matricu rizika. [21]

9.5.5. Prioritizacija rizika

Ovaj korak rangira i daje prioritet ishodima prema njihovom riziku. Većina tvrtki koristi politiku upravljanja rizicima u kojoj su svi ishodi u crvenom području neprihvatljivi i stoga se moraju ublažiti. Rezultati koraka od 2 do 5 često se zajednički nazivaju „Registar rizika“, a potrebni se podaci obično prikupljaju na zajedničkom sastanku s ključnim dionicima. Dionike čine operativni i uslužni dio tvrtke te svi bitni partneri. [21]

9.6. Trenutni standardi u izradi matrica rizika

Neki od standarda koji se koriste u području naftne industrije su API, NORSOK i ISO. Svi ovi standardi preporučuju matrice rizika kao element odnosno alat upravljanja rizikom. [21]

9.6.1. API

API RP 581 (2008) preporučuje matrice rizika za svoju rizikom vođenu inspekciju (engl. *risk-based-inspection - RBI*). RBI je metoda za optimizaciju planiranja inspekcije generiranjem rangiranja rizika za opremu i procese, a iz toga slijedi određivanje prioriteta inspekcije razne opreme. API RP 581 određuje kako izračunati vjerojatnosti i posljedice koje će se koristiti u matricama rizika. Specifikacija je funkcija opreme koja se analizira. Izračunava se vjerojatnost i posljedica kvara upotrebom nekoliko čimbenika. API RP 581 tvrdi da je „Predstavljanje rezultata u matrici rizika učinkovit način prikazivanja raspodjele rizika za različite komponente u procesnoj jedinici bez numeričkih vrijednosti".[21]

9.6.2. NORSOK

NORSOK norme su razvijene od strane norveške naftne industrije. Cilj normi je da osiguraju odgovarajuću sigurnost i vrijednost te da dodaju isplativost razvoju naftne industrije. Norme su pokušale što je više moguće zamijeniti specifikacije naftne tvrtke i služiti kao reference u propisima vlasti. Preporučuje korištenje matrica rizika za većinu njihovih ilustracija analize rizika. Njihove matrice rizika su manje striktne nego one API RP-a jer se mogu prilagoditi široj paleti problema.NORSOK S-012 HSE JE dokument koji se odnosi na izgradnju naftne infrastrukture i koristi matrice rizika veličine 3x3. [21]

9.6.3. ISO 31000

ISO 31000 utječe na mnogo raznih industrija. U ISO IEC 31010 postoji tablica koja sažima primjenjivost alata koji se koriste za procjenu rizika. ISO tvrdi da je matrica rizika "jako primjenjiv" alat za utvrđivanje i analizu rizika te je „primjenjiv“ za ocjenjivanje rizika. Kao i kod norme NORSOK, ISO ne standardizira broj boja,shemu bojanja i veličina raspona za svaku kategoriju. ISO cijeni matrice rizika zbog njihove praktičnosti, jednostavnosti upotrebe i brzih rezultata. Međutim, ISO također navodi ograničenja matrica rizika, uključujući i neke njihove nedosljednosti koje slijede u nastavku. [21]

9.7. Limiti i nedostatci matrica za procjenu rizika

Matrice rizika imaju nekoliko svojih mana. Neke od njih mogu se ispraviti, dok se druge čine problematičnijima. Jedna od mana je poredak koji donosi matrica rizika, a ovisi o proizvoljnim izborima s obzirom na dizajn. Primjer je odabir skale za ocjenjivanje koja se može povećavati ili smanjivati. [21]

Prema ISO standardu limiti matrica rizika su sljedeći:

- za oblikovanje valjane matrice potrebna je velika stručnost;
- može biti teško definirati uobičajene ljestvice koje se primjenjuju u nizu okolnosti relevantnih za organizaciju;
- teško je jednoznačno definirati ljestvice kako bi se korisnicima omogućilo da odmjere ozbiljnost i vjerojatnost dosljedno;
- valjanost ocjena rizika ovisi o tome koliko su ljestvice razvijene i kalibrirane;
- ispravno kalibrirana matrica uključivat će vrlo male razine vjerojatnosti za mnoge pojedinačne rizike koje je teško konceptualizirati;
- upotreba matrica je vrlo subjektivna i različiti ljudi često dodjeljuju vrlo različite ocjene za isti rizik. To ostavlja velik prostor za manipulaciju;
- rizici se ne mogu izravno agregirati;
- teško je kombinirati ili uspoređivati razinu rizika za različite kategorije posljedica;
- svaka ocjena ovisit će o načinu opisivanja rizika i razini detalja.Iz tog razloga način na koji su scenariji grupirani u opisivanju rizika treba biti dosljedan i definiran prije rangiranja. [22]

9.7.1. Neusklađenost prihvaćanja rizika

Matrice rizika moraju precizno i pouzdano kategorizirati moguće ishode u zelenu, žutu i crvenu regiju.Prvo pravilo je da očekivani gubitak u zelenoj boji uvijek moram biti manji od onog

u crvenoj. Jedno od pravila je žutu boju koristiti za razdvajanje između crvene i zelene te se kao takva ne bi trebala koristiti za kategorizaciju ishoda. Tvrde da je matrica rizika nedosljedna ako je očekivani gubitak u žutom području veći od onog u crvenom. Puno članaka krši ovo pravilo koje je predložio Cox 2008., a kršenjem tih pravila dovodi se do nedosljednosti u matricama rizika. [21]

9.7.2. Kompresija dosega

Kompresija dosega u matricama rizika je mana koja se opisuje kao kvantitativno dodjeljivanje identične ocjene dvama vrlo različitim rizicima. Kompresija dosega je neizbježna kada se posljedice i vjerojatnosti pretvaraju u bodove. U tom pretvaranju bodova udaljenosti između rizika ne odražavaju stvarnu udaljenost. [21]

9.7.3. Centriranje pristranosti

Centriranje pristranosti odnosi se na tendenciju ljudi kako bi se izbjegle ekstremne vrijednosti. Na primjer, ako je raspon rezultata od 1 do 5, većina ljudi odabrat će vrijednost od 2 do 4. U istraživanju iz 2009. otkriveno je da 75% od odabranih rezultata 3 ili 4 na skali od 1 do 5. To dodatno komprimira ljestvica matrice rizika, pogoršavajući kompresiju dometa. [21]

9.8. Prednosti matrica rizika

Neke od prednosti matrica rizika su:

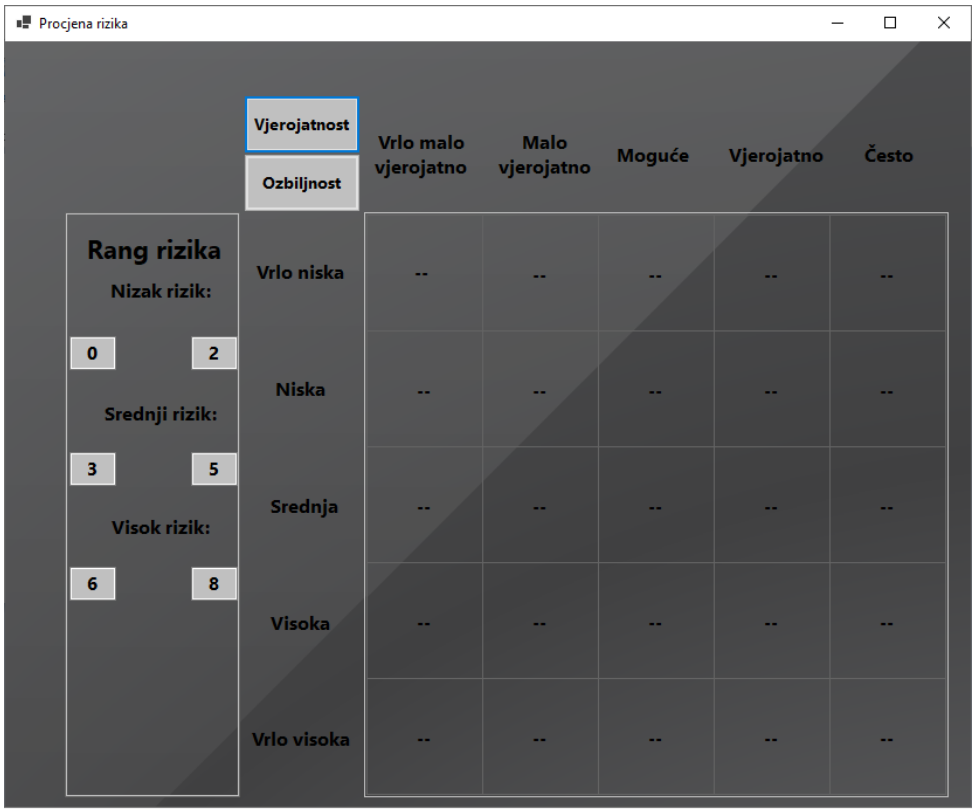
- relativno jednostavna uporaba;
- pruža brzo rangiranje rizika na različite razine značajnosti;
- pruža jasan vizualni prikaz relevantnog značaja rizika kao posljedice, vjerojatnosti ili razine rizika;
- može se koristiti za usporedbu rizika s različitim vrstama posljedica; [22]

10. Izrada alata za procjenu rizika

U poglavlju će biti opis način izrade alata za procjenu rizika. Objasnit će se pokretanje i izgled aplikacije te njezina svrha. Poglavlje završava opisom korištenja aplikacije.

10.1. Općenito o aplikaciji

Alat za procjenu rizika izrađen je u C# programskom jeziku. Aplikacija se sastoji od 3 forme. Može se pronaći na sljedećem linku: https://github.com/igradiski/diplomskiRiskMatrix. Link nudi izvorni kod aplikacije kao i njezin instalacijski paket. Namijenjena je za pokretanje na operacijskom sustavu Windows 10, a troši vrlo malo računalnih resursa. Pokrenuti se može preuzimanjem izvornog koda i otvaranjem istog u Visual Studio razvojnom okruženju ili klikom na ikonu aplikacije nakon instalacije. Nakon pokretanja aplikacije otvara se početni ekran koji je prikazan na slici ispod.

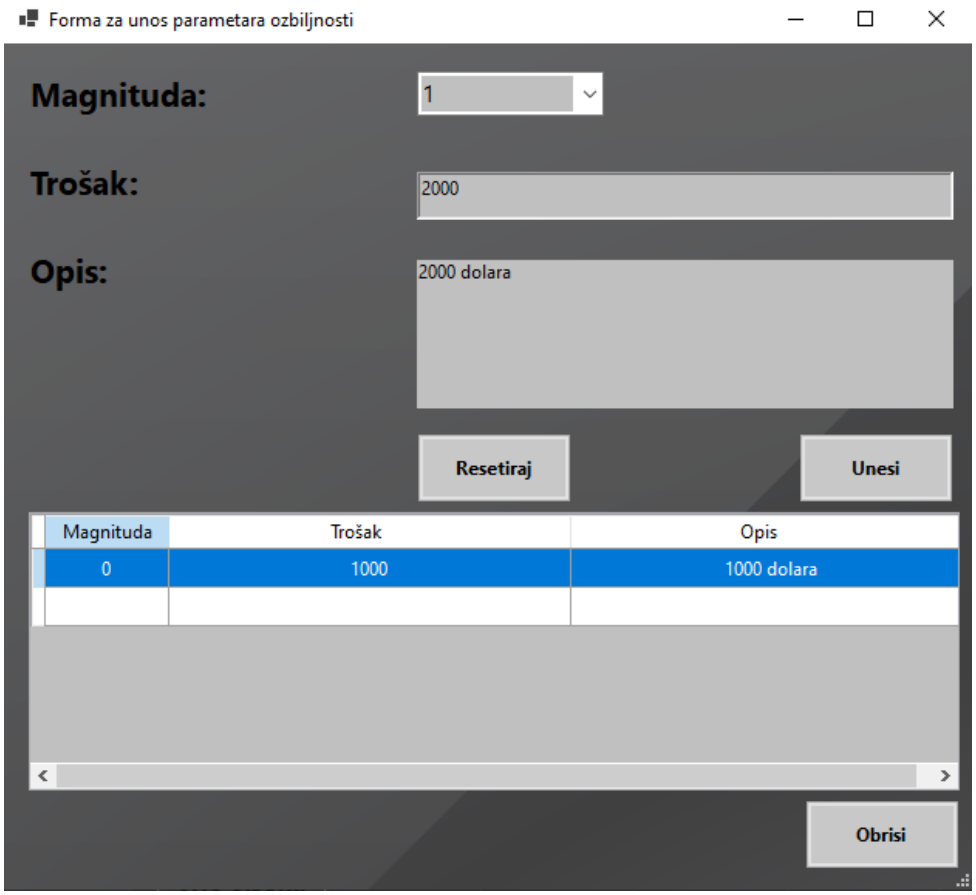


Slika 9: Glavni ekran aplikacije (autorski rad)

Glavni izbornik se sastoji od panela u kojima su zapisani rangovi rizika, gumba za unos vjerojatnosti i ozbiljnosti te panela u kojem će biti prikazana matrica rizika. Nakon uspješnog unosa vjerojatnosti i ozbiljnosti prikazuje se gumb za kreiranje matrice rizika no samo ako su svi parametri ispravno uneseni jer u suprotnom matrica neće davati ispravne rezultate.

10.2. Korištenje aplikacije

Nakon pokretanja aplikacije potrebno je unijeti parametre za vjerojatnost i ozbiljnost. Klikom na gumb otvara se forma za unos koja izgleda kao na slici ispod.

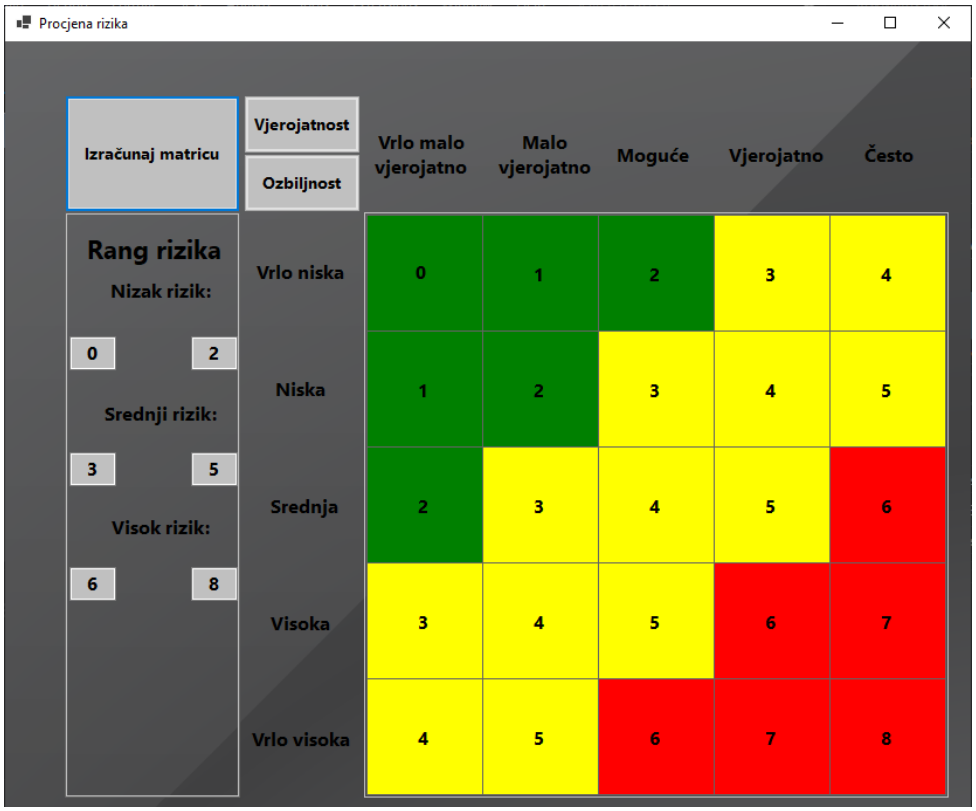


Slika 10: Forma za unos ozbiljnosti (autorski rad)

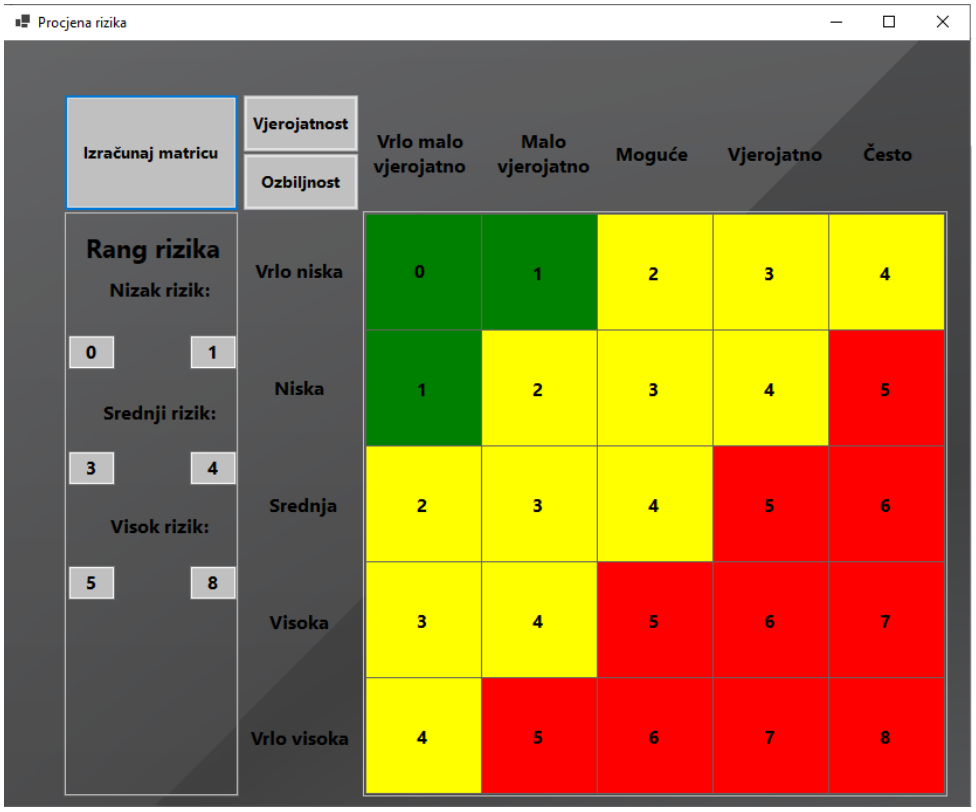
Potrebno je unijeti 5 magnituda ozbiljnosti iz razloga jer je matrica rizika veličine 5x5. U slučaju da se ne unesu svi parametri, a forma se želi zatvoriti aplikacija izbaci upozorenje za korisnika. Gumb resetiraj služi da se obrišu trenutno ispunjena polja za trošak i opis. Na gumb unesi se unosi nova magnituda koja se tada vidi u pregledu. Klikom na gumb obriši se briše odabrani red. Forma za unos vjerojatnosti je gotovo ista osim što se unosi broj pojava te ju zato neću prikazivati no u aplikaciji se ona i dalje normalno koristi.

Nakon unosa svih potrebnih parametara prikazuje se gumb izračunaj matricu. Klikom na njega izračunava se matrica s obzirom na unesene vrijednosti. Kada su vrijednosti izračunane program automatski boja polja u jednu od tri boje. Zelenu za niski rizik, žutu za srednji rizik i crvenu za visok rizik. Važno je napomenuti da se rangovi rizika mogu proizvoljno mijenjati ako je to potrebno. Na slikama 12 i 13 ispod mogu se vidjeti dvije ispunjene matrice.

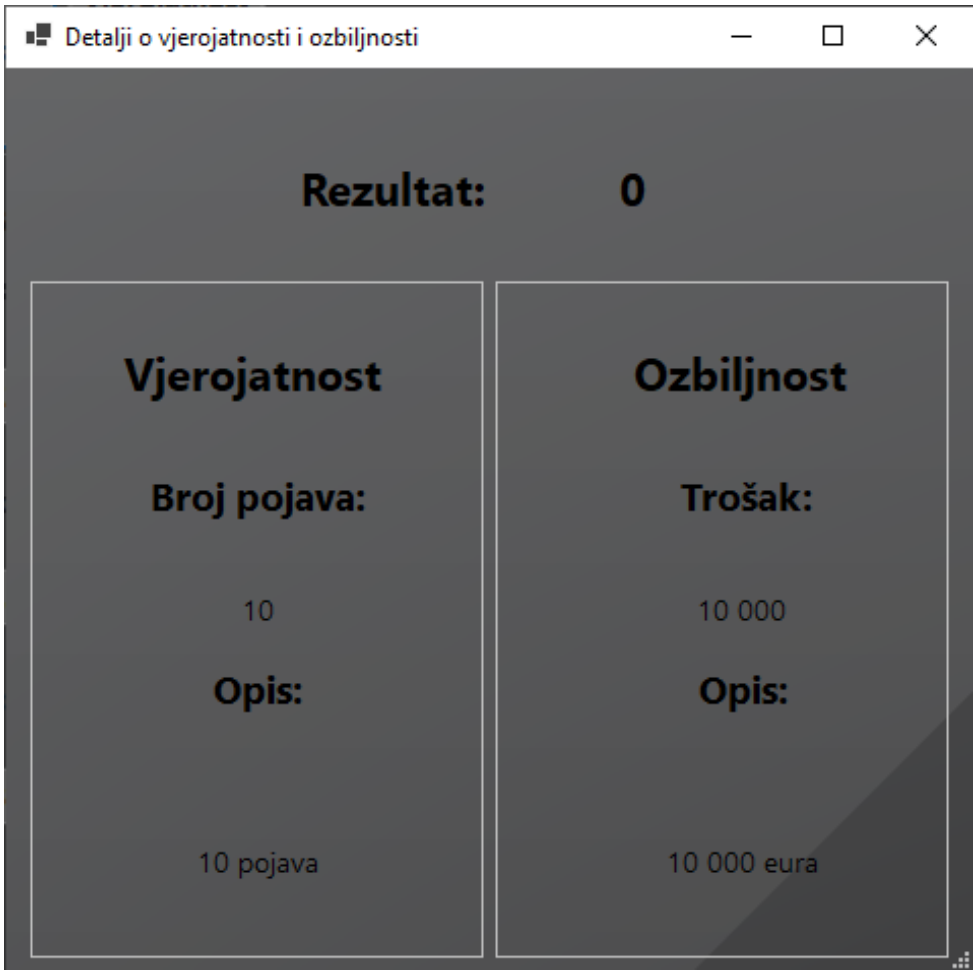
Klikom na određeno polje u matrici dobivamo detaljan prikaz unesenih vrijednosti. Prikaz se može vidjeti na slici 14.



Slika 11: Ispunjena matrica rizika (autorski rad)



Slika 12: Ispunjena matrica rizika (autorski rad)



Slika 13: Detalji rizika (autorski rad)

11. Zaključak

Izrada alata za izradu rizika je jako zanimljiva tema. Glavna motivacija za rad bila je kombinacija domene procjene rizika s informatikom koja mi je struka. Kao što sam već ranije napomenuo rizici postoje i uvijek će postajati u svim sferama ljudskog djelovanja. Procjenu rizika mnogi smatraju nepotrebnim teretom, no ako se ispravno provodi od tereta postaje sredstvo kojim se indirektno utječe na povećanje dobiti organizacije.

U radu sam odradio razne okvire i standarde za procjenu rizika. Postoji mnogo standarda i svaki ima domenu u kojoj je kvalitetniji od ostalih. Također procjene rizika koliko god bile različite od standarda do standarda imaju zajednički kostur po kojima se provode no naravno razlikuju se u nekim detaljima. U središnjem dijelu rada dotaknuo sam se ISO standarda i razrada tog dijela dala mi je odličan uvid u kompletan proces procjene rizika s kojim se prije nisam susretao. Razrada procjene rizika kod informacijske sigurnosti je vrhunac rada jer se u tom dijelu moja struka i procjena rizika vrlo usko susreću.

Posljednji dio rada je vezan uz matrice rizika koje se koriste u procjeni rizika. Osim što se koriste za procjenu rizika njih ću implementirati u alatu. Matrice rizika su jednostavna, ali moćna metoda za procjenu rizika i vrlo su zanimljive za implementaciju.

Gledajući rad općenito bilo mi je iznimno zanimljivo koristiti svoju struku u jednom od područja s kojim se nisam doticao. Procjena rizika je jako opsežna tema, ali kada se krene u dubinu sve počinje dobivati smisao i vrlo je zanimljivo. Osim velikog znanja koje sam dobio razradom ove teme kreiran je i alat za procjenu rizika koji je kombinacija mojih programerskih vještina i novog znanja.

Popis literature

[1] Overleaf, „About Overleaf," *Overleaf, preuzeto 20.5.2021. sa: https://www.overleaf.com/about*,

[2] diagrams.net, „About diagrams.net," *preuzeto 20.5.2021. sa: https://www.diagrams.net/about*,

[3] P. Hopkin, „Fundamentals of Risk Management," 2010.

[4] R. W. Johnson, „Risk Management by Risk Magnitudes," 1998.

[5] D. Geoghegan, „The Successful Leader Part 1," *The Successful Leader Part 1*, 2011.

[6] S. Jennings, „Risk Management Framework," *Hywel Dda University Health Board*, 2017.

[7] R. R. Moeller, „Understanding the New Integrated ERM Framework," 2007.

[8] British Standards Institute BSI, „Risk management – Code of practice," 2011.

[9] Institute of Risk Management, „A Risk Management Standard," 2002.

[10] N. Turnbull, „Internal Control: Guidance for Directors on the Combined Code (The Turnbull Report)," *Risk Management: An International Journal*, 1999.

[11] UK Goverment, „The orange Book," *The orange Book Management of risk-Priciples and Concepts*, 2020.

[12] Goverment of South Australia Department, „Risk Management Framework," 2010.

[13] International Organization for Standardization ISO, „INTERNATIONAL STANDARD ISO 31000 Risk management — Guidelines," ISO, 2018.

[14] British Standards Institute BSI, „Information technology — Security techniques — Information security risk management," 2008.

[15] Risk Management Studio, „Common Challenges to Effective Risk Assessment," 2019.

[16] M. Beasley, „Today's Risk Management Challenges: It's a Small World After All," 2019.

[17] Rescue Services Agency, „Handbok för riskanalys," *Handbok för riskanalys*, 2003.

[18] D. Geoghegan, „Risk and Reward Analysis," 2017.

[19] M. Elmontsri, „Review of Strenghts and Weaknesses of Risk Matrices," *The Journal of Risk Analysis and Crisis Response*, 2014.

[20] P. N. Leveson, „Improving the Standard Risk Matrix: Part 1," 2019.

[21] P. Thomas, „The Risk of Using Risk Matrices," 2013.

[22] International Organization for Standardization ISO, „Risk management – Risk assessment techniques," 2019.

Popis slika

Popis tablica