

MINISTARSTVO FINANSIJA

**SMJERNICE
ZA UPRAVLJANJE KLJUČNIM/STRATEŠKIM
RIZICIMA U JAVNOM SEKTORU**

Podgorica, decembar 2022.

Sadržaj

1. Uvod	3
1.2 Šta su ključni/strateški rizici?	4
1.3 Šta je upravljanje ključnim/strateškim rizicima?.....	5
2. Upravljanje ključnim/strateškim rizicima i odgovornost za njihovo upravljanje	7
3. Proces, alati i metodologije upravljanja ključnim/strateškim rizicima.....	8
3.1 Identifikacija ključnih/strateških rizika	8
3.2 Procjena rizika	13
3.3 Reagovanje na rizik.....	14
3.4 Praćenje rizika i izvještavanje o rizicima.....	16
PRILOG A: Primjeri (globalni, nacionalni ili organizacioni) ključni rizici.....	20
PRILOG B: Primjeri (vizuelni dio) godišnjeg izvještaja o ključnim/strateškim rizicima	22

1. Uvod

Ministarstvo finansija je kao pomoć subjektima u implementaciji procesa upravljanja rizicima u javnom sektoru Crne Gore pripremio Smjernice za uspostavljanje i sprovođenje procesa upravljanja rizicima u javnom sektoru¹, koje su se tokom vremena kontinuirano unapređivale u skladu sa zahtjevima korisnika i stepenom razvoja ovog sistema.

U skladu sa nedavnim razvojem reformi javne uprave i upravljanja javnim finansijama, prepoznata je potreba za strukturiranim pristupom za upravljanje ključnim/strateškim rizicima u subjektima javnog sektora.

Implementacija procesa upravljanja rizicima, a posebno integracija u procese strateškog upravljanja (planiranje i kontrola) zahtijeva vrijeme i suočava se sa mnogim izazovima i preprekama. Efektivna implementacija zahtijeva iterativni proces, korak po korak koji je pažljivo kreiran da odgovara kulturi organizacije. Primjena heurističkog pristupa omogućava organizaciji da na svakom koraku razumije šta funkcioniše ili ne, a da zatim prilagodi upravljanje rizicima kako bi osigurali ostvarenje ciljeva.

Smjernice za upravljanje ključnim/strateškim rizicima imaju za cilj da kroz uputstva i sugestije podrže subjekte u javnom sektoru da uvedu ili ojačaju dizajn i funkcionisanje upravljanja ključnim/strateškim² rizicima.

Osnovna razlika u odnosu na **Smjernice za uspostavljanje i sprovođenje procesa upravljanja rizicima** je u vrsti rizika koji su u fokusu, jer je u **Smjernicama za upravljanje ključnim/strateškim rizicima** veći naglasak na ključnim/strateškim rizicima.

Ove Smjernice su nastale u okviru projekta koji je finansiran sredstvima Evropske unije.

¹ Sastavni dio Pravilnika o načinu uspostavljanja i unapređenja upravljanja i kontrola u javnom sektoru (Službeni list CG, broj 71/19)

² Proces upravljanja rizicima već je opisan u Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima u javnom sektoru, tako da se koraci koji su u njima opisani neće ponavljati u ovim Smjernicama.

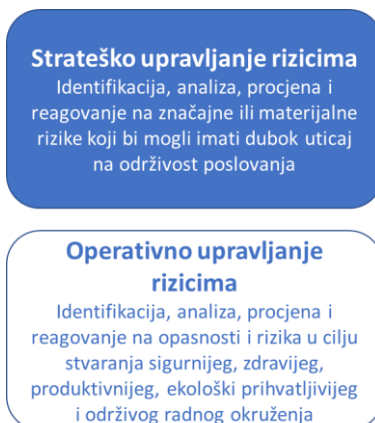
1.2 Šta su ključni/strateški rizici?

„Rizik” se definiše kao mogućnost nastanka nekog događaja koji može uticati na postizanje ciljeva (COSO)³ ili kao uticaj neizvjesnosti na ciljeve (ISO)⁴.

Drugim riječima, rizik je povezan sa neizvjesnošću i izloženošću „nepoznatim” i/ili „neočekivanim” budućim mogućim događajima i uticajem na ciljeve subjekta. Tradicionalno, na rizik se gleda kao na nešto negativno. Međutim, mora se imati na umu da neizvjesni, nepoznati i neočekivani događaji, sa kojima se subjekat suočava, mogu predstavljati i (izgublenu) priliku. Rizik se, dakle, može povezati sa nastankom nepoželjnih događaja, ali takođe i sa propustom da se ostvare povoljni rezultati.

Strateški rizici su rizici koji utiču na strateške ciljeve subjekta ili proizilaze iz strateških pravaca i odluka.

Operativni rizici su glavni rizici koji utiču na sposobnost subjekta da izvrši svoj strateški plan.



Jednostavno rečeno, strateški rizici su rizici koji potencijalno mogu dovesti do velikog gubitka. Takav rizik može nastati iz operativnog rizika ili kombinacije operativnih rizika koji eskaliraju. Takođe, može da potiče od spoljašnjeg događaja, jednog ili više njih, koji demantuju pretpostavke⁵ zaposlenih ili narušavaju strategiju ili strateške ciljeve.

Strateški rizici predstavljaju rizik donošenja odluka na višem nivou, gdje se razmatra opšti strateški plan.

Operativni rizici predstavljaju rizik donošenja odluka na nižem, operativnom nivou, gdje se i sprovodi strateški plan.

U praksi nije lako napraviti jasnu razliku između ove dvije vrste rizika, jer – kao što je gore navedeno – eskalacija ili kombinacija operativnih rizika takođe može uticati na održivost subjekta. Stoga se ponekad pravi razlika između rizika s kojima se može

³ COSO – Komitet sponzorskih organizacija Tredvej komisije (eng. Committeem on Sponsoring Organisation – COSO of the Treadwey Commission)

⁴ ISO – Međunarodna organizacija za standardizaciju

⁵ Svaka strategija je izgrađena na određenim pretpostavkama i nosi određene rizike.

nositi niže rukovodstvo i onih rizika o kojima, zbog svoje prirode i veličine, treba razgovarati i o njima odlučivati na nivou višeg rukovodstva. Posljednji se obično nazivaju „ključnim rizicima” ili „visokim rizicima”. U ovim Smjernicama, ovi rizici će se nazivati „ključni/strateški rizici”.

Rukovodilac subjekta treba da bude informisan o operativnim rizicima, koji mogu uticati na realizaciju strateških ciljeva i prioriteta, odnosno čiji kumulativni uticaj može izazvati strateške rizike i/ili ključne rizike. Takođe, rukovodioci organizacionih jedinica treba da budu informisani o strateškim rizicima subjekta, kako bi prepoznali i procijenili u kojoj su mjeri operativni rizici iz njihove nadležnosti povezani i/ili međusobno uslovljeni strateškim rizicima.



1.3 Šta je upravljanje ključnim/strateškim rizicima?

Upravljanje rizicima se definiše kao proces identifikovanja, procjene i praćenja događaja, koji mogu negativno uticati na ostvarivanje utvrđenih ciljeva i preduzimanje potrebnih mjera radi smanjenja rizika do nivoa razumne uvjerenosti da će ciljevi biti ostvareni. Drugim riječima, to je upravljanje potencijalnim rizicima u cilju predviđanja promijenjenih okolnosti i blagovremenog reagovanja na njih.

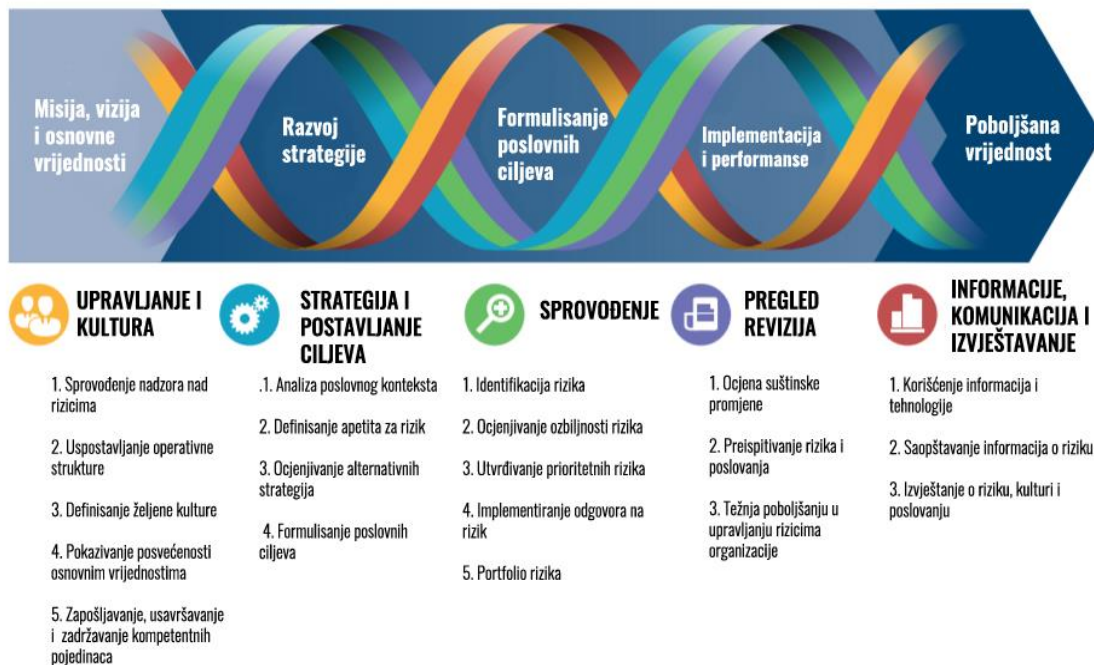
Upravljanje rizicima nije proces koji je izolovan od strategija, planiranja ili donošenja dnevnih odluka, niti se radi o usklađenosti. Upravljanje rizicima je dio organizacione kulture, baš kao i što je donošenje odluka koje utiču na ciljeve dio organizacione kulture.

U novom ažuriranom COSO okviru za Upravljanje rizikom organizacije (Enterprise Risk Management) - upravljanje rizikom organizacije definisano je kao:

»Kultura, sposobnosti i iskustvo, integrisani u proces izrade i implementacije strategije organizacije, na koje se organizacija oslanja prilikom upravljanja rizicima radi stvaranja, očuvanja i realizacije vrijednosti«.

Pomenuta definicija ukazuje na značaj povezanosti strategija i upravljanja rizicima kako bi se ostvarili utvrđeni ciljevi, odnosno očuvala vrijednost subjekta.

Na narednoj slici dat je pregled komponenti i principa koji ukazuju na zahtjeve koje treba primijeniti za uspješno upravljenje rizicima:



Izvor: COSO, *Upravljanje rizicima organizacije: Integriranje sa strategijom i poslovanjem*

Upravljanje ključnim/strateškim rizicima omogućava višem rukovodstvu da razmišlja o budućnosti, a ne samo da se bavi svakodnevnim planovima rada. Ukoliko se zanemari ovaj proces, često će se donositi odluke samo za rješavanje problema i pitanja koja su aktualna, ne uzimajući u obzir širu sliku. Znanje o budućim prijetnjama pomaže u suočavanju sa njima i daje priliku za pripremu mnogo prije nego što problemi isplivaju na površinu.

Ukoliko subjekti ne uspostave efektivan proces upravljanja u vezi sa ključnim/strateškim rizicima, onda se mogu naći u situaciji koja zahtijeva značajna sredstva i vrijeme samo za eliminisanje posljedica ili u situaciji gdje su prilike za razvoj propuštene. Stoga je važno da upravljanje rizicima postane **sastavni dio upravljanja**, a posebno procesa planiranja i donošenja odluka.

Upravljanje rizikom doprinosi organizaciji tako što pomaže rukovodiocu da donese bolje odluke o strategijama i povezanim rizicima sa kojima se organizacija suočava.

Samim tim, doprinosi se povećanju pozitivnih ishoda i smanjenju negativnih iznenađenja.

2. Upravljanje ključnim/strateškim rizicima i odgovornost za njihovo upravljanje

Neke od uloga lica odgovornih za upravljanje rizicima su već definisane u zakonskoj regulativi koja reguliše upravljanje i unutrašnje kontrole⁶, a rukovodilac subjekta može dodatno dodijeliti određene odgovornosti i uloge zaposlenima. Uloge i odgovornosti svih lica uključenih u proces upravljanja rizicima trebalo bi da budu jasno opisane u uputstvima, smjernicama, internim pravilima/procedurama subjekta.

Rukovodilac subjekta je odgovoran za utvrđivanje strateških ciljeva subjekta, izradu i sprovođenje strateških i drugih planova, te programa za ostvarivanje ovih ciljeva. Dakle, rukovodilac subjekta je odgovoran za identifikaciju, procjenu i reagovanje na ključne/strateške rizike.

Rukovodilac subjekta može osnovati **posebno radno tijelo**, sastavljeno od nekoliko viših rukovodilaca, gdje se identifikuju ključni/strateški rizici, diskutuje se o njima i upravlja⁷. U slučaju da subjekat nema radno tijelo, **kolegijumu** subjekta se po potrebi dostavljaju izvještaji u vezi sa upravljanjem ključnim/strateškim rizicima. Pitanja upravljanja rizicima treba da su stalna tačka dnevnog reda kolegijuma.

Rukovodilac subjekta dužan je da odredi lice za koordinaciju procesa upravljanja rizicima (u daljem tekstu: **koordinator za rizike**) u subjektu. Koordinator za rizike pruža podršku rukovodstvu u uspostavljanju integrisanog procesa upravljanja rizicima. Ukoliko je formirano posebno radno tijelo, koordinator može pružiti podršku i u upravljanju ključnim/strateškim rizicima⁸.

Koordinator za rizike nije odgovoran za upravljanje ključnim/strateškim rizicima, već je to odgovornost rukovodioca subjekta.

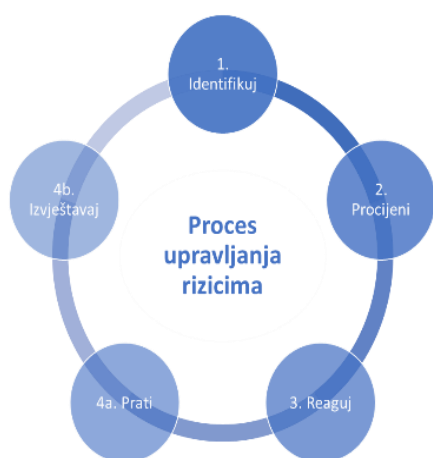
⁶ Zakon o upravljanju i unutrašnjim kontrolama u javnom sektoru

Smjernice za uspostavljanje i sprovođenje procesa upravljanja rizicima, kao sastavni dio Pravilnika o načinu uspostavljanja i unapređenja upravljanja i kontrola u javnom sektoru

⁷ Razmatraju se i ključna pitanja u vezi sa operativnim rizicima i funkcionisanjem procesa upravljanja rizicima.

⁸ On/ona saraduju sa rukovodiocima organizacionih jedinica na identifikaciji njihovih operativnih rizika.

3. Proces, alati i metodologije upravljanja ključnim/strateškim rizicima



Četiri glavne faze u procesu upravljanja ključnim/strateškim rizicima su⁹:

- Identifikacija rizika;
- Analiza i procjena rizika;
- Reagovanje na rizike;
- Praćenje i izvještavanje o rizicima.

Faze su međusobno povezane i potrebno ih je posmatrati kao kontinuirani proces, koji se nikada u potpunosti ne završava, jer su ključni/strateški rizici po svojoj prirodi dinamični i podložni promjenama tokom vremena.

Osnovni preduslov za upravljanje ključnim/strateškim rizicima je da su strateški ciljevi subjekta jasno definisani. Na osnovu ovih ciljeva razmatraju se događaji koji mogu ugroziti ili pospješiti njihovo postizanje, a rukovodstvo treba da odluči o preduzimanju aktivnosti u skladu sa tim.

3.1 Identifikacija ključnih/strateških rizika



Ključni/strateški rizici možda nemaju istorijski presedan i/ili nijesu u nadležnosti subjekta. Signali koji ukazuju na nove ključne/strateške rizike često su slabi ili isprekidani, zbog čega ih je teško otkriti, lako ih je odbaciti i teško ih je protumačiti. Pored toga, ključne/strateške rizike lako je previdjeti, jer se često čine nebitnim, neugrožavajućim ili vrlo malo vjerovatnim — a rukovodstvo može vjerovati da se rizici nadgledaju i da se njima upravlja i kada nije tako.

Prilikom identifikacije ključnih/strateških rizika, predlaže se da se fokus stavi na sljedeća pitanja:

- Šta je potrebno subjektu za postizanje strateških ciljeva i njegovu održivost? (npr. ljudski i finansijski resursi)
- Šta nam je potrebno van subjekta, a nije u našoj nadležnosti, za postizanje strateških ciljeva i njihove održivosti? (npr. usvojeni propis, ponašanje građana)

⁹ Slično kao u glavnim fazama procesa upravljanja operativnim rizikom.

- Koje su pretpostavke razmatrane prilikom odlučivanja o strateškim ciljevima? (npr. ekonomski rast, podrška EU)
- Koliko smo sigurni da će sve što je neophodno biti uspostavljeno kada bude potrebno?
- Šta ako se ispostavi da jedna pretpostavka nije tačna? Kako to utiče na postizanje strateških ciljeva i održivost subjekta?
 - Koliko je vjerovatno da će se to dogoditi?
 - Kako bi to uticalo na subjekat? (pozitivni i negativni uticaji)
 - Da li su ovi uticaji prihvatljivi?
 - Da li će to imati finansijskog uticaja na subjekat?
 - Da li postoje posebne oblasti u koje bi subjekat mogao da uloži (ljudske resurse, IT,...) kako bi smanjio negativne uticaje i spremno dočekaog mogućí scenario?
 - Da li treba promijeniti strateški cilj? Šta bi se desilo ako bi se cilj promijenio?

Ostala opšta pitanja koja treba postaviti da bi se dobila šira slika, odnose se na to kako bi budućnost izgledala za 5-15 godina i kako će to uticati na subjekat.

Identifikacija ključnih/strateških rizika kroz različite perspektive

Prilikom identifikovanja ključnih/strateških rizika, važno je konsultovati se sa širim krugom zainteresovanih strana, jer samo jedna osoba ne može znati sve. Rezultati inkluzivne identifikacije rizika biće uravnoteženiji od onih koji su nastali iz samo jedne perspektive. Na taj način se stvara više holistički pristup.

Preporuka da se razmišlja o pretpostavkama (mogućim događajima) umjesto o rizicima je takođe vrijedna pažnje, jer pretpostavke mogu da preispitaju sve zainteresovane strane. Na ovaj način bi se rizici (koje bismo previdjeli koristeći bilo koji tradicionalni pristup upravljanja rizicima) prepoznali kroz identifikaciju nekonzistentnih ili kontradiktornih pretpostavki.

Razgovor o pretpostavkama za mnoge ljude ima manje negativan prizvuk (može biti prijatniji) nego razgovor o rizicima.

Konsultacije tokom procesa identifikacije ključnog/strateškog rizika mogu se ostvariti uz pomoć:

- Radionica o ključnim/strateškim rizicima (razmjena mišljenja, uz pomoć koordinatora za rizike subjekta);
- Intervjua sa zainteresovanim stranama subjekta;
- Anketa ili upitnika (unutar i van subjekta);
- Rizika i pretpostavki iz strateških dokumenata;
- Izvještaja o sprovođenju strategije;
- Pregleda godišnjih izvještaja o učinku (finansijskih i nefinansijskih);
- Zaključaka i rizika identifikovanih internim i eksternim pregledima subjekta (npr. od strane međunarodnih institucija);
- Rezultata i identifikovanih rizika interne i eksterne revizije;
- Registara operativnih rizika (naročito rizici koji se procjenjuju malom vjerovatnoćom i velikim uticajem, rizici koji se procjenjuju velikom

vjerovatnoćom i velikim uticajem, kao i rizici koji se ponavljaju u registrima rizika različitih organizacionih jedinica);

- Ključnih/strateških rizika identifikovanih u drugim nacionalnim i međunarodnim subjektima;
- Pregleda najvećih rizika koje su pripremile međunarodne konsultantske ili istraživačke firme.

Svi potencijalni rizici su vrijedni razmatranja, ma koliko malo vjerovatni u početku izgledali. Zato učesnike treba ohrabriti da razmišljaju van okvira i predlože praktično svaki rizik koji bi se mogao dogoditi. Najbolje je imati dugačku listu koja se može smanjiti eliminacijom: potcjenjivanje rizika može dovesti do toga da organizacije budu nespremlne.

Primjeri najvećih rizika, koje su identifikovale međunarodne konsultantske i istraživačke firme, mogu se naći na internetu i mogu dati dobru osnovu prilikom identifikacije ključnih/strateških rizika subjekta. U Prilogu A dati su neki od tih primjera.

Kategorije ključnih/strateških rizika

Za provjeru da li su sve vrste rizika uzete u obzir tokom identifikovanja rizika, kao i za podsticanje njihove dalje identifikacije, preporučuje se korišćenje kategorija rizika kao kontrolne liste (nakon inicijalne ideje/identifikacije). Široko korišćena kategorizacija strateških rizika, takođe upućuje na PESTLE¹⁰.

Politički	Ekonomski	Socijalni	Tehnološki	Pravni	Ekološki
<ul style="list-style-type: none"> • Stabilnost Vlade • Vladina politika • Sloboda govora, korupcija • Regulatorna tijela i procesi • Poreska politika, i trgovinska kontrola • Rat • Izbori • Terorizam • Promjene u političkom okruženju 	<ul style="list-style-type: none"> • Faza poslovnog ciklusa • Tekući i projektovani privredni rast • Međunarodni trendovi • Rast poslovanja • Inflacija i kamatne stope • Nezaposlenost i ponuda radne snage • Nivoi raspoloživog dohotka u privredi i raspodjela dohotka • Globalizacija • Vjerovatne promjene u ekonomskom okruženju 	<ul style="list-style-type: none"> • Rast stanovništva i demografija • Zdravstvo, obrazovanje i socijalna mobilnost stanovništva • Stavovi potrošača • Oglašavanje i mediji • Nacionalna i regionalna kultura • Izbor životnog stila i stavovi prema njima • Nivoi zdravlja i obrazovanja • Glavni događaji • Socio-kulturne promjene 	<ul style="list-style-type: none"> • Uticaj novih tehnologija • Izumi i inovacije • Internet i kako on utiče na rad i poslovanje • Licenciranje i patenti • Finansiranje i razvoj istraživanja 	<ul style="list-style-type: none"> • Zakonodavstvo u zemlji • Međunarodno zakonodavstvo • Novi zakoni • Regulatorna tijela • Regulacija životne sredine • Propisi specifični za industriju • Zaštita potrošača 	<ul style="list-style-type: none"> • Ekologija • Međunarodna pitanja životne sredine • Nacionalna pitanja životne sredine • Lokalna ekološka pitanja • Propisi o zaštiti životne sredine • Organizaciona kultura • Moral i stavovi zaposlenih

Još primjera za kategorije rizika koje se mogu uzeti u obzir tokom identifikacije ključnih/strateških rizika može se naći u Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima.

Opis ključnih/strateških rizika

Kao što je navedeno i u Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima identifikovane rizike potrebno je jasno opisati kako bi se osiguralo da svi zainteresovani jednako razumiju isti rizik. Razlika u odnosu na operativne rizike je u tome što su ključni/strateški rizici često opštije opisani.

¹⁰ PESTLE znači: politički, ekonomski, socijalni, tehnološki, pravni i ekološki. Ponekad se dodaje još jedno „E” za etiku.

Rizik se opisuje na način da je to vjerojatnoća/mogućnost da se neka nepovoljna situacija/događaj desi, zbog nekog ili nekoliko razloga, a koji mogu dovesti do negativnih posljedica u izvršavanju osnovnih funkcija subjekta, odnosno negativnih posljedica u ostvarivanju ciljeva tog subjekta.

Dobro je da prije početka identifikovanja mogućih rizika uzmemo u obzir osnovne funkcije tog subjekta i koji su njegovi osnovni ciljevi rada. Svaki subjekat treba da navede najbitnije (a ne sve moguće rizike) koji, ukoliko se ostvare, direktno ugrožavaju rad i ciljeve tog subjekta.

Rizik je najbolje opisan kada se osim vjerojatnoće da se desi neka nepovoljna situacija, navede i razlog (uzrok) zbog čega bi mogla nastati ta nepovoljna situacija (događaj), kao i posljedice koje mogu nastati ukoliko bi se taj nepovoljni događaj/situacija stvarno desio.

I dok je navesti posljedicu poželjno (zbog sagledavanja realnog negativnog uticaja), **navođenje uzroka za nastajanje rizika je presudno:** za shvatanje prirode i suštine rizika, za ocjenjivanje stepena vjerojatnoće nastanka rizika, a najviše zbog predlaganja korektivnih mjera (kojima se utiče na rješavanje uzroka nastanaka rizika).

Primjeri opisa ključnih/strateških rizika, iz registara rizika subjekata u drugim zemljama, dati su u nastavku:

Ključni/strateški rizik	Opis rizika
IT pouzdanost	Postoji stalna potražnja za daljim razvojem postojećih IT sistema zbog operativnih i bezbjednosnih zahtjeva (posebno zbog rizika od sajber napada). Postoji rizik od nedostatka odgovarajućeg nivoa stručnosti i kapaciteta zbog malog tržišta rada, zbog čega ne mogu svi IT sistemi da zadovolje zahtjeve. Posljedica ovoga je da subjekat ne uspijeva da ispuni svoje strateške ambicije i ne može da garantuje kontinuitet svojih usluga.
Zdravlje grada	Kako se gradovi šire, gradi se više zgrada. Ali te zgrade ozbiljno ugrožavaju zdravlje naših gradova, kako na nivou zemljišta (sva ta toksična isparenja koja zgrade emituju) tako i na širem biosferskom nivou, pošto su zgrade glavni emiteri gasova staklene bašte.
Nisko zadovoljstvo zainteresovanih strana i kupaca jer su njihovi interesi loše protumačeni	Da bi se postigli ciljevi, saradnja sa zainteresovanim stranama i kupcima je ključna. Donošenje odluka je ponekad složeno i uključuje mnogo različitih interesa i odnosa. Ovaj visok rizik je u vezi sa odnosom prema kupcima, ministarstvima, opštinama, građanima i inspekcijama.
Klimatski fizički rizici	Možda nećemo moći dovoljno brzo da odgovorimo na fizičke uticaje klimatskih promjena na naše poslovanje, kao i unaprijediti naše proizvode/usluge i krajnja tržišta.
Stručnost i kompetentnost	Postoji rizik da mi možda nećemo moći da privučemo, zadržimo i unapređujemo stručnost potrebnu da transformišemo našu kompaniju i ostvarimo našu strategiju.

Popis „Crnog labuda“ (i planiranje scenarija)

Ključni/strateški rizici mogu proisteći iz takozvanih događaja „**crnog labuda**“ (tj. događaja za koje je vjerovatnoća da će se desiti niska, ali ako se dese, uticaj je visok). Ovi događaji mogu brzo eskalirati i one koji ih nijesu očekivali učiniti zbunjenima, paralizovanim ili sklonim greškama. Prilikom prepoznavanja „crnog labuda“ od zaposlenih se očekuje da razmišljaju o nepoznatom i o moći nepoznatog, naročito o određenoj vrsti događaja kojeg je teško zamisliti, ali koji može biti izuzetno štetan za subjekat. Takav događaj ima tri osobine:



1. Njegova vjerovatnoća je niska i zasnovana na dosadašnjim saznanjima;
2. Iako je njegova vjerovatnoća niska, kada se dogodi, ima visok uticaj;
3. Ljudi ne predvide da će se to dogoditi, ali poslije događaja, svi shvate da su ipak na neki način vidjeli neke signale da će se to desiti. Dakle, prospektivno je nepredvidljivo, ali retrospektivno je predvidljivo.

Primjer događaja „crnog labuda“ je pandemija Covid-19 i reakcije koje je pokrenula. Oštra reakcija političkih lidera i medija nije se mogla predvidjeti i dovela je do potpunog zastoja mnogih aktivnosti.

„Razmišljanje o nezamislivom“ - Ako smo nešto naučili u posljednjih 10 godina, to je da se događaji ekstremnog rizika dešavaju mnogo češće nego što je bilo koji model to predvidio. S obzirom na to, rukovodioci subjekta treba da provedu vrijeme razmišljajući o potencijalnom uticaju ekstremno rizičnih događaja na njihov subjekat, kao što smo iskusili tokom nedavne pandemije.

Preporučuje se planiranje „popisa crnog labuda“ najmanje jednom u dvije godine.

Kako bi se nosio sa ovim neizvjesnostima i donio prave odluke, subjekat može da testira svoju strategiju kroz sagledavanje različitih scenarija, na osnovu stvari koje se znaju o budućnosti i potencijalnog ishoda tih neizvjesnosti. Ova tehnika se zove „**Planiranje scenarija ili razmišljanje o scenariju**“ i koristi se za kreiranje alternativnih vjerovatnih verzija „budućnosti“ koje se mogu koristiti za testiranje strategije subjekta.

U najjednostavnijoj verziji, biraju se dvije neizvjesnosti i dva potencijalna ishoda za svaku od neizvjesnosti, koje bi se mogle desiti do kraja perioda evaluacije (obično pet, deset ili petnaest godina).

Kada se dvije neizvjesnosti ukrste jedna sa drugom (svaka sa dva moguća ishoda), to rezultira sa četiri različite kombinacije.

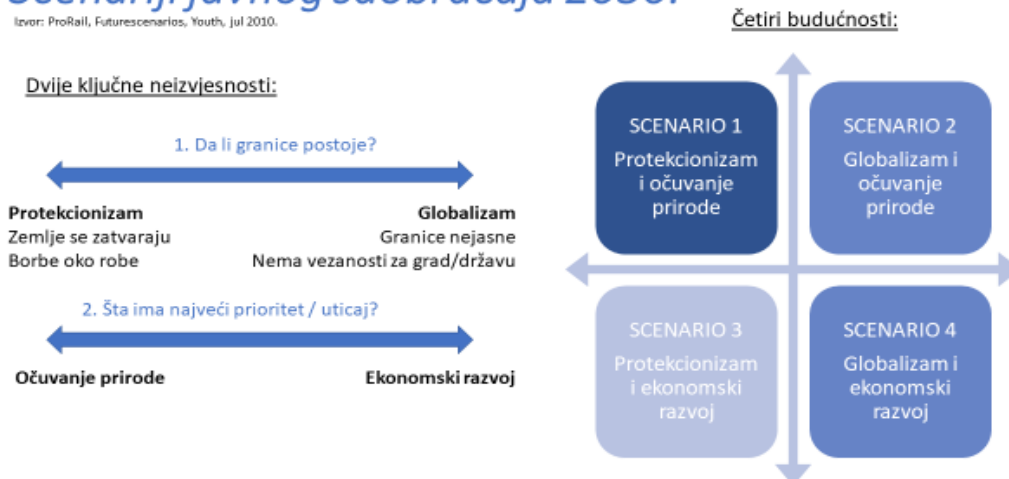
Svaka od ove četiri kombinacije, zajedno sa već identifikovanim trendovima (npr. u analizi životne sredine u strategiji) čini potencijalni scenario, koji je samo vjerovatna verzija budućnosti.

Posljednji korak je da se razmisli o uticajima svake kombinacije i da se dopune budućim stanjem poznatih trendova.

Ovi scenariji se mogu koristiti za testiranje strategije subjekta u odnosu na svaki scenario i da se u skladu sa tim prilagode strateški planovi ili planovi za vanredne situacije, ako je potrebno.

Scenariji javnog saobraćaja 2030.

Izvor: ProRail, Futurescenarios, Youth, Jul 2010.



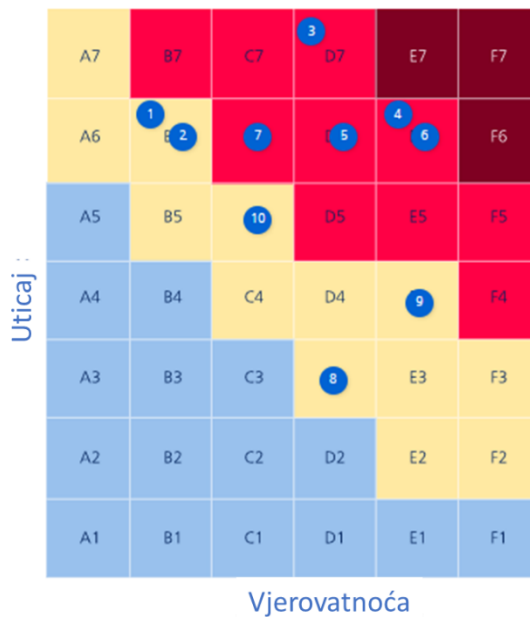
3.2 Procjena rizika

Procjena vjerovatnoće i uticaja identifikovanih ključnih/strateških rizika

Proces kreiranja registra rizika započinje identifikacijom širokog spektra rizika, ali ih onda treba filtrirati kako bi se omogućilo subjektu (rukovodiocu subjekta i kolegijumu) da se koncentriše na rizike sa najvećim potencijalnim uticajem na strateške ciljeve subjekta. Sužavanjem broja rizika (npr. do dvadeset ključnih rizika/prilika) rukovodstvo se fokusira na ono što je važno.

Procjena vjerovatnoće nastanka rizika i njegovog mogućeg uticaja na postizanje strateških ciljeva, omogućava rangiranje rizika, utvrđivanje prioriteta i pružanje informacija rukovodstvu da odluči na koji način će reagovati na rizike. Procjena ključnih/strateških rizika se može vršiti na način opisan u Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima.

U nastavku je primjer matrice rizika sa procjenom 10 ključnih rizika Holandske željeznice:



Rizik 1: Bezbjednost – neispunjavanje naše obavezne brige u slučajevima velikih bezbjednosnih incidenata, koji uključuju putnike i/ili zaposlene

Rizik 2: Neusaglašenost

Rizik 3: Prihodi

Rizik 4: Štednja

Rizik 5: Poslovanje u inostranstvu

Rizik 6: Infrastruktura

Rizik 7: IT (uključujući i sajber bezbjednost)

Rizik 8: Agilnost

Rizik 9: Angažovanje (zdravlje zaposlenih)

Rizik 10: Kapacitet kadrova

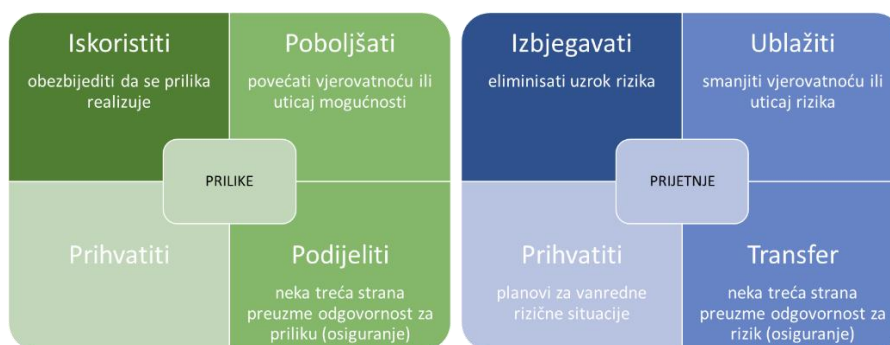
3.3 Reagovanje na rizik

Reagovanje na rizike niske vjerovatnoće najčešće izostaje kao posljedica previše optimističnog pristupa događajima.

Tipičan i čest odgovor na rizik, posebno na rizik niske vjerovatnoće, je poricanje. Ljudi su previše optimistični u pogledu stvari koje su dovoljno daleko u budućnosti, gdje ne mogu da se vide detalji ili kada je vjerovatnoća da će se nešto desiti veoma niska, te smatraju da se to ne može dogoditi. Ovo je poznato kao „pristrasnost optimizma“.

Svrha reagovanja na rizik je da se neizvjesnost okrene u korist subjekta, ograničavanjem prijetnji i korišćenjem pruženih prilika.

Odluku o reagovanju na rizik, donose rukovodioci u okviru svojih nadležnosti.



Mogući načini reagovanja na rizike (pogledajte sliku iznad), detaljnije su opisani u Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima.

Uopšteno govoreći, u pogledu prijetnji, subjekat traži načine da smanji njihovu vjerovatnoću i uticaj na najmanju moguću mjeru (imajući na umu postizanje ravnoteže između troškova i koristi). Događaji „crnog labuda” se ne mogu predvidjeti i stoga je nemoguće da subjekat pokuša da ih spriječi. Međutim, mogu se preduzeti koraci da se njihov uticaj svede na najmanju moguću mjeru, npr. kroz planove za nepredviđene situacije.

Plan za nepredviđene situacije primjenjuje se kada se rizik pojavi, a svrha mu je da se smanji šteta od rizika. Bez pripremljenog plana, puni uticaj rizika mogao bi u velikoj mjeri pogoditi subjekat. Plan za nepredviđene situacije je posljednja linija odbrane od rizika.

Preporučuje se da se izdvoje resursi za izradu planova za nepredviđene situacije za potencijalni razvoj „pesimističkog” scenarija.

Primjeri kontrolnih mjera, kao reagovanje na ključne/strateške rizike, iz registara rizika subjekata u drugim zemljama, dati su u nastavku:

Ključni/strateški rizici	Dodatne mjere kontrole za narednu godinu(e)
Nedostatak/Odlazak zaposlenih	<ul style="list-style-type: none"> • Strateški kadrovski plan po poziciji • Kampanja na tržištu rada • Fokus na zadržavanju zaposlenih • Povećanje kapaciteta obuka
Nisko zadovoljstvo zainteresovanih strana i kupaca, jer su njihovi interesi loše protumačeni	<ul style="list-style-type: none"> • Razgovarati sa rukovodećim timom svake 2 nedjelje o rizicima vezanim za reputaciju i okruženje • Skenirati polugodišnje trendove zadovoljstva i probleme, izložiti ključna (goruća) pitanja rukovodiocu subjekta • Tromjesečni sastanci sa glavnim kupcima
Neusaglašenost sa nacionalnim i institucionalnim propisima	<ul style="list-style-type: none"> • Obezbjediti obuke u svim dijelovima subjekta, kako bi znanje zaposlenih o zakonodavstvu i propisima bilo ažurirano
Bezbjednost hrane	<ul style="list-style-type: none"> • Potrebno je intenzivno i kontinuirano praćenje, npr. za upravljanje rizicima od mikotoksina i biljnih toksina u sastojcima hrane za životinje. • Pripremiti plan za vanredne situacije za slučaj da je zatrovana hrana ušla na tržište (npr. objavljivanje u medijima, direktna komunikacija sa maloprodajnim prodavcima uz uputstva za povlačenje proizvoda sa policia itd.).

Primjer ključnih/strateških rizika i kontrolnih mjera (reagovanja na rizik), u pojedinim crnogorskim subjektima javnog sektora (2021):

Kategorija rizika / naziv	Eksterni rizici
Opis rizika	Ekonomska stabilnost Crne Gore zavisi i od spoljnih razvoja događaja. Ovakav razvoj događaja se ne može promijeniti, ali reakcija i „spremnost“ za to mogu. Primjeri ovih eksternih rizika su slab ekonomski razvoj (u dijelu) zemlje, uticaj klimatskih promjena na proizvodnju i

	<p>cijene, prirodne katastrofe (npr. poplave, zemljotres), pandemije, nestanak električne ili vodovodne infrastrukture, odliv stanovništva u inostranstvo, razvoj sajber valute.</p>
Reagovanje na rizik	<ul style="list-style-type: none"> • Adekvatne makroekonomske politike • Dobro planirane stavke za hitne i nepredviđene budžetske izdatke - budžetska rezerva • Adekvatne procedure za postupanje u slučaju prirodnih katastrofa • Paketi pomoći za ugroženo stanovništvo • Koordinacija sa lokalnim samoupravama u cilju podsticaja lokalnog ekonomskog razvoja.
Kategorija rizika / naziv	IT rizici
Opis rizika	<p>Neki od ključnih procesa ministarstva, u velikoj mjeri zavise od dostupnosti i pouzdanosti IT sistema. Postoji rizik od kvara i prekida mreže na kojoj funkcionišu ključni procesi ministarstva i nedostatak alternativnih sistema. Na ministarstvo bi mogli negativno uticati sajber kriminal ili e-prevara. Narušavanje sajber bezbjednosti može imati različite uzroke, npr. preko napada virusa i malvera, ransomvera i pokušaja neovlašćenog pristupa. Takav napad na sistem može dovesti do pitanja povjerljivosti, integriteta i dostupnosti (podataka) za ministarstvo ili ometanja aktivnosti, negativno utičući na reputaciju, finansije, poslovanje i potencijalno dovesti do troškova vezanih za oporavak i forenzičke aktivnosti. Razlozi za eventualno pojavljivanje ovih IT rizika su da je bezbjednost IT sistema nedovoljna i da interfejsi IT sistema tek treba da budu uspostavljeni ili su slabi. Nedostaju važni kontrolni mehanizmi, a svijest o sajber bezbednosti je niska.</p>
Reagovanje na rizik	<ul style="list-style-type: none"> • Značajna ulaganja u sigurnost mreže informacionih sistema • Integracija IT sistema • Uspostavljeni adekvatni mehanizmi opšte IT kontrole i kontrole aplikacija • Kontinuirana evaluacija i razvoj postojećih i novih informacionih sistema • Revizija IT sistema i njihov razvoj • Povećati svijest zaposlenih o IT rizicima i sajber bezbjednosti

3.4 Praćenje rizika i izvještavanje o rizicima

Pošto se subjekat i njegovo okruženje stalno mijenjaju, treba uspostaviti proces praćenja rizika kako bi se razmotrilo da li je došlo do promjene strateških ciljeva, da li ključni/strateški rizici i dalje postoje, da li su se pojavili novi rizici, da li su se vjerovatnoća i uticaj rizika promijenili, te da li su kontrolne mjere efektivne.

Analizirajte i protumačite signale za ključne/strateške rizike!

Mnogi subjekti vjeruju da se već prate ključni/strateški rizici, i kada to nije tako. Ovo je posebno slučaj kada su u pitanju novi ključni/strateški rizici – razvoj događaja u ranoj fazi, van radara, koji mogu brzo da eskaliraju ili se transformišu u događaje koji narušavaju poslovanje. Važno je pratiti okruženje i tumačiti signale, te pratiti promjene i ublažavanje ključnih/strateških rizika.

Dobra međunarodna praksa je da rukovodeći tim subjekta kvartalno raspravlja o mogućim signalima i statusu ključnih/strateških rizika, kao i da se ohrabruju zaposleni da prijave nove rizike i da preuzmu odgovornost za identifikaciju rizika koji se pojavljuju – kako bi pomogli donosiocima odluka da se prilagode na promjenljive realnosti u procesu i na sprovođenje planova za nepredviđene situacije.

Takozvani **sistem strateškog ranog upozoravanja**¹¹ može podržati praćenje signala. Rano upozorenje uključuje gledanje dalje od pristrasnosti informacija i tumačenja dvosmislenih signala. Ovaj sistem omogućava akterima da jasnije vide čak i pored očigledne konfuzije, da uoče razvoj događaja prije nego što postanu trendovi i da uoče njihove obrasce prije nego što se u potpunosti ispolje.

Rano upozorenje se sastoji od tri povezane mogućnosti: sposobnost da se otkriju i rano procijene promjenljivi uslovi i sposobnost da se na vrijeme reaguje na otkrivene promjene.

Funkcionalni sistem zahtijeva sposobnost prikupljanja prave vrste informacija, tumačenja mogućih značenja signala za subjekat i strategiju subjekta i formulisanja mogućih odgovora za reagovanje.

Upozorenje je signal za nastajanje trenda koji je relevantan za subjekat i/ili njegovu strategiju. Relevantnost može biti pozitivna, negativna ili nedefinisana. Upozorenje može da ukaže na prijetnju, ali i na priliku da se napravi neočekivan napredak.



Često se koristi metafora osmatračnice **na brodu**: signali mogu biti vezani za dešavanja daleko na horizontu, o dešavanjima oko broda, kao i o dešavanjima na palubi i ispod nje. Rano upozorenje nije ograničeno na gledanje daleko „van subjekta”, već i da se gleda okolo i unutar subjekta.

Iako subjekat treba da bude otvoren za svaki signal, takođe je dobro identifikovati i neke **ključne indikatore rizika** (KRI). KRI su aktivnosti ili ishodi koji signaliziraju onome koji upravlja rizikom da određeni rizični događaj postaje manje ili više vjerovatan. Oni takođe mogu ukazivati na to da se rizični događaj već dogodio, kao i na njegov uticaj ili ozbiljnost.

KRI su obično kvantitativni (iako mogu biti i kvalitativni) i prate se u odnosu na gornje i/ili donje granice tolerancije¹².

Kada vrijednost indikatora premaši prag tolerancije, to se posmatra kao abnormalna pojava i kao snažan signal da rizični događaji povezani sa indikatorom postaju mnogo vjerovatniji.

¹¹ EWS – Strategy early warning system

¹² Prag tolerancije, kako je definisano COSO ERM okvirom, je prihvatljivi nivo varijacije u odnosu na postizanje pojedinačnih ciljeva.

Primjeri KRI-a su broj žalbi, fluktuacija zaposlenih, upražnjena sistematizovana radna mjesta, prekoračenje vremena i finansija na projektu, sporovi oko ugovora, zadovoljstvo građana.

Primjer opisa sistema ranog upozorenja holandskog subjekta u javnom sektoru:

Da bi se uspostavio sistem ranog upozoravanja, formiran je „Tim za rano upozoravanje“. Tim su u početku činila dva iskusna službenika u subjektu javnog sektora a proširen je kreiranjem mreže „dopisnika“. Mreža se sastojala od zaposlenih na višim pozicijama u subjektu i eksternih stručnjaka za određene teme iz oblasti kojom se bavi subjekat. Od dopisnika je traženo da prikupe signale na koje je, po njihovom mišljenju, trebalo obratiti više pažnje. Slabi signali se prikupljaju kako bi se pružio uvid u razvoj tri ključna proizvoda/usluge koje subjekt isporučuje. Uvidi se prikupljaju i tumače, a zatim se prezentuju rukovodećem timu (u daljem tekstu: RT) koji treba da odluči kako postupiti sa signalima. Signali koji su smatrani dovoljno važnim praćeni su takozvanim „strateškim istraživanjem“. Strateško istraživanje je interni istraživački projekat kojim se prikuplja više informacija o signalu i obično kao krajnji ishod ima izvještaj o samom signalu, osnovnim trendovima i razvoju i mogućim posljedicama po subjekat. Koraci procesa su:

1. prikupljanje signala,
2. tumačenje signala,
3. izbor signala koji se prezentuju RT-u,
4. prezentacija RT-u,
5. strateški odgovor RT-a, i
6. praćenje odgovora RT-a (u smislu aktivnosti subjekta, praćenja aktivnosti, i povratnog izvještavanja RT-u).

Sistem ranog upozoravanja se brzo razvio u priznat i cijenjen instrument za olakšavanje strateških diskusija na nivou RT-a, npr. pomogao je zaposlenima da daju direktan signal RT-u, bez potrebe da prolaze kroz uobičajne birokratske procedure („prečica“ do dnevnog reda RT-a). Štaviše, sami članovi RT-a su veoma cijenili diskusije koje su vodili kao odgovor na signale, smatrali su da im je to dalo prijeko potrebnog prostora na njihovim sastancima za „pravu“ diskusiju o strateškim neizvjesnostima i unutrašnjim preokupacijama u subjektu i unutar samog RT-a.

Izvještaj o ključnim/strateškim rizicima

Međunarodna praksa je da se u godišnji izvještaj subjekta uključi poglavlje o procesu upravljanja rizicima uopšte, a posebno o upravljanju ključnim/strateškim rizicima. To znači da je izvještaj dostupan unutar, ali i van subjekta. Sve zainteresovane strane biće obaviještene o identifikovanim i procijenjenim ključnim/strateškim rizicima, kao i o mjerama/aktivnostima koje je subjekt preduzeo u izvještajnoj godini, npr. da ublaži rizik ili bude pripremljen u slučaju njegovog nastanka i koliko je bila efektivna reakcija subjekta. U izvještaju takođe treba navesti uticaj promjena u subjektu i njegovom okruženju, da li su neki rizici procijenjeni kao rizici nižeg prioriteta u narednoj godini, da li su se pojavili novi rizici, itd.

U nastavku je dat primjer kako može izgledati dio godišnjeg izvještaja o upravljanju ključnim/strateškim rizicima, kada se vizuelno da pregled ključnih/strateških rizika i „trend“ u izvještajnoj godini. Drugi primjeri vizuelizacije mogu se naći u Prilogu B.

Primjer iz Holandske željeznice (NS, Godišnji izvještaj 2021)

Tema rizika i sklonost ka rizicima	Rizici glavne grupe	Trendovi
① Zaštita <i>Netolerantna</i>	1. Zaštita: Neispunjavanje naše obavezne brige u slučajevima velikih bezbjednosnih incidenata koji uključuju putnike i/ili osoblje.	+
② Usaglašenost <i>Netolerantna</i>	2. Neusaglašenost: Neusaglašenost sa zakonom ili propisima ili prekoračenje važećih normi i vrijednosti.	+
③ Finansije <i>Netolerantna</i>	3. Prihodi: Dugoročni pad prihoda.	-/-
	4. Uštede: Nesprovođenje mjera za uštedu troškova zbog uticaja krize COVID-19.	+
	5. Poslovanje u inostranstvu: Ulaganja koja stvaraju gubitke zbog zastoja u poslovanju u inostranstvu.	-/-
④ Poslovanje <i>Netolerantna</i>	6. Infrastruktura: Neugodnost za kupce uzrokovana nedostatkom infrastrukturnih kapaciteta i kašnjenjem u poboljšanju kvaliteta.	-/-
	7. IT (uklj. sajber sigurnost): Neispunjavanje operativnih i bezbjednosnih zahtjeva u IT sistemima ili onih koje zahtijevaju zakoni i propisi.	=
	8. Agilnost: Pružanje prekasnog unapređenja ili sa nedovoljnim rezultatima.	=
	9. Angažovanje: Psihosocijalni problemi koji proizilaze iz stresa na poslu i mjera povezanih sa COVID-19.	-/-
	10. Kadrovski kapacitet: Nedostatak osoblja kao rezultat male ponude na tržištu rada.	-/-
⑤ Reputacija <i>Neutralna</i>	<i>Glavna grupa rizika se ne odnosi na temu reputacije.</i>	
⑥ Održivost <i>Tolerantna</i>	<i>Glavna grupa rizika se ne odnosi na temu održivosti. Ovo predstavlja velike mogućnosti za Holandsku željeznicu</i>	
+	Trend se poboljšao	
=	Trend je nepromijenjen	
-/-	Trend se pogoršao	

U nastavku je dat primjer iz teksta izvještaja o rizicima i preduzetim mjerama, kao i onima koje treba preduzeti.

Rad u digitalnom svijetu

Postoji rizik da bi na nas negativno mogao uticati sajber kriminal, pa smo nastavili da jačamo našu sajber bezbjednost tokom 2019. godine. Nakon procjene rizika, uvodi se višegodišnji program koji se fokusira na poboljšanje naših mogućnosti za sajber bezbjednost u tri oblasti: informacione tehnologije, operativne tehnologije i laboratorijski sistemi za istraživanje i razvoj. Program se bavi sajber bezbjednošću posmatrajući identifikaciju rizika, zaštitu, otkrivanje, reagovanje i oporavak, te uzimajući u obzir ljude, tehnologiju i dimenzije procesa.

Kako sajber prijetnje nastavljaju da se razvijaju i postaju sve sofisticiranije, kao i povećanje broja digitalnih inicijativa u subjektu, rizik ostaje uprkos napretku koji je postignut u ovoj oblasti.

Dalje mjere ublažavanja podrazumijevaju nastavak sprovođenja našeg višegodišnjeg programa sajber bezbjednosti. Paralelno sa tim, planirani su dodatni projekti za 2020. godinu, uključujući novu kampanju podizanja svijesti o sajber bezbjednosti i uspostavljanju poboljšanog praćenja i izvještavanja.

PRILOG A: Primjeri (globalni, nacionalni ili organizacioni) ključni rizici



Geopolitički rizici	<ul style="list-style-type: none"> • Uspon multipolarnog svijeta • Budući pravac Evropske unije • Odnos Irske, nakon Bregzita, sa Ujedinjenim Kraljevstvom • Oružani sukob, terorizam i hibridne prijetnje
Ekonomski rizici	<ul style="list-style-type: none"> • Ekonomski „ožiljci“ • Javne finansije i finansijski sistem • Nedostatak radne snage, lanac snabdijevanja i ograničenja kapaciteta • Inflacija • Ranjivost koja proizilazi iz kombinacije preduzeća u Irskoj • Promjene u međunarodnim trgovinskim odnosima • Prekid bezbjednog i održivog snabdijevanja energijom
Socijalni rizici	<ul style="list-style-type: none"> • Socijalna kohezija • Stanovanje i održivi razvoj • Migracije i integracije • Demografske promjene • Digitalno isključenje
Ekološki rizici	<ul style="list-style-type: none"> • Klimatske promjene • Gubitak biodiverziteta • Ekstremne vremenske prilike i druge prirodne katastrofe • Pandemije • Antimikrobna rezistencija
Tehnološki rizici	<ul style="list-style-type: none"> • Bezbjednost hrane • Tokovi podataka, skladištenje i bezbjednost • Disruptivna tehnologija • Sajber bezbjednost • Nuklearna kontaminacija

Izvor: Nacionalna procjena rizika Irske, Tabela 1: Strateški rizici – 2021/2022

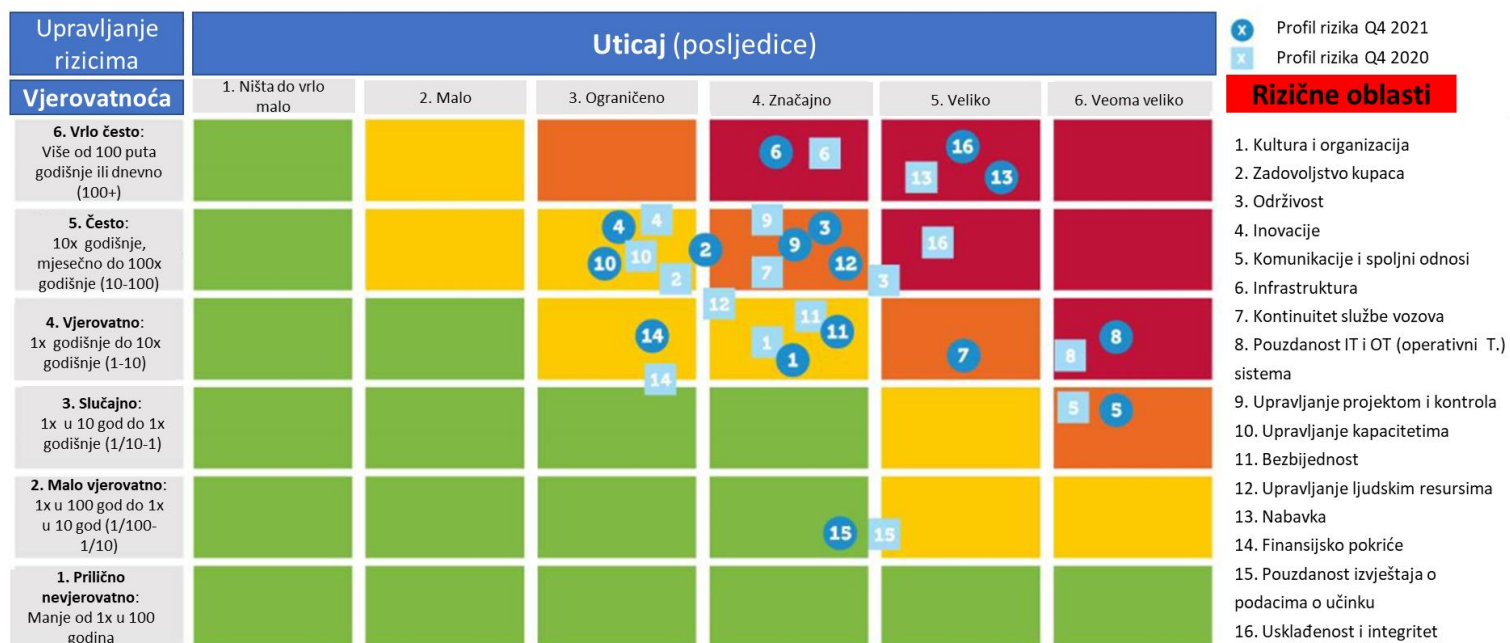
Link: <https://assets.gov.ie/220847/1291534a-9b27-4c05-92ed-d3bd21adc89a.pdf>

Koji su pet najvećih rizika sa kojima se trenutno vaša organizacija suočava?



PRILOG B: Primjeri (vizuelni dio) godišnjeg izvještaja o ključnim/strateškim rizicima

Primjer izvještaja o ključnim rizicima (ProRail, Godišnji izvještaj 2021)



x Profil rizika Q4 2021
x Profil rizika Q4 2020

Kategorije rizika	Najveći rizici	Mjere	Nizak	Srednji	Visok	Vrlo visok
Strateški	Zadovoljstvo zainteresovanih strana i kupaca	<ul style="list-style-type: none"> Trendovi zainteresovanih strana i rizici na strateškom nivou uključeni su u dvogodišnju analizu. U slučaju (prijetećih) pitanja, omogućen je pristup najvišem rukovodstvu/ upravnom odboru. Uključiti uticaj na reputaciju i životnu sredinu u donošenje odluka za (stratešku) mobilnost i bezbjednost, projekte, održavanje i nesreće. Sezonske konsultacije sa prevoznicima. 				
	Strateški programi i projekti	<ul style="list-style-type: none"> Kontrola projekata kroz redovno upravljanje projektima. Kontrola i odgovornost kroz ciklus planiranja i kontrole. 				
	Rizici dobavljača	<ul style="list-style-type: none"> Projekat upravljanja lancem snabdijevanja. Master planiranje i implementacija programa „Ka budućnosti orijentisan rad na prugama“. Analizirati mogućnosti za povećanje kritičnog kapaciteta na tržištu (kroz dodjelu naloga). 				
Operativni	Sigurnost	<ul style="list-style-type: none"> Adekvatna kontrola kroz sistem upravljanja bezbjednošću. Prilagođavanje na osnovu identifikovanih osnovnih bezbjednosnih i sigurnosnih rizika. Program unapređenja, npr. „prevencija samoubistava, i naknadna njega“... Kultura bezbjednosti i sigurnosti. 				
	Kvalifikovano osoblje	<ul style="list-style-type: none"> Obuka i razvoj zaposlenih. Pripravnici. Kampanja na tržištu rada kao dio ProRail šire strategije kampanje – cilj je da bude atraktivan poslodavac. Instalirati pretraživač za zapošljavanje da bi se aktivno „pratili“ potencijalni zaposleni. Program raznovrsnosti. 				

