Sveučilište u Zagrebu
Pravni fakultet

Vedran Krunić

TEMELJNI KONCEPTI UPRAVLJANJA RIZIKOM

ZAVRŠNI SPECIJALISTIČKI RAD

Mentor: prof. dr. sc. Petar Miladin

Zagreb, 2025.

1. UVOD

Tvrdnja da su rizici posvuda oko nas ne iznenađuje i pretpostavka je da će se akademska zajednica i praktičari s njom potpuno složiti. Također, ne iznenađuje ni tvrdnja da su u nekoj mjeri trgovačka društva u poslovanju izložena rizicima (manje ili više ozbiljnim/bitnim). Da je razborito upravljati rizicima, također ne izaziva posebne rasprave ili dileme.

Međutim, ulazeći dublje i detaljnije u materiju upravljanja rizicima, nailazimo na određene pojmove i koncepte koji zahtijevaju dodatnu analizu i pojašnjenja jer o njima ne postoji nesporan konsenzus u stručnoj literaturi i među praktičarima.

Drugo poglavlje ovog rada služi rasvjetljavanju određenih ključnih pitanja u vezi s rizicima i upravljanju rizicima te postavljanju temelja za kasniji detaljniji diskurs o tome kako teče proces upravljanja rizicima. Tako, primjerice, u drugom poglavlju čitatelj može pronaći informaciju o tome jesu li neizvjesnost i rizik sinonimi, što se podrazumijeva pod pojmom rizika, je li rizik isključivo opasnost ili je možda i prilika te postoji li jedna globalna općeprihvaćena definicija upravljanja rizicima. U drugom poglavlju, nakon objašnjenja razlike između tradicionalnog i integriranog upravljanja rizicima, daje se i prikaz propisa iz financijske industrije koji obligatorno zahtijevaju uspostavu „sustava“ upravljanja rizicima. Nakon rasprave o tome koja ih društva moraju obligatorno imati na temelju zakona, čitatelja se navodi na razmišljanje o tome postoji li „skrivena“ opća obveza za trgovačka društva upravljanja rizicima (u nekom obliku, u nekoj mjeri) propisana odredbama hrvatskog zakona kojim su uređena trgovačka društva pri donošenju poduzetničkih odluka, o čemu se detaljno obrazlaže u petom poglavlju ovog rada.

Treće poglavlje sadržava objašnjenja temeljnih koncepata u vezi s upravljanjem rizicima. Ti su temeljni koncepti: sklonost preuzimanju rizika, sposobnost podnošenja rizika, profil rizičnosti, tolerancija na rizike i strategija upravljanja rizicima. Ti pojmovi prepoznati su u hrvatskom pravnom sustavu u dijelu pravila koja reguliraju „financijsku industriju“. Bez razumijevanja tih temeljnih koncepata u kontekstu upravljanja rizicima nemoguće je tvrditi upravlja li društvo rizicima na odgovarajući način. Također, bez unificiranog pristupa tumačenju tih pojmova teško je razumjeti/raspravljati/dokazivati je li član uprave društva uime društva kod donošenja poduzetničkih odluka preuzeo „preveliki rizik“ protivno načelu

poslovne prosudbe. Budući da su ti temeljni koncepti „okvir“ koji se reflektira i utječe na sam proces upravljanja rizicima, ne iznenađuje da su oni i objašnjeni prije prezentiranja odabranih modela upravljanja rizicima (a modela koji sadržavaju pravila o procesu upravljanja rizicima).

Temeljni je cilj četvrtog poglavlja utvrditi općenito prihvaćene „zajedničke“ faze/etape/korake/aktivnosti što čine neizostavan dio procesa upravljanja rizicima i to bez obzira na to o kojoj je točno vrsti rizika riječ (opći modeli upravljanja rizicima). S tim ciljem analiziraju se i međusobno uspoređuju dva najviše korištena modela upravljanja rizicima kako bi se utvrdile zajedničke etape procesa upravljanja rizicima. Kao i u svakodnevnom životu, da bi se određeni „problem“ mogao držati pod kontrolom ili pokušao riješiti, potrebno je prvo utvrditi da on postoji. Stoga, u kontekstu procesa upravljanja rizicima, rizici se najprije moraju identificirati kako bi se na njih mogao u odgovarajućem trenutku primijeniti prikladan „odgovor“ odnosno mjera. S obzirom na to da svi rizici nisu jednako bitni te uzimajući u obzir to da su novčani, vremenski i ljudski kapaciteti u pravilu ograničeni, faze procjene bitnosti odnosno analize rizika te njegove prioritizacije prethodit će odabiru mjere koja se treba primijeniti na rizik.

Peto poglavlje najbolje je najaviti na pomalo laički način inspirirajući se primjerima iz svakodnevnog života s kojima se svi možemo najlakše poistovjetiti. Takvi primjeri služe tomu da bi čitatelj u konačnici mogao lakše pristupiti proučavanju predmetne materije bez straha od možda naizgled kompleksne materije što se tiče izričaja i korištenih pojmova. Naime, katkad posjet doktoru opće prakse možda nije dovoljan zbog toga što rješavanje određenog zdravstvenog problema zahtijeva stručni pregled specijalista koji je usko specijaliziran za određeno područje materije. U kontekstu upravljanja rizicima katkad opći modeli upravljanja rizicima neće biti dostatni, dovoljno jasni ili precizni ili prilagođeni za upravljanje pojedinim vrstama rizika. U nekim slučajevima možda će nedostajati samo mala nadogradnja ili sitne dorade u okviru općih modela. U tom smislu, a s ciljem razumijevanja procesa upravljanja rizicima i u područjima određenih „specijalizacija rizika“, potrebno je „proviriti“ izvan općih modela upravljanja svim vrstama rizika i zakoračiti u modele upravljanja kvalitetom, projektom i usklađenošću, zatim digitalne operativne otpornosti i rada na daljinu, što su također područja obilježena važnošću upravljanja rizicima.

U šestom poglavlju objašnjava se važnost (internog i eksternog) komuniciranja o rizicima kao sastavnog elementa procesa upravljanja rizicima. U kontekstu eksternog izvještavanja o upravljanju rizicima, autor ovog rada pomiče i usmjerava pravnički diskurs prema ekonomskoj znanosti, računovodstvu i financijskom izvještavanju (financijska izvješća). Naime, predmet interesa ovog rada ujedno je i identificirati „ekonomske“ izvore informacija o rizicima (uključujući i o njihovu upravljanju) u praksi na hrvatskom tržištu kapitala. U tom kontekstu razmatra se koja je uloga izvješća poslovodstva, komentara poslovodstva, bilješki uz financijske izvještaje te prospekata vrijednosnih papira kao izvora takvih informacija. Prospekt javne ponude i/ili uvrštenja vrijednosnih papira, iako je „pravni dokument“, zaslužuje biti naveden u „ekonomskom“ poglavlju ovog rada zbog toga što se takvim prospektom omogućuje sekundarno trgovanje vrijednosnim papirima ili prikupljanje „svježeg“ inicijalnog kapitala na tržištu kapitala (ovisno o okolnostima konkretnog slučaja), pa i ne začuđuje da upravo zbog elementa prikupljanja kapitala od javnosti (a što uključuje i male neprofesionalne ulagatelje) o komuniciranju u vezi s rizicima, tj. o načinu i kvaliteti predstavljanja rizika u prospektu postoje posebna pravila ujednačena na razini prava Europske unije.

Cilj je sedmog poglavlja privući što veći krug zainteresiranih čitatelja. Stoga, sedmo poglavlje promatra upravljanje rizicima u širokom poduzetničkom kontekstu, odnosno u kontekstu donošenja poduzetničkih odluka, i to kroz prizmu pravila poslovne prosudbe. Neovisno o tome čime se trgovačko društvo bavi, odnosno pripada li financijskom sektoru ili ne, članovi uprave i nadzornog odbora / upravnog odbora dioničkog društva ili društva s ograničenom odgovornošću moraju voditi računa o „prevelikim“ rizicima jer ih u skladu s pravilima poslovne prosudbe ne smiju preuzimati. S obzirom na to da pojam prevelikih/prekomjernih rizika izaziva mnogobrojne rasprave, u sedmom poglavlju predlažu se točke/kriteriji usporedbe koji služe utvrđivanju prekomjernosti rizika.

2. OPĆENITO O POJMU RIZIKA I UPRAVLJANJU RIZICIMA

2.1. Neizvjesnost i rizik

Hoće li konj pobijediti u utrci konja, primjer je neizvjesnosti. Može se samo nagađati, odnosno pokušati odrediti koja je vjerojatnost njegove pobjede. Ako je on već otprije pobjeđivao, moglo bi se tvrditi da je vjerojatnost njegove pobjede „veća". Neizvjesnost hoće li konj pobijediti može, ali i ne mora biti rizik. Ako smo se, primjerice, kladili u pobjedu nekog konja, tada će neizvjesnost pobjede tog konja biti rizik gubitka uloženog novca u okladi, odnosno rizik dobitka. Međutim, ako se nismo kladili, nismo vlasnici konja koji se natječu, nemamo nikakav imovinski interes ni neki drugi cilj na koji utječe ishod takve utrke, onda neizvjesnost za nas (tj. za naše ciljeve) nije rizik.[1]

Navedeni primjer uvodi nas u razmatranje odnosa između pojmova „neizvjesnost" i „rizik". S time u vezi, ključno pitanje na koje treba dati odgovor jest kada neizvjesnost postaje rizikom i za koga.

Naime, svi rizici jesu neizvjesni, ali svaka neizvjesnost nije rizik.[2] Iz te tvrdnje jasno proizlazi da su neizvjesnost i rizik očigledno povezani (engl. *clearly related*), ali nisu istoznačnice.[3]

U situacijama potpune izvjesnosti kada postoji samo jedan mogući ishod, ne postoje rizici zbog toga što rizici proizlaze isključivo iz neizvjesnosti.[4] Drugim riječima, bez postojanja neizvjesnosti i ne možemo govoriti o eventualnom (ne)postojanju rizika.

Neizvjesnost može, ali ne mora ujedno biti i rizik. Stoga, rizik je pojam koji je u svom opsegu uži/specijalniji od pojma neizvjesnosti. Svaka neizvjesnost neće biti upisana u registar rizika koji vodi društvo niti će biti u fokusu upravljanja rizicima. Nadalje, svaka neizvjesnost neće biti predmetom rasprave stručnjaka o njezinoj materijalnosti, javnog objavljivanja zainteresiranim dionicima ili internog izvještavanja o rizicima.[5]

Treba osvijestiti što čini neizvjesnost rizikom, odnosno koja su to njezina ključna obilježja. Odgovor na to pitanje dao je američki ekonomist Frank Knight u svojem djelu „Rizik, neizvjesnost i profit" čime je 1921. prvi definirao razliku između neizvjesnosti i rizika.[6] Prema

[1] Moran, A., Agile Risk Management, Zurich, 2014., str. 18.
[2] Hillson, D., The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk, London, 2016., str. 2.
[3] *Ibid.*
[4] Miloš Sprčić, D., Dvorski Lacković, I., Upravljanje rizicima, Jastrebarsko, 2023., str. 5.
[5] Hillson, D., *op. cit.* u bilj. 2, str. 2.
[6] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 4.

Franku Knightu, rizik je ona neizvjesnost koja je mjerljiva.[7] „Kada za neki događaj možemo pretpostaviti vjerojatnost njegove pojave, radi se o riziku.“[8] Drugim riječima, ako je neizvjesnost nemjerljiva, ona nije rizik.

Slijedom navedenog teorijskog pristupa Franka Knighta, neizvjesnost je širi pojam upravo zbog toga što može biti mjerljiva i nemjerljiva, a rizik (prema Franku Knightu) može biti samo ona neizvjesnost koja je mjerljiva. Iako se u teoriji takav pristup može činiti jasnim i korisnim, upitna je njegova pragmatičnost u praksi.[9]

S obzirom na to da je od 1921. pa do danas prošlo čitavo stoljeće, a znanosti napreduju, teorijsko tumačenje Franka Knighta u kontekstu odnosa između neizvjesnosti i rizika treba nadopuniti dodatnim razlikovnim kriterijima.

Uzmimo, primjerice, društvo osnovano u Republici Hrvatskoj koje u svom vlasništvu ima isključivo hotel koji se nalazi u Zagrebu i jedini izvor prihoda društva proizlazi iz poslovanja hotela u Zagrebu. Društvo bi moglo izračunati neizvjesnost pojave tornada u Sjedinjenim Američkim Državama i takva bi neizvjesnost bila mjerljiva. Naime, pitanje je u kojoj bi mjeri izračun neizvjesnosti bio točan, ali načelno govoreći, neizvjesnost pojavljivanja tornada u SAD-u mogla bi se hipotetski izračunati/izmjeriti ili od stručnjaka nabaviti kao znanstveni podatak. Ključno je pitanje u tom kontekstu, je li mjerljiva neizvjesnost pojave tornada u SAD-u rizik za društvo iz Republike Hrvatske.

Razumno je pretpostaviti da upravljanje rizicima ne obuhvaća upravljanje svim mjerljivim neizvjesnostima, već samo onima koje su na neki način i u nekoj dostatnoj mjeri relevantne za konkretnu osobu (fizičku ili pravnu). Stoga, mjerljiva se neizvjesnost može podijeliti u dvije kategorije: ona koja je u određenoj mjeri relevantna (bitna ili ozbiljna) za osobu koja upravlja rizikom i ona koja je za nju irelevantna (engl. *uncertainties that matter to us and those that do not matter*).[10] Na tragu takva razmišljanja, neizvjesnost u vezi s pojavom tornada u SAD-u nije rizik za društvo koje ostvaruje prihode isključivo od poslovanja hotela

[7] Hillson, *op. cit.* u bilj. 2, str. 2.
[8] *Cit.*, Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 4.
[9] Hillson, D., *op. cit.* u bilj. 2, str. 2.

[10] *Ibid.*, str. 3.

koji se nalazi u Zagrebu jer takva mjerljiva neizvjesnost nije relevantna za društvo da bi „prerasla“ u kategoriju rizika.

Rizik je mjerljiva neizvjesnost koja je relevantna u smislu toga što potencijalno može utjecati na postizanje ciljeva fizičke ili pravne osobe.[11] U kontekstu društava ciljevi su, primjerice, završetak poslovne godine s određenim iznosom dobiti, ostvarenje ciljeva održivosti (smanjenje ispuštanja CO_2 u prirodu, korištenje isključivo recikliranog papira), povećano zadovoljstvo klijenata, lansiranje inovativnog proizvoda ili više njih, proboj na inozemno tržište, kontinuirana usklađenost s pravnim propisima, ali i internim aktima društva. S druge strane, neizvjesnost pojave tornada u SAD-u za hotel u Zagrebu ne bi bila relevantna neizvjesnost jer je teško pretpostaviti (na temelju okolnosti koje su dane za primjerični slučaj) da bi tornado u SAD-u mogao utjecati na ostvarenje određene razine dobiti društva (financijskog cilja) ili nekog drugog nefinancijskog cilja društva koje ima u vlasništvu isključivo hotel u Zagrebu (npr. smanjenje ispuštanja CO_2 u prirodu, korištenje isključivo recikliranog papira). Uzimajući u obzir kriterij „relevantnosti“, rizik je mjerljiva neizvjesnost koja može utjecati na ostvarenje cilja/ciljeva ako se neizvjesnost ostvari.[12]

Nadalje, iz same sintagme „upravljanje rizicima“ proizlazi da se rizikom kao mjerljivom neizvjesnosti može upravljati, za razliku od nemjerljive neizvjesnosti kojom se upravo zbog svoje nemjerljivosti ne može upravljati.[13] To znači da se mjerljiva neizvjesnost kao rizik (upravljanjem) može pokušati smanjiti/prilagoditi/održavati na određenoj razini. U tom kontekstu društvo može implementirati određene mjere (odgovore na rizik, tretmane, reakcije, kontrole) s ciljem održavanja rizika na prihvatljivoj razini (mjerljivog) stupnja neizvjesnosti. S druge strane, neizvjesnošću koja nije mjerljiva ne može se upravljati.[14] Naime, ako je neizvjesnost nemjerljiva, onda ju je i nemoguće održati na odgovarajućoj/željenoj razini, odnosno stupnju neizvjesnosti (njome upravljati) upravo zbog izostanka mogućnosti njezina mjerenja prije i nakon odgovora na rizik.

---

[11] *Ibid.*, str. 4.
[12] *Ibid.*, str. 4.
[13] Tako i Ramakrishna, S., Enterprise Compliance Risk Management: An essential Toolkit for Banks and Financial Services, Singapore, 2015., str. 213–239.
[14] KC, Megh, Relationship between Risk and Uncertainty, 2020., https://www.researchgate.net/publication/340503291_Relationship_between_Risk_and_Uncertainty (posljednji pristup 27. veljače 2024.)

Slijedom teorijskog tumačenja Franka Knighta, zatim kriterija relevantnosti i sintagme „upravljanja rizicima“, zaključuje se da su rizici samo one neizvjesnosti koje su mjerljive, relevantne za ciljeve pravne osobe te kojima se može i upravljati.

Napominje se da treba voditi računa da u teoriji i praksi zasad ne postoji univerzalno prihvaćena definicija rizika, već je riječ o čitavu spektru definicija rizika[15], pa stoga teoriju koja rizik definira u odnosu na neizvjesnost treba promatrati samo kao jedan od mogućih pristupa razmatranja pojma rizika koji ne isključuje i ostale moguće pristupe koji rizik ne definiraju u odnosu na neizvjesnost.[16]

2.2. Opasnost i prilika

Iako je učestalo u ljudskom poimanju rizika te u dostupnoj literaturi da se rizik veže pretežno uz negativan utjecaj na ostvarenje ciljeva, treba voditi računa o tome da to nije nužno uvijek tako.[17]

Naime, ako se rizik promatra kao devijacija od cilja, odnosno ciljane vrijednosti (engl. *target value*), takva devijacija iliti otklon može se potencijalno kretati u pozitivnom, ali i u negativnom smjeru.[18] Stoga, ako se uzimaju u obzir samo negativni utjecaji, takva je definicija rizika definicija u užem smislu (engl. *narrower sense*). U slučaju uzimanja u obzir negativnog i pozitivnog utjecaja, takva je definicija rizika bila definicija rizika u širem smislu (engl. *broader sense*).[19]

Može se postaviti pitanje koji je ispravniji pristup proučavanju rizika – treba li se rizik proučavati u užem ili u širem smislu. Nema jednoznačnog odgovora na to pitanje. Naime, u stručnoj literaturi postoje autori koji uzimaju u obzir i prilike koje proizlaze iz rizika[20], ali i autori koji stavljaju naglasak isključivo na negativne učinke rizika.[21]

---

[15] Kampmann, A., The Role of Storytelling for Communication in Risk Management: A Conceptual and Experimental Study, Baden-Baden, 1. izdanje, 2021., str. 32.
[16] Hopkin, P., Thompson, C., Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management, London, 6. izdanje, 2022., str. 16 i 17.
[17] Vidi primjerice u Moran, *op. cit.* u bilj. 1, str. 18, i Bonime-Blanc, The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency, London, 1. izdanje, 2014., str. 41 i 42.
[18] Kampmann, A., *op. cit.* u bilj. 15, str. 33.
[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid.*

Negativan utjecaj rizika na ostvarenje ciljeva zove se čisti rizik (engl. *pure risk*)[22] ili prijetnja (engl. *threat*)[23]. Obilježje je tradicionalnog sustava upravljanja rizicima da je ono usmjereno isključivo na negativne učinke rizika[24] te na uzročnike neželjenih događaja[25], što implicira da tradicionalni sustav upravljanja rizicima ne prepoznaje pozitivnu stranu rizika u vidu prilika koje rizik potencijalno donosi.

Primjer je čistog rizika rizik „održivosti" kako je definiran Uredbom (EU) 2019/2088 Europskog parlamenta i Vijeća od 27. studenoga 2019. o objavama povezanim s održivosti u sektoru financijskih usluga. Prema toj uredbi rizik održivosti jest „okolišni, socijalni ili upravljački događaj (ili uvjet) koji, ako do njega dođe, može uzrokovati stvaran ili potencijalno negativan bitan učinak na vrijednost ulaganja".[26] Imajući na umu da definicija rizika održivosti uzima u obzir samo stvaran ili potencijalan „negativan bitan učinak" na određeni cilj (u konkretnom slučaju cilj je vrijednost ulaganja), razvidno je da je europski zakonodavac definiranju predmetnog rizika održivosti u konkretnom slučaju pristupio na uži način (rizik održivosti kao čisti rizik ili prijetnja).

Nadalje, informacijsko-komunikacijsko-tehnološki (IKT) rizik definiran je u Uredbi (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor kao razumno prepoznatljiva okolnost koja se odnosi na upotrebu mrežnih i informacijskih sustava, koja, ako do nje dođe, može „dovesti do negativnih učinaka" u digitalnom ili fizičkom okružju te time „ugroziti" sigurnost mrežnih i informacijskih sustava, svih alata ili procesa koji ovise o tehnologiji, operacija i procesa ili pružanja usluga.[27] Uzimajući u obzir izričaj te definicije, sasvim je razvidno da je IKT rizik definiran na uži način u smislu da je prijetnja ciljevima u vezi sa sigurnošću ili ih ugrožava.

Međutim, utjecaj neizvjesnosti na ostvarenje ciljeva može biti i pozitivan, što je prepoznato i u različitim standardima/modelima upravljanja rizicima.[28] Prilika je potencijalno

[22] Hopkin, P.; Thompson, C., *op. cit.* u bilj. 16, str. 13.
[23] Hillson, D., *op. cit.* u bilj. 2, str. 4.
[24] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 59.
[25] Ramakrishna, S., *op. cit.* u bilj. 13, str. 213–239.
[26] Čl. 2., toč. 22. Uredbe (EU) 2019/2088 Europskog parlamenta i Vijeća od 27. studenoga 2019. o objavama povezanim s održivosti u sektoru financijskih usluga (Tekst značajan za EGP).
[27] Čl. 3., toč. 5. Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (Tekst značajan za EGP).
[28] Hillson, D., *op. cit.* u bilj. 2, str. 5.

pozitivan utjecaj rizika na ciljeve društva.[29] Upravljanje rizicima kojima se razmatraju ne samo potencijalne prijetnje i gubitci već i prilike za stvaranje vrijednosti jedno je od obilježja integriranog upravljanja rizicima.[30] Dualna priroda rizika sugerira da on može u isto vrijeme biti i kombiniranog pozitivno-negativnog učinka.[31]

Rizik gubitka ključnog kupca primjer je čisto negativnog utjecaja na ciljeve društva. Naime, teško je zamisliti da bi gubitak ključnog kupca mogao imati pozitivne utjecaje na ciljeve društva. Prevelika potražnja kupaca za proizvodom koji društvo proizvodi i prodaje može imati pozitivan utjecaj na financijski položaj društva ako ono uspije uspješno i kvalitetno odgovoriti na tržišnu potražnju (veća prodaja – veći prihodi – pretpostavka veće dobiti zbog obujma proizvodnje). Međutim, prevelika potražnja potencijalno može povećati rizik nastanka problema/zastoja/grešaka u proizvodnji ili lancu nabave u okviru kojeg se nabavljaju sirovine za proizvodnju predmetnog proizvoda (u slučaju da društvo nije spremno, odnosno nema kapaciteta uspješno u kontekstu vremena i kvalitete odgovoriti na takvu potražnju). Naime, to se u konačnici može negativno odraziti na reputaciju društva (greške u proizvodnji, slabija kvaliteta proizvoda zbog povećane potražnje).[32] Stoga, iz prethodnog primjera vidljivo je da rizik može u isto vrijeme imati potencijalno pozitivan učinak na jedan cilj društva (npr. financijski – povećanje prihoda), ali i potencijalno negativan utjecaj na neki drugi cilj društva (npr. održavanje pozitivne reputacije društva).

2.3. Nepostojanje univerzalno prihvaćene definicije upravljanja rizicima

Većina društava upravlja rizicima u nekoj mjeri.[33]

S obzirom na to da je upravljanje rizicima u određenoj mjeri (više ili manje) prihvaćeno u praksama društava, potrebno je osvrnuti se na pojam „upravljanje rizicima“ na način da se utvrdi što upravljanje rizicima obuhvaća. Jesu li ključne odrednice upravljanja rizicima ljudi

[29] *Ibid.*
[30] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 59.
[31] ISO (Međunarodna organizacija za normizaciju), ISO 31000, Upravljanje rizicima – Smjernice, Geneva, 2. izdanje, 2018. (dalje u tekstu: ISO 31000:2018), t. 3.1., str. 1.
[32] COSO (Committee of Sponsoring Organizations of the Treadway Commission), Enterprise Risk Management: Integrating with Strategy and Performance, 2017., str. 9.
[33] Hardy, K., str. 38, Enterprise Risk Management: A Guide to Government Professionals, 1. izdanje, New York, 2014., str. 38.

(zaposlenici), operativno ustrojstvo, posebno izdvojene i neovisne funkcije upravljanja rizicima, komunikacija (interna i eksterna), identificiranje rizika i procjena rizika, definiranost procesa, odgovori na rizik, metode identificiranja rizika, mapa rizika, vrijednosti, linije podjela odgovornosti, politike, povelje? Može li se upravljanje rizicima promatrati kao „kombinacija aktivnosti koje minimiziraju negativan utjecaj izloženosti različitim vrstama financijskih, strateških i operativnih rizika na očekivane poslovne ciljeve i rezultate, a time i vrijednost poduzeća“?[34]

Upravljanje rizicima počelo se razvijati u Sjedinjenim Američkim Državama u djelatnosti osiguranja 60-ih godina 20. stoljeća, nakon čega se širi na ostale djelatnosti (većinom bankarstvo i energetiku) te je 1993. u SAD-u imenovan prvi glavni menadžer za rizike.[35]

S obzirom na to da u teoriji i praksi ne postoji jedna općeprihvaćena definicija rizika, ne iznenađuje posljedično tomu da ne postoji ni jedna globalno prihvaćena definicija pojma „upravljanje rizicima“.[36] Nije nedostatak definicija ono što čini problematičnim pokušaj definiranja upravljanja rizicima na jedinstven i univerzalan način, nego upravo proliferacija mnoštva različitih korištenih definicija koje se mogu naći u literaturi.[37] Drugim riječima, upravo je zbog postojanja mnoštva različitih definicija teško izabrati (ili kreirati) jednu koja bi uspjela obuhvatiti sve ili pretežnu većinu elemenata ili obilježja kojom se različite definicije koriste kako bi definirale pojam upravljanja rizicima.

Tako, primjerice, standard upravljanja rizicima ISO 31000 koji je 2018. izdala Međunarodna organizacija za normizaciju[38] (dalje u tekstu: ISO 31000:2018) upravljanje rizicima definira kao koordinirane aktivnosti kojima se vodi i nadzire organizacija s obzirom na rizike.[39]

[34] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. XVI.
[35] *Ibid.*, str. 58.
[36] Kampmann, A., *op. cit.* u bilj. 15, str. 34.
[37] Yoe, C., Principles of Risk Analysis: Decision Making Under Uncertainty, 2. izdanje, Boca Raton, 2019., str. 47.
[38] Vidjeti više o Međunarodnoj organizaciji za normizaciju na https://www.iso.org/about-us.html.
[39] Toč. 3.2. ISO 31000:2018.

COSO[40] ERM standard o integriranom upravljanju rizicima koji je objavljen 2004., a nadopunjen 2017.[41], integrirano upravljanje rizicima (engl. *Enterprise risk management* – ERM) definira kao kulturu, sposobnosti i prakse koje su integrirane sa strategijom i performansama na koje se organizacije oslanjaju u upravljanju rizicima s ciljem stvaranja, zaštite i realiziranja vrijednosti.[42]

Nadalje, Zakon o leasingu upravljanje rizicima definira kao sveobuhvatan proces, odnosno skup postupaka, metoda i tehnika za identificiranje, mjerenje i procjenu te upravljanje i ovladavanje rizicima kojima je *leasing* društvo izloženo ili bi moglo biti izloženo u svom poslovanju, uključujući i izvještavanje o njima.[43] Sveobuhvatan i učinkovit sustav *leasing* društva upravljanja rizicima mora uključivati najmanje: strategije, politike, postupke i mjere upravljanja rizicima, zatim tehnike mjerenja rizika te podjelu odgovornosti u vezi s upravljanjem rizicima.[44]

Iz navedenih triju definicija uočava se kako se upravljanje rizicima može promatrati na različite načine, i to kroz aktivnosti, kulturu, sposobnosti, prakse, proces, ali i kao sveobuhvatan i učinkovit sustav.

Određene definicije upravljanje rizicima vide kao proces u službi donošenja odluka društva (naglasak na svrsi / krajnjem cilju upravljanja rizicima), dok druge vide upravljanje rizicima kao strukture koje omogućuju upravljanje opasnostima i prilikama (naglasak na organizaciji upravljanja rizicima) ili kao skup mjera kojima se nastoji smanjiti, kontrolirati ili regulirati rizik (alati koji su dostupni u kontekstu upravljanja rizicima; npr. ugovori o izvedenicama, ugovori o osiguranju).[45]

Upravljanje rizicima može se promatrati i kao „važan element učinkovitog i sveobuhvatnog sustava korporativnog upravljanja“ [46], što upućuje na to da ono može činiti dio nekog drugog šireg sustava poput sustava korporativnog upravljanja.

[40] COSO – Committee of Sponsoring Organizations of the Treadway Commission.
[41] Vidjeti više na https://www.coso.org/guidance-erm.
[42] COSO, *op. cit.* u bilj. 32, str. 109.
[43] Čl. 69., st. 1. Zakona o leasingu (NN, br. 141/13).
[44] Čl. 69., st. 2. Zakona o leasingu (NN, br. 141/13).
[45] Yoe, C., *op. cit.* u bilj. 37, str. 47.
[46] Cit., Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. XVI.

Stoga, umjesto pokušaja formuliranja univerzalne definicije upravljanja rizicima, neki autori zagovaraju „procesni“ pristup, odnosno identificiranje onih aktivnosti koje su zajedničke svim modelima upravljanja rizicima poput faze identifikacije rizika, procjene bitnosti rizika, primjene odgovora na rizik, nadzora (kontinuirane evaluacije) te komuniciranja/izvještavanja o rizicima.[47] Za potrebe ovog rada autor se odlučio za stavljanje fokusa na „procesni“ pristup koji se temelji na fazama/koracima/etapama koji su u određenoj mjeri zajednički različitim modelima upravljanja rizicima te na komunikaciji/izvještavanju što je ujedno i protkano u svim navedenim fazama.

2.4. Razlika između tradicionalnog i integriranog pristupa

Tradicionalni pristup upravljanju rizicima koji je bio dominantno korišten u upravljanju rizicima do početka 21. st. temeljio se na izoliranom upravljanju rizicima u „silosima“.[48] U okviru takva tradicionalnog pristupa upravljanju rizicima u društvu ne postoji organizacijska jedinica posebno zadužena za holističko (cjelovito) upravljanje rizicima, nego se rizicima upravlja u različitim organizacijskim jedinicama koje usko razmatraju samo one rizike kojima su izložene bez analize povezanosti s ostalim vrstama rizika koje se pojavljuju u društvu (odnosno drugim organizacijskim jedinicama).[49] Na takav način izostaje sustavno razumijevanje međuovisnosti i korelacije među rizicima, odnosno izostaje precizna slika izloženosti rizicima na razini cijelog društva. Nedostatak je tradicionalnog pristupa rizicima taj što se naglasak stavlja na upravljanje financijskim rizicima, dok se za upravljanje operativnim ili strateškim rizicima ne uspostavljaju jasne mjere upravljanja.[50] Identifikacija, procjena, praćenje rizika i komunikacija o rizicima su *ad hoc* i nisu sustavne.[51]

Za razliku od tradicionalnog upravljanja rizicima, u okviru integriranog ili strateškog upravljanja rizicima analiziraju se korelacije između različitih rizika, proces upravljanja je strukturiran, jasno definiran, sustavan i sveobuhvatan te su nadzorni odbor i visoko

[47] Yoe, C., *op. cit.* u bilj. 37, str. 47.

[48] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 56.
[49] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 56.
[50] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 59.
[51] *Ibid.*

rukovodstvo te uprava direktno uključeni u integrirano upravljanje rizicima i koriste se informacijama koje proizlaze iz sustava upravljanja rizicima u donošenju strateških odluka.[52]

Upravo su posljedice globalne financijske krize navele društva da se okrenu integriranom upravljanju rizicima.[53]

2.5. Obveza uspostave sustava upravljanja rizicima društva?

2.5.1. Financijski sektor

Hrvatskim zakonom kojim su uređena trgovačka društva[54] nije propisano da sva trgovačka društva obvezatno moraju uspostaviti sustav upravljanja rizicima. Stoga, uzimajući u obzir nepostojanje izričite zakonske obveze da sva trgovačka društva ili određene vrste trgovačkih društava (npr. d. d. ili d. o. o.) moraju uspostaviti sustav upravljanja rizicima, zaključuje se da sustav upravljanja rizicima nije nužan dio operativnog ustrojstva poslovanja svih trgovačkih društava u Republici Hrvatskoj prema ZTD-u. Međutim, a što će biti prikazano i detaljno argumentirano poslije u radu (vidi 7. poglavlje), a sada se navodi samo opaske radi – nepostojanje izričite zakonske obveze organiziranja sustava upravljanja rizicima na razini društva (prema ZTD-u) ne znači da primjerice članovi uprave trgovačkih društava u donošenju poduzetničkih odluka ni na koji način ne moraju (u određenim slučajevima, u određenoj mjeri) upravljati rizicima. Nepostojanje zakonske obveze sustava upravljanja rizicima ne znači da članovi uprave mogu potpuno ignorirati postojanje „prevelikih rizika“ i tvrditi da nepostojanje zakonske obveze uspostave i implementiranja sustava upravljanja rizicima znači da o rizicima društva ne treba voditi računa.

S time u vezi, a s ciljem poredbenopravne analize, treba istaknuti specifičnost koja proizlazi iz njemačkog prava, a tiče se dioničkih društava osnovanih u Njemačkoj. Naime, člankom 91., stavkom 2. njemačkog Zakona o dioničkim društvima iz 1965., izmijenjenog i dopunjenog 2023., propisano je da je uprava dioničkog društva dužna poduzeti odgovarajuće

[52] *Ibid.*
[53] *Ibid.*
[54] Zakon o trgovačkim društvima (NN, br. 111/93, 34/99, 121/99, 52/00, 118/03, 107/07, 146/08, 137/09, 125/11, 152/11, 111/12, 68/13, 110/15, 40/19, 34/22, 114/22, 18/23, 130/23; dalje u tekstu: ZTD).

mjere, a posebice uspostaviti sustav praćenja, s ciljem ranog identificiranja događaja koji dovode u opasnost nastavak postojanja društva.[55] To znači da su po njemačkom pravu dionička društva dužna uspostaviti sustav praćenja koji uključuje rano identificiranje rizika koji dovode u pitanje nastavak postojanja društva. Kada je riječ o dioničkom društvu uvrštenom na burzi, ovlašteni revizor mora procijeniti je li uprava poduzela odgovarajuće mjere u skladu s člankom 91., stavkom 2. njemačkog Zakona o dioničkim društvima te je li sustav praćenja koji se treba uspostaviti sposoban ispuniti svoje zadaće.[56] Nadalje, a u vezi s dioničkim društvima uvrštenima na njemačkoj burzi, uprava je dužna implementirati i sustav unutarnje kontrole i sustav upravljanja rizicima koji je odgovarajući i efektivan s obzirom na poslovne aktivnosti društva i s obzirom na stanje rizika.[57]

Iako hrvatski zakonodavac ZTD-om nije predvidio opću obvezu uspostave sustava upravljanja rizicima za trgovačka društva (ni obvezu implementiranja ograničenog sustava upravljanja rizicima koji omogućuje rano identificiranje događaja koji dovode u opasnost nastavak postojanja društva), posebnim zakonima / pravnim izvorima EU-a (uredbama i direktivama) za neka društva koja obavljaju posebne „regulirane financijske“ djelatnosti propisana je izričita obveza uspostave sustava upravljanja rizicima. Područje hrvatske regulative koje obilato sadržava detaljna pravila o sustavima upravljanja rizicima i o upravljanju rizicima općenito upravo je područje financijske industrije (bankarski sektor, tržište kapitala, osiguranje).

Da je tomu tako, vidljivo je iz primjera koji se navode u nastavku.

Zakonom o osiguranju predviđeno je da je društvo za osiguranje dužno uspostaviti i provoditi sustav upravljanja rizicima kojima je ono izloženo u pojedinačnim, odnosno svim vrstama poslova osiguranja koje obavlja.[58] Sustav upravljanja rizicima društva za osiguranje obuhvaća strategije, procese i postupke izvješćivanja nužne za identificiranje, mjerenje, praćenje, upravljanje rizicima te kontinuirano izvještavanje na pojedinačnoj i grupnoj osnovi

[55] Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), das zuletzt durch Artikel 13 des Gesetzes vom 11. Dezember 2023 (BGBl. 2023 I Nr. 354) geändert worden ist, njemački Zakon o dioničkim društvima od 6. rujna 1965. izmijenjen Zakonom od 22. veljače 2023. (dalje u tekstu: AktG), preuzeto s https://www.gesetze-im-internet.de/englisch_aktg/index.html
Stock Corporation Act (gesetze-im-internet.de).
[56] 317. 4 Handelsgesetzbuch – HGB, HGB - englisch (gesetze-im-internet.de).
[57] Čl. 91., st. 3. AktG-a.
[58] Čl. 91., st. 2 Zakona o osiguranju (NN, br. 30/15, 112/18, 63/20, 133/20, 151/22).

o rizicima kojima je društvo za osiguranje izloženo ili bi moglo biti izloženo u svom poslovanju te o međusobnoj ovisnosti tih rizika.[59]

Sustav upravljanja rizicima u društvu za osiguranje mora biti učinkovit i dobro integriran u organizacijsku strukturu i postupke donošenja odluka društva za osiguranje, uzimajući u obzir osobe koje upravljaju društvom ili obavljaju druge ključne funkcije.[60] Društvo za osiguranje dužno je ustrojiti učinkovitu i neovisnu funkciju upravljanja rizicima. Uprava društva za osiguranje odgovorna je za proces upravljanja rizicima, a u provođenju moraju sudjelovati svi zaposlenici društva za osiguranje u okviru svojih zaduženja.[61]

Iz danog primjera vidljivo je da proces upravljanja rizicima, uključujući i komuniciranje o njima, čini dio šireg sustava upravljanja rizicima. Za društva za osiguranje zakonodavac je predvidio posebnu funkciju upravljanja rizicima koja je nužan element sustava upravljanja rizicima.[62]

Nadalje, i *leasing* društvo dužno je uspostaviti sveobuhvatan i učinkovit sustav upravljanja rizicima u skladu s vrstom, opsegom i složenosti svoga poslovanja[63] te ustrojiti funkciju upravljanja rizicima.[64] Sustav upravljanja rizicima sastoji se najmanje od strategija, politika, postupaka i mjera upravljanja rizicima, tehnika mjerenja rizika i podjele odgovornosti u vezi s upravljanjem rizicima. Uprava *leasing* društva sudjeluje u procesu upravljanja rizicima i odgovorna je za njega, a svi radnici *leasing* društva moraju sudjelovati u provođenju sustava upravljanja rizicima. *Leasing* društvo dužno je utvrditi prihvatljiv stupanj rizika za pojedine vrste rizika, što upućuje na to da je sklonost preuzimanju rizika također jedan od elemenata sustava upravljanja rizicima.[65]

Također, faktoring društvo dužno je uspostaviti sveobuhvatan i učinkovit sustav upravljanja rizicima u skladu s vrstom, opsegom i složenosti svoga poslovanja.[66]

Člankom 23., stavkom 1. Delegirane uredbe Komisije (EU) 2017/565 propisane su mjere koje je investicijsko društvo dužno poduzimati u okviru upravljanja rizikom. Naime,

[59] Čl. 94., st. 1. Zakona o osiguranju.
[60] Čl. 94., st. 2. Zakona o osiguranju.
[61] Čl. 95., st. 7. Zakona o osiguranju.
[62] Čl. 95. Zakona o osiguranju.
[63] Čl. 69., st. 2. Zakona o leasingu (NN, br. 141/13; dalje u tekstu: ZL).
[64] Čl. 68., st. 2. ZL-a.
[65] Čl. 4., st. 3. Pravilnika o kriterijima i načinu upravljanja rizicima leasing društva (NN, br. 86/18).
[66] Čl. 64., st. 2. Zakona o faktoringu (NN, br. 94/14, 85/15, 41/16).

investicijska društva, kada je to prikladno i razmjerno s obzirom na prirodu, opseg i složenost njihova poslovanja te prirodu i raspon investicijskih usluga i aktivnosti koje obavljaju tijekom svojeg poslovanja, uspostavljaju i održavaju funkciju upravljanja rizikom. Za investicijska društva bitno je naglasiti da europski zakonodavac nije predvidio u svim slučajevima obvezu uspostave posebne funkcije upravljanja rizicima, nego samo kada je to prikladno i razmjerno poslovanju.

Što se tiče kreditne institucije, ona je dužna sustavom upravljanja rizicima obuhvatiti kreditni rizik, koncentracijski rizik, sekuritizacijske rizike, rezidualni rizik, tržišne rizike, operativni rizik, likvidnosni rizik, kamatni rizik u knjizi pozicija kojima se ne trguje, rizik prekomjerne financijske poluge i ostale rizike kojima je izložena ili bi mogla biti izložena u svojem poslovanju.[67] Kreditna institucija dužna je, razmjerno vrsti, opsegu i složenosti poslova koje obavlja i rizicima svojstvenima poslovnom modelu, uspostaviti i provoditi djelotvoran i pouzdan sustav upravljanja rizicima koji se primjenjuje u svim poslovnim linijama i organizacijskim jedinicama kreditne institucije.[68] Kreditna institucija dužna je uspostaviti funkciju kontrole rizika.[69] Proces upravljanja rizicima sastoji se od kontinuiranog utvrđivanja rizika, redovitog mjerenja/procjene utvrđenih rizika, ovladavanja rizicima u smislu primjene odgovora na rizike (prihvaćanje, smanjenje, izbjegavanje ili prijenos rizika), izvješćivanja odnosno komuniciranja o rizicima te usklađivanja profila rizičnosti sa sklonošću preuzimanju rizika.[70]

Obveza imanja i primjene okvira za upravljanje rizicima predviđena je i za europske pružatelje usluga skupnog financiranja.[71]

Društvo za upravljanje UCITS fondovima također je primjer društva koje mora imati sustav upravljanja rizicima. Ono je dužno uspostaviti sveobuhvatan i učinkovit sustav upravljanja rizicima koji pogađaju društvo za upravljanje, ali i UCITS fondove kojima društvo

[67] Čl. 103., st. 2. Zakona o kreditnim institucijama (NN, br. 159/13, 19/15, 102/15, 15/18, 70/19, 47/20, 146/20, 151/22; dalje u tekstu: ZOKI).
[68] Čl. 29., st. 1. Odluke HNB-a o sustavu upravljanja (NN, br. 96/18, 67/19, 145/20, 145/21 i 51/23).
[69] Čl. 105., st. 1. ZOKI-ja.
[70] Čl. 29. Odluke HNB-a o sustavu upravljanja.
[71] Vidi čl. 4. Uredbe (EU) 2020/1503 Europskog parlamenta i Vijeća od 7. listopada 2020. o europskim pružateljima usluga skupnog financiranja za poduzeća i izmjeni Uredbe (EU) 2017/1129 i Direktive (EU) 2019/1937 (Tekst značajan za EGP).

upravlja, u skladu s vrstom, opsegom i složenosti svoga poslovanja, koji mora uključivati najmanje:

1. relevantne dijelove organizacijske strukture društva za upravljanje s definiranim ovlastima i odgovornostima za upravljanje rizicima, pri čemu središnju ulogu ima funkcija upravljanja rizicima
2. postupke i principe za utvrđivanje te tehnike i alate za mjerenje rizika
3. strategije, politike, postupke i mjere vezane za upravljanje rizicima i
4. praćenje i izvještavanje o rizicima.[72]

Iz toga je vidljivo da su proces upravljanja rizicima i komunikacija o rizicima jedni od okosnica sustava upravljanja rizicima društava za upravljanje UCITS fondovima.

Sustav upravljanja rizicima dužni su uspostaviti i upravitelji alternativnih investicijskih fondova.[73] U kontekstu upravitelja alternativnih investicijskih fondova bitno je naglasiti da upravljanje rizicima čini „minimalne poslove" koje upravitelji alternativnih investicijskih fondova moraju obavljati u sklopu upravljanja ulaganjima.[74] To implicira da je upravljanje rizicima u konkretnom slučaju obvezatna poslovna djelatnost koju takvo društvo mora obavljati. Naime, za razliku od društava za upravljanje UCITS fondovima, upravitelji alternativnih investicijskih fondova ne mogu biti kao takvi licencirani ako ne izvršavaju poslove upravljanja rizicima u sklopu upravljanja ulaganjima.[75]

Zakonom o tržištu kapitala predviđena je obveza uspostave sustava upravljanja rizicima i za burzu, središnju drugu ugovornu stranu, središnje klirinško depozitarno društvo.[76]

Slijedom svih navedenih primjera društava koja moraju imati sustav upravljanja rizicima, evidentno je da je obveza uspostave sustava upravljanja rizicima tipična i dominantna karakteristika za bankarski sektor, nebankarski financijski sektor, sektor osiguranja, ali i za infrastrukturu tržišta kapitala.

---

[72] Čl. 56., st. 1. Zakona o otvorenim investicijskim fondovima s javnom ponudom (NN, br. 44/16, 126/19, 110/21, 76/22).
[73] Čl. 58., st. 1. Zakona o alternativnim investicijskim fondovima (NN, br. 21/18, 126/19, 110/21, 83/23).
[74] Vidi Prilog 1, točku 1. b Direktive 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i o izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010 (Tekst značajan za EGP) (dalje u tekstu: AIFMD).
[75] Claude, K., Lebbe, I., Organismes de placement collectif et vehicules d investissement apparentes en droit luxemboureois, Luxembourg, 3. izdanje, t. 631, str. 254.
[76] Čl. 652., čl. 297., čl. 550. Zakona o tržištu kapitala (NN, br. 65/18, 17/20 i 83/21; dalje u tekstu: ZTK).

2.5.2. Korporativno upravljanje dioničkih društava uvrštenih na burzi

U nastavku ovog rada prikazuje se jedan „tip“ društva koji bi trebao imati sustav upravljanja rizicima. Preporuka uspostave sustava upravljanja rizicima ne postoji zbog pružanja financijskih usluga, nego je plod povećanih obveza transparentnosti zbog povećanog interesa javnosti koji proizlazi iz mogućnosti ulaganja u takvo društvo široka kruga potencijalnih ulagatelja (uključujući i „malih“ odnosno neprofesionalnih ulagatelja). Konkretno, riječ je o društvima čije su dionice uvrštene na uređeno tržište poput uređenog tržišta Zagrebačke burze, pa su one samim time dostupne velikom krugu zainteresiranih ulagatelja, odnosno javnosti. U tom kontekstu upravljanje rizicima promatra se kao dio šireg sustava korporativnog upravljanja.

S time u vezi, OECD[77] je 2015. prihvatio preporuke neobvezujućeg karaktera o principima korporativnog upravljanja koje su izmijenjene i dopunjene 2023. godine.[78] Preporuke nisu zamjena za nacionalno zakonodavstvo niti su pravne snage iznad normi nacionalnog prava.[79] Iako se principi korporativnog upravljanja OECD-a primjenjuju na društva čije su dionice uvrštene na uređeno tržište (engl. *publicly traded companies*), i to neovisno o tome je li riječ o društvu iz financijskog sektora, navedene preporuke koristan su alat (putokaz) za unaprjeđenje korporativnog upravljanja i za društva čijim se vrijednosnim papirima javno ne trguje.[80] Korporativno upravljanje (engl. *corporate governance*) kao pojam uključuje odnose između uprave, nadzornog odbora, dioničara i dionika (engl. *stakeholders*).[81] Općenito govoreći, principi korporativnog upravljanja sadržavaju pojašnjenja o strukturama i sustavima upravljanja društvom, uspostavljanju ciljeva, njihovu postizanju i nadzoru. Principi korporativnog upravljanja OECD-a predviđaju objavu dostatnih i potpunih informacija kako bi se informirali investitori o razumno predvidljivim materijalnim rizicima društva (engl.

[77] Organisation for Economic Co-operation and Development.
[78] OECD, G20/OECD Principles of Corporate Governance 2023, Pariz, dostupno na https://www.oecd-ilibrary.org/governance/g20-oecd-principles-of-corporate-governance-2023_ed750b30-en (posljednji pristup 25. veljače 2024.)
[79] OECD, *op. cit.* u bilj. 78, str. 6.
[80] OECD, *op. cit.* u bilj. 78, str. 7.
[81] OECD, *op. cit.* u bilj. 78, str. 6.

reasonably foreseeable material risk of the company) koji mogu uključivati rizike specifične za industriju ili geografsko područje u kojem društvo posluje.[82] Takve informacije daju pregled ovisnosti o određenim robama i lancima nabave, rizicima kamatnih stopa, valutnim rizicima, operativnim rizicima, rizicima u vezi s usklađenošću, rizicima održivosti.[83] Ističe se da je objava rizika najefikasnija kada je prilagođena konkretnom društvu i industriji u kojoj posluje.[84] To znači da rizici koji se objavljuju moraju biti specifični, a ne generički, što je zapravo odraz pravila o ispravnom komuniciranju rizika javnosti. Objavljivanje informacija o sustavu upravljanja rizicima smatra se prema OECD-u dobrom praksom.[85] Drugim riječima, komunikacija je bitan element upravljanja rizicima.

Jedna od važnih dužnosti nadzornog odbora društva jest nadzor nad sustavom upravljanja rizicima.[86] Nadzor koji provodi nadzorni odbor osigurava da uprava upravlja rizicima na način da se oni kreću u okvirima postizanja željenog profila rizičnosti.[87]

Nadzorni odbor dužan je osigurati da se uzimaju u obzir i rizici održivosti.[88] Nadzorni odbor dužan je osigurati da društvo ima uspostavljene adekvatne procese u vezi s upravljanjem rizicima koji proizlaze iz zdravstvenih kriza, disrupcija u lancima nabave i geopolitičkih tenzija, što znači da nema sustava upravljanja rizicima bez procesa upravljanja rizicima. Preporuke OECD-a ističu važnost upravljanja rizicima digitalne sigurnosti, sigurnosti podataka, korištenja usluga *clouda*, poreza, što sugerira aktualnost i važnost upravljanja tim pojedinim vrstama rizika.[89] Upravljanje rizicima digitalne sigurnosti obuhvaća upravljanje incidentima iz područja digitalne sigurnosti poput neautoriziranog pristupa sustavu ili softveru te gubitak ili krađu podataka. Kako bi se pomoglo nadzornom odboru u nadzoru upravljanja rizicima, društva mogu uspostaviti odbor za rizike i/ili proširiti djelokrug rada odbora za reviziju (engl. *audit committee*).[90] Kada je to opravdano veličinom društva, njegovom strukturom i industrijom u kojoj društvo posluje, uspostava odbora za rizike može poboljšati

[82] OECD, *op. cit.* u bilj. 78, str. 30 i 31.
[83] *Ibid.*
[84] *Ibid.*
[85] OECD, *op. cit.* u bilj. 78, str. 31.
[86] OECD, *op. cit.* u bilj. 78, str. 36.
[87] *Ibid.*
[88] *Ibid.*
[89] *Ibid.*
[90] *Ibid.*

rad nadzornog odbora i omogućiti fokus na specifičnim poljima rizika. Preporuke OECD-a ističu da varijanta uspostave odbora za rizike i odvajanje funkcija u vezi s rizicima između revizijskog odbora i odbora za rizike mogu biti svrhoviti. Jedna je od mogućih opcija da financijski rizici potpadnu pod nadležnost revizijskog odbora, a rizici nefinancijske prirode pod djelokrug odbora za rizike, čime se rasterećuje revizijski odbor i omogućuje više posvećenosti (ekspertize) u upravljanju rizicima nefinancijske prirode osnivanjem odbora za rizike.[91]

Što se tiče Republike Hrvatske, a isto u domeni „mekog prava", svrha Kodeksa korporativnog upravljanja Zagrebačke burze i Hrvatske agencije za nadzor financijskih usluga[92] „promicanje je djelotvornog upravljanja i odgovornosti u društvima čije su dionice uvrštene na uređeno tržište Zagrebačke burze".[93] Kodeks se primjenjuje na sva društva čije su dionice uvrštene na uređeno tržište Zagrebačke burze, osim dionica zatvorenog investicijskog fonda.[94] Prema Kodeksu, upravljanje rizicima sastavni je dio uspjeha društva.[95]

Društvo na koje se primjenjuje hrvatski Kodeks mora održavati djelotvoran sustav upravljanja rizicima koji je adekvatan za njegove ciljeve, veličinu i razmjer djelatnosti.[96] Sustav upravljanja rizicima mora uključivati procedure koje osiguravaju pouzdano prepoznavanje rizika, mjerenje, odgovore, prijavljivanje i njihovo nadziranje.[97] Jedno je od načela hrvatskog Kodeksa da je nadzorni odbor dužan osigurati ustrojenost djelotvornih struktura, politika i postupaka radi identificiranja, prijavljivanja, upravljanja i nadgledanja znatnih rizika s kojima se suočava društvo te nadzirati djelotvornost sustava upravljanja rizicima.[98] Prema hrvatskom Kodeksu uprava mora izvještavati nadzorni odbor u redovitim intervalima o znatnijim financijskim i nefinancijskim rizicima, što je primjer interne komunikacije o rizicima.[99] Uprava je dužna prepoznati znatnije financijske, operativne i vanjske rizike te implementirati djelotvorne sustave upravljanja rizicima.[100] Odredbom 65.

[91] OECD, *op. cit.* u bilj. 78, str. 41.
[92] Hrvatska agencija za nadzor financijskih usluga (HANFA), Zagrebačka burza d. d. (ZSE), Kodeks korporativnog upravljanja, Zagreb, 2019.
[93] Cit., HANFA, ZSE, *op. cit.* u bilj. 92, str. 7.
[94] HANFA, ZSE, *op. cit.* u bilj. 92, str. 8.
[95] HANFA, ZSE, *op. cit.* u bilj. 92, str. 24.
[96] HANFA, ZSE, *op. cit.* u bilj. 92, t. 66., str. 26.
[97] *Ibid.*
[98] *Ibid.*
[99] HANFA, ZSE, *op. cit.* u bilj. 92, t. 4., str. 11.
[100] HANFA, ZSE, *op. cit.* u bilj. 92, t. 42., str. 20.

Kodeksa propisano je da revizijski odbor mora najmanje jedanput godišnje ocijeniti djelotvornost upravljanja rizicima i sustava unutarnje kontrole kao cjeline te po potrebi dati preporuke nadzornom odboru i upravi društva.

Što se tiče prakse na hrvatskom tržištu kapitala, „u 2022. većina izdavatelja dionica, njih 96 %, održava djelotvoran sustav upravljanja rizicima, koji osigurava pouzdano prepoznavanje i mjerenje rizika te njihovo nadziranje (u 2021. njih 93 %).“[101] To znači da postoje izdavatelji dionica uvrštenih na uređeno tržište Zagrebačke burze koji nemaju sustav upravljanja rizicima, što je u skladu s pravnom prirodom Kodeksa koja nije obvezujuće naravi (engl. *comply or explain*). Njemački je zakonodavac, a kako je prije objašnjeno, za razliku od hrvatskog pristupa, obvezu uspostave sustava upravljanja rizicima za dionička društva koja kotiraju na burzi propisao zakonom.[102]

Prema podatcima HANFA-e, „37 % izdavatelja imalo je u 2022. osobu zaduženu za upravljanje rizicima (u 2021. godini 31 %)“.[103]

3. TEMELJNI KONCEPTI U KONTEKSTU UPRAVLJANJA RIZICIMA

Temeljni su koncepti upravljanja rizicima za potrebe ovog rada sklonost preuzimanju rizika, kapacitet za rizik, profil rizičnosti, tolerancija, strategija upravljanja rizicima.[104]

3.1. Sklonost preuzimanju rizika

Postojanje definiranog apetita društva u službenoj pisanoj izjavi karakteristika je integriranog upravljanja rizicima.[105]

---

[101] Cit., HANFA, Godišnji izvještaj o korporativnom upravljanju, 2022., dostupno na https://www.hanfa.hr/publikacije/godisnji-izvjestaj-o-korporativnom-upravljanju/ (posljednji pristup 15. veljače 2024.).
[102] Čl. 91., st. 3. AktG-a.
[103] HANFA, *op. cit.* u bilj. 102.
[104] „Temeljni koncepti“ upravljanja rizicima nije pravni termin definiran odredbama hrvatskog pravnog sustava. Temeljni koncept može varirati od autora do autora. Tako primjerice, po Yoe, C., *op. cit.* u bilj. 37, temeljni koncepti upravljanja rizicima jesu profil rizika, sklonost preuzimanju rizika, tolerancija za rizik. Vidi detaljnije za obuhvat „temeljnih koncepata i teorija upravljanja rizicima“ prema Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4. Sprčić, poglavlje 1.
[105] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 59.

Društvo može u svojem internom aktu navesti da je sklonost tržišnom i kreditnom riziku minimalna. Što se tiče operativnog rizika, društvo može navesti da ono može prihvatiti određeni stupanj rizika kako bi ostvarilo željeni rezultat vodeći se znatnom mogućnošću ostvarivanja dobiti, s time da je omjer potencijalne dobiti i rizika važan faktor. Što se tiče rizika neusklađenosti, društvo može biti sklono potpunom izbjegavanju ostvarenja takva rizika. Kreditna institucija može u svojim internim politikama i postupcima navesti da neće poslovati s određenim fizičkim ili pravnim osobama zbog toga što je pružanje usluga takvim osobama potencijalno povećani rizik od pranja novca u mjeri iznad sklonosti kreditne institucije preuzimanju rizika pranja novca / financiranja terorizma.[106]

Navedeni primjeri prikazuju način na koji se može izraziti apetit društva za preuzimanjem određene vrste rizika (tržišnog, kreditnog, rizika usklađenosti, pranja novca i financiranja terorizma).

Apetit društva za rizikom (engl. *risk appetite*) koncept je koji obuhvaća rizike koje je društvo spremno preuzeti u postizanju svojih ciljeva.[107] On može biti izražen kvalitativno ili kvantitativno.[108] Primjer je kvalitativnog označavanja apetita društva za rizikom tvrdnja da je apetit društva za određenom vrstom rizika mali, srednji ili visok.[109] Apetit društva za rizikom definira se prema pojedinom riziku poduzeća.[110] To znači da ne postoji jedan apetit društva za rizikom, nego postoji više različitih apetita ovisno o pojedinim rizicima na koje se oni odnose.[111]

---

[106] Vidi više o sklonosti preuzimanju rizika od pranja novca i financiranja terorizma u Smjernicama EBA-e na temelju članka 17. i članka 18., stavka 4. Direktive (EU) 2015/849 o dubinskoj analizi stranaka i čimbenicima koje bi kreditne i financijske institucije trebale uzeti u obzir pri procjeni rizika od pranja novca i financiranja terorizma koji je povezan s pojedinačnim poslovnim odnosima i povremenim transakcijama („Smjernice o čimbenicima rizika od pranja novca i financiranja terorizma"), kojima se stavljaju izvan snage i zamjenjuju Smjernice JC/2017/37 https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20(revised)%202021-02/Translations/1016919/Guidelines%20ML%20TF%20Risk%20Factors_HR.pdf (posljednji pristup 2. veljače 2024.).

[107] Moeller, R., COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, 2007., poglavlje 3. Components of COSO ERM.

[108] *Ibid.*

[109] *Ibid.*

[110] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 240.

[111] The Institute of Risk management, Risk Appetite & Tolerance, Guidance Paper, str. 7, dostupno na https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf (posljednji pristup 28. veljače 2024.).

Apetit društva za preuzimanjem rizika nije isto što i apetit pojedinca (fizičke osobe) za preuzimanjem rizika te ih je potrebno razlikovati.

Uzmimo, primjerice, situaciju da je fizička osoba (radnik) zaposlena u društvu te je zadužena za izbor dobavljača ili drugih poslovnih partnera s kojima će društvo surađivati. Zamislimo da su ekološke vrijednosti iznimno bitne društvu te da je društvo svojim internim aktima, strategijama, politikama, ciljevima prihvatilo pristup da će u najvećoj mogućoj mjeri izbjegavati poslovnu suradnju s dobavljačima koji štete okolišu. Zamislimo da radnik svjesno odabere dobavljača koji ima iznimno negativnu reputaciju ekološke osviještenosti, ali koji je ponudio jako dobre uvjete koji će vjerojatno pozitivno utjecati na zaradu društva. Radnik ima drugačiji apetit za rizicima i osobno prihvaća veći rizik onečišćenja okoliša jer je vođen mogućnostima veće zarade zbog dobrih uvjeta ugovora. Iz toga je vidljivo da se apetit za rizikom radnika i apetit za rizikom društva u konkretnom slučaju ne poklapaju. U kontekstu odgovornosti radnika za štetu društvu ili potencijalne povrede radnog odnosa zasigurno se može postaviti pitanje je li radnik (i u kojoj mjeri) postupao protivno apetitu društva za rizikom, odnosno je li bio ovlašten tako postupati.

Isto je primjenjivo i na člana uprave društva / višeg rukovodstva. U kontekstu postupanja člana uprave u vezi s apetitom društva za preuzimanjem rizika važno je da članovi uprave / visoko rukovodstvo, koji donose poduzetničke odluke, razumiju „dopuštene“ rizike i njihove stupnjeve/razine. Stoga, a na tragu navedenog, izjava o apetitu društva za preuzimanjem rizika treba biti dostupna (komunicirana), jasna i praktična kako bi omogućila članovima uprave / višem rukovodstvu donošenje „mudre“ poduzetničke odluke u okružju rizika kojima je društvo izloženo (engl. *risk – intelligent decision*).[112]

Određivanjem granica preuzimanju rizika osigurava se da uprava i nadzorni odbor[113] ne donose odluke koje bi izložile društvo prekomjernom riziku (u odnosu na sklonost društva preuzimanju rizika). Također, određivanjem sklonosti društva preuzimanju rizika štiti se društvo i od pretjerano konzervativnih odluka rukovodstva koje bi bile pretjerano ispod razine

[112] The Institute of Risk Management, *op. cit.* u bilj. 110, str. 9.
[113] Epetimehin, Festus M., Impact of risk appetite on the value of a firm, European Scientific Journal, August 2013 edition, Vol. 9, No. 22, str. 336, 1660-Article Text-5109-1-10-20130903.pdf.

sklonosti društva preuzimanju rizika. To je povezano s uzrečicom „tko ne riskira, taj ne profitira“.

U stručnoj literaturi postoji više različitih definicija i razrada koncepata apetita za rizikom, s time da najveći broj njih apetit za rizikom dovodi u vezu s pojmom prihvaćanja rizika.[114]

Autor ovog rada analizirao je 13 definicija apetita za rizikom.[115] U 11 definicija od njih 13 apetit za rizikom odnosi se na preuzimanje/prihvaćanje rizika (engl. *retain, accept, take, pursue*). Preuzima / prihvaća se iznos/količina (engl. *amount/quantum*), vrsta (engl. *type*), razina (engl. *level*), definirana razina (engl. *defined level*) ili ukupnost (engl. *total*) rizika. Iz ispitanog uzorka definicija proizlazi da, iako postoje jezično-stilske varijacije u definiranju pojma apetita društva za rizikom, pristupi definiranju predmetnog koncepta imaju svoje temeljne sličnosti. Stoga, apetit za rizikom je koncept koji daje odgovor na pitanje koje je vrste rizika i u kojoj mjeri društvo spremno preuzeti u svom poslovanju. Drugim riječima, radi se o sklonosti društva preuzimanju prihvatljivih vrsta i razina rizika.

Neki teoretičari smatraju da apetit za rizikom ima konotacije koje vode na pogrešan trag (engl. *misleading connotations*) – da je dosad objavljeno više neodgovarajućih definicija te da se umjesto izraza „apetit za rizikom“ treba koristiti izrazom „politike preuzimanja rizika“.[116]

Što se tiče hrvatskog pravnog sustava, u zakonima i podzakonskim pravnim propisima zastupljen je izraz „sklonost preuzimanju rizika“, što zapravo i odgovara biti koncepta apetita za rizikom kako je i objašnjeno.

Tako je, primjerice, odlukom Hrvatske narodne banke o sustavu upravljanja[117] navedeno sljedeće: „Sklonost preuzimanju rizika (engl. *risk appetite*) jest razina i vrste rizika koje je kreditna institucija spremna preuzeti unutar definirane sposobnosti podnošenja rizika kako bi ostvarila svoje strateške ciljeve.“

---

[114] Aven, T., On the Meaning and Use of the Risk Appetite Concept, Risk Analysis, Vol. 33, No. 3, 2013., risk apetit koncept.pdf.

[115] Definicije su preuzete iz Aven, T., *op. cit.* u bilj. 113, tablice I., str. 464.: ISO, COSO, HM Treasury's Orange book, Institute of Internal Auditors (from it glossary), Dupoy, Office Government Commerce UK, Towers Watson, IRMI, BS, BCI, KPMG, PWC, Fxtimes.

[116] Vidi primjerice Leitch, M, Working In Uncertainty: Risk appetite definitions, 2009., preuzeto s https://www.workinginuncertainty.co.uk/appetitedef.shtml (posljednji pristup 20. veljače 2024.).

[117] Čl. 3., toč. 12. Odluke HNB-a o sustavu upravljanja.

Također, Zakon o tržištu kapitala umjesto riječju „apetit“ koristi se konceptom „sklonost preuzimanju rizika“. Konkretno, čl. 577. ZTK-a propisano je da nadzorni odbor središnjeg depozitorija (ako je primjenjivo) daje suglasnost upravi na strategije i politike preuzimanja rizika. Također, čl. 637. ZTK-a propisano je da nadzorni odbor središnjeg klirinškog depozitarnog društva daje suglasnost upravi na strategije i politike preuzimanja rizika. Isto tako, čl. 30., st. 8. ZTK-a propisano je da je uprava investicijskog društva dužna odobravati i periodično provjeravati strategije i politike investicijskog društva u vezi sa sklonosti preuzimanju rizika.

Točka 58. Kodeksa korporativnog upravljanja Zagrebačke burze i Hrvatske agencije za nadzor financijskih usluga navodi cit.: „Uprava će, uz prethodnu suglasnost nadzornog odbora, usvojiti politiku koja određuje prirodu i opseg rizika koje društvo mora i koje je voljno preuzeti kako bi se postigli svi dugoročni strateški ciljevi ('sklonost preuzimanju rizika').“

Iz citirane odredbe Kodeksa korporativnog upravljanja proizlazi da zapravo sklonost preuzimanju rizika uređuje postupanje s dvije vrste rizika: s rizicima koji se preuzimaju slobodnom voljom društva i s rizicima koje društvo mora preuzeti. Također, vidljivo je da se rizici preuzimaju kako bi se ostvarili strateški, odnosno dugoročni strateški ciljevi, što je u skladu s time da su rizici mjerljive neizvjesnosti koje utječu na ciljeve društva.

Na temelju navedenih odredbi hrvatskog pravnog sustava razvidno je da su u pravilu uprava i nadzorni odbor društva iz financijske industrije uključeni u postupak određivanja sklonosti društva za preuzimanje rizika.

Da se ne bi stekao pogrešan dojam da je sklonost preuzimanju rizika isključivo izjava društva o sklonosti preuzimanju pojedinih rizika, ističe se da se okvir sklonosti preuzimanju rizika (engl. *risk appetite framework*) može sastojati od politika, procesa, kontrola i sustava putem kojih se uspostavlja, komunicira i prati sklonost društva preuzimanju rizika te da je izjava u pisanom obliku o sklonosti preuzimanju rizika samo jedan od mogućih elemenata predmetnog okvira.[118] U vezi sa sklonošću preuzimanju rizika, ističe se važnost postojanja eskalacijskih procedura (engl. *escalation procedures*).[119] Eskalacijske procedure u kontekstu

[118] Financial Stability Board, Principles for An Effective Risk Appetite Framework, 2013., str. 2.
[119] United Nations System, Guidelines on Risk Appetite Statements (Final), 2019., t. 3.2., str. 15, https://unsceb.org/sites/default/files/imported_files/2019.HLCM_.26%20-

upravljanja rizicima propisuju što se događa kada je prijeđen određeni prag ili limit pojedinog rizika koji je određen u izjavi o sklonosti preuzimanju rizika. „Eskalacija se sastoji od obavještavanja (engl. *raising the flag*) visokog rukovodstva te ako je potrebno uprave / nadzornog odbora.“[120] Iz toga proizlazi da je eskalacija primjer komunikacije o rizicima kao sastavnog dijela procesa upravljanja rizicima. Takve procedure, između ostalog, uključuju pojašnjenja tko koga i u kojem roku obavještava. Procedure uređuju odnose između odgovorne poslovne jedinice za konkretan rizik, nositelja funkcije upravljanja rizicima, visokog rukovodstva, uprave i nadzornog odbora. Brzina obavještavanja te koga je potrebno obavijestiti, varira ovisno o vrsti i ozbiljnosti rizika. Neka društva u okviru svojih sustava upravljanja rizicima imaju uspostavljene preventivne limite (engl. *pre-emptive trigger limits)*.[121] Naime, eskalacijski procesi mogu biti „preventivno“ aktivirani i prije nego što je prag određen izjavom o sklonosti za preuzimanjem rizika uistinu prijeđen, čime se osigurava preventivna obaviještenost određenih relevantnih osoba prije nego što su kritične razine gubitaka / potencijalnih gubitaka ostvarene.[122]

3.2. Kapacitet za rizik

Uz sklonost preuzimanju rizika, znanost upravljanja rizicima prepoznaje i koncept kapaciteta za rizik (engl. *risk capacity*).[123] Ti koncepti imaju različito značenje i nisu sinonimi.

Kapacitet za rizik maksimalna je količina rizika koje je društvo sposobno apsorbirati u svom poslovanju (na putu ostvarivanja svojih ciljeva).[124]

Uzmimo, primjerice, situaciju da je društvo koje isporučuje proizvod kupcu A odredilo da je sklonost preuzimanju rizika kašnjenja u isporuci proizvoda (dalje u tekstu: rizik kašnjenja) iznimno niska, odnosno do 2 % ukupnih isporuka proizvoda. To znači da će društvo logistički morati poduzeti sve potrebne mjere da potencijalno kašnjenje izbjegne u 98 % isporuka

%20Guidelines%20on%20Risk%20Appetite%20Statements%20-%20Final_1_0.pdf (posljednji pristup 29. siječnja 2024.).

[120] *Ibid.*

[121] *Ibid.*

[122] *Ibid.*

[123] Tako i standard COSO ERM, ISO 31000:2018, Deloitte, Risk Appetite Frameworks: How to spot the genuine article, 2014., str. 6, dostupno na deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf, str. 6.

[124] COSO, *op. cit.* u bilj. 32, str. 51.

proizvoda kupcu A. Zamislimo hipotetsku situaciju da je društvo utvrdilo da ako rizik kašnjenja bude ostvaren i u 20 % isporuke, društvo neće snositi štetne posljedice jer su ugovorena dopuštena odstupanja koja zapravo omogućuju društvu da rizik kašnjenja bude ostvaren u 20 % isporuka kupcu A. Pretpostavimo da je tih 20 % ujedno i maksimalna količina ostvarenog rizika koje je društvo sposobno apsorbirati jer iznad toga praga za društvo mogu nastupiti iznimno štetne posljedice koje ne može apsorbirati. To znači da je sklonost preuzimanju rizika kašnjenja manja od kapaciteta društva da uspješno apsorbira rizik. Drugim riječima, prihvatljiva količina rizika (koja je u konkretnom primjeru izražena s 2 % isporuka) manja je od maksimalne količine rizika (koja je u konkretnom primjeru izražena s 20 % isporuka). Možemo reći da je takva kultura društva ili stav prema riziku (engl. *attitude towards risk*)[125] iznimno oprezan iliti nesklon riziku kašnjenja isporuke.

Omogućavanje većeg kapaciteta za rizik košta. U konkretnom slučaju pretpostavka je da je društvo možda smanjilo kupoprodajnu cijenu svog proizvoda (nego što bi cijena inače bila), a zauzvrat dobilo veću mogućnost kašnjenja. Stoga, uzimajući u obzir da je cijena hipotetski mogla biti veća u slučaju bez mogućnosti kašnjenja, možemo zaključiti da kapacitet za rizik u konkretnom slučaju nije besplatan te se dovodi u pitanje njegova troškovna opravdanost. Stoga, je li racionalna takva (velika?) razlika između sklonosti preuzimanju rizika i kapaciteta za rizik? Odnos između kapaciteta za rizik i sklonosti preuzimanju rizika može biti indikator hoće li se društvo u budućnosti možda naći u određenim problemima ako se preuzeti rizik ostvari. Naime, ako je sklonost preuzimanju rizika jako visoka, a kapacitet nije dovoljno velik da apsorbira negativne učinke ako se rizik ostvari (manji kapacitet nego sklonost), takav odnos između sklonosti i kapaciteta može se protumačiti na način da postoji (povećani) rizik da će se društvo u budućnosti možda naći u poteškoćama (zbog nemogućnosti apsorbiranja negativnih učinaka). S druge strane, ako je obratna situacija (vidi navedeni primjer rizika kašnjenja gdje je razina kapaciteta „puno“ iznad sklonosti), društvo možda gubi priliku za zaradom (npr. moglo je ugovoriti veću kupoprodajnu cijenu). S time u vezi, COSO model (kao jedan od mogućih modela upravljanja rizicima) naglašava da kapacitet za rizik treba biti uzet

[125] Vidi više o pojmu „stav prema riziku“ u Rittenberg, L.; Martens, F., COSO, Enterprise Risk Management: Understanding and Communicating Risk Appetite, 2012., str. 4, dostupno na https://www.coso.org/_files/ugd/3059fc_b0013c9344764b0b8c30a7eb7e5c27c9.pdf (posljednji pristup 10. veljače 2024.).

u obzir u određivanju sklonosti preuzimanju rizika, da u pravilu društva određuju sklonost preuzimanju rizika u okvirima kapaciteta za rizik te da nije tipično da je sklonost preuzimanju rizika veća od kapaciteta za rizik. Stoga, najčešći je pristup (a i najlogičniji) da sklonost preuzimanju rizika ne prelazi kapacitet društva.

Istoznačnica je kapaciteta za rizik u hrvatskom pravnom sustavu „sposobnost podnošenja rizika“. To je vidljivo iz članka 3., točke 13. Odluke HNB-a o sustavu upravljanja koja navodi da je sposobnost podnošenja rizika (engl. *risk capacity*) najveća razina rizika koju kreditna institucija može preuzeti s obzirom na svoju kapitalnu osnovu, sposobnosti upravljanja rizicima i kontrole te regulativna ograničenja. Iako se predmetna odredba odnosi na kreditne institucije, ona je smjer u kojem se može promatrati kapacitet za rizik i to kao sposobnost podnošenja rizika društva. Preporuka je društvima ne poslovati koristeći se sto posto svojim kapacitetom za rizik zbog toga što bi takvo poslovanje bilo povezano s velikim realnim rizikom potencijalnog prelaska preko kapaciteta društva.[126]

3.3. Profil rizičnosti i tolerancija

Uz sklonost preuzimanju rizika (apetit za rizikom) te kapacitet za rizik (sposobnost podnošenja rizika) postoji i treći pojam koji ima posebno značenje, a to je profil rizičnosti (engl. *risk profile*). Profil rizičnosti smatra se jednim od bitnih koncepata upravljanja rizicima.[127] Profil rizičnosti procjena je rizika kojima jest ili kojima bi moglo biti izloženo društvo u svojem poslovanju.[128] Profil rizičnosti sveukupna je izloženost pojedinačnim konkretnim rizicima ili skupini rizika u točno određenom trenutku u vremenu.[129] Drugim riječima, profil rizičnosti odraz je iliti plod barem faza identifikacije i procjene ozbiljnosti rizika (u slučaju kada je riječ o profilu rizičnosti prije primjene odgovora na rizik). Pojednostavnjeno i slikovitije, profil rizičnosti možemo promatrati kao krvnu sliku rizika koja

[126] Deloitte, *op. cit.* u bilj. 123, str. 6.
[127] Yoe, C., *op. cit.* u bilj. 37, str. 204.
[128] Čl. 3., toč. 10. Odluke HNB-a o sustavu upravljanja.
[129] Yoe, C., *op. cit.* u bilj. 37, str. 200.

pokazuje (stvarno) stanje i ozbiljnost/bitnost situacije na određeni datum (trenutak vađenja krvi), a sklonost preuzimanju rizika kao namjeru, smjer, okvir, politiku.[130]

U pravilu profil rizičnosti temelji se na podatcima u registru/mapi rizika koja sadržava informacije o rizicima kojima je društvo izloženo.[131] U registru rizika koje vodi društvo mogu se pronaći opisi rizika, uspostavljene kontrole, dodatne kontrole ako su potrebne te identifikacija nositelja rizika i osoba odgovornih za kontrole.[132]

U praktičnom životu društva može se dogoditi da stvarno stanje, odnosno postojeći profil rizičnosti (engl. *existing risk profile*) ne odgovara, to jest nije u skladu s politikom preuzimanja rizika zbog toga što su, primjerice, osobe odgovorne za vođenje društva donosile odluke iznad granica iz politika preuzimanja rizika. Postavlja se pitanje treba li politike sklonosti preuzimanju rizika promatrati kruto i kategorički bez ikakvih mogućnosti odstupanja u stvarnom životu društva ili ipak postoji određeni stupanj mogućnosti odstupanja, odnosno tolerancije u odnosu na zacrtanu politiku preuzimanja rizika. Toleriranje rizika iznad sposobnosti podnošenja rizika nije održivo i takav pristup upravljanju rizicima podložan je ranjivosti.[133] Jedna od najčešćih zabluda u vezi s upravljanjem rizicima jest ta da su sklonost preuzimanju rizika i tolerancija prema rizicima istoznačnice.[134] Prema nekim autorima i dalje postoji znatno nerazumijevanje predmetnih pojmova i raširena je percepcija da se definicije tih koncepata mijenjaju iz dana u dan.[135] U nastavku se daje pregled tvrdnji iz stručne literature koje upućuju na to da sklonost i tolerancija nose različito značenje:

- „Apetit za rizikom i tolerancija prema rizicima definirani su te ih zaposlenici jasno razumiju.“[136]
- Sklonost preuzimanju rizika, tolerancija prema rizicima i profil rizičnosti jesu tri koncepta integriranog upravljanja rizicima.[137]

[130] Tako i *ibid.*
[131] Hopkin, P.; Thompson, C., *op. cit.* u bilj. 16, str. 159.
[132] *Ibid.*, str. 435.
[133] *Ibid.*, str. 248.
[134] Fraser, R. S.; Simkins, B. J., Ten Common Misconceptions About Enterprise Risk Management, Journal of Applied Corporate Finance, Volume 19, Number 4, str. 76.
[135] *Ibid.*
[136] Cit., Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 62.
[137] Yoe, C., *op. cit.* u bilj. 37, poglavlje 6.9.

- „Usko povezano sa sklonošću preuzimanju rizika je tolerancija…“[138]
- Za razliku od sklonosti preuzimanju rizika, tolerancija je taktična i precizna.[139]

Postoje različite definicije i pristupi definiranju pojma tolerancije prema riziku[140], a neki od njih mogu doprinijeti više konfuziji što taj pojam znači nego rasvjetljavanju značenja pojma.[141]

Zamislimo situaciju da je dopuštena vožnja do 70 km/h i da je ona naš apetit za rizikom. Vožnja više od 80 km/h zasigurno će nas dovesti do prekršajne kazne. Međutim, vožnja između 70 i 80 km određeni je raspon koji bismo možda mogli tolerirati u smislu da iznimno prihvaćamo takvu vožnju nadajući se da možda nećemo biti kažnjeni i da neće doći do nesreće. Toleranciju prema riziku možemo promatrati kao prihvatljivo odstupanje od sklonosti preuzimanju rizika (engl. *acceptable deviation from the organization's risk appetite*).[142] Maksimalne granice tolerancije ne smiju biti prijeđene uopće ili samo iznimno u slučaju izvanrednih okolnosti, ako je tolerancija izražena na način da su određene stroge granice tolerancije (engl. *hard limits*), a u slučaju tolerancije koja je izražena na način da su granice indikativne (engl. *soft limits*), ona djeluje kao smjernica za one kojima je upućena.[143] Upravo zbog različitih mogućnosti poimanja tolerancije prema riziku važno je da pravni izvori koji se koriste pojmom tolerancije prema riziku njega i definiraju.

3.4. Strategija upravljanja rizicima (engl. *risk management strategy*)

Strategija upravljanja rizicima kao interni akt društava, odnosno sastavni dio sustava upravljanja rizicima predviđena je, između ostalog, odredbama Zakona o leasingu, Zakona o

[138] Cit., COSO, *op. cit.* u bilj. 32, str. 62.
[139] *Ibid.*
[140] Vidi više u Manoukian, J. G., Risk appetite and risk tolerance: what’s the difference?, 2016., dostupno na https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference (posljednji pristup 5. siječnja 2024.).
[141] Yoe, C., *op. cit.* u bilj. 37, str. 202.
[142] Tako i Carmichael, M., Risk Appetite vs. Risk Tolerance: What is the Difference?, 2022., dostupno na https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/risk-appetite-vs-risk-tolerance-what-is-the-difference (posljednji pristup 1. ožujka 2024.). Tako i Chapple, M., Risk appetite vs. risk tolerance: How are they different, 2023., dostupno na https://www.techtarget.com/searchcio/feature/Risk-appetite-vs-risk-tolerance-How-are-they-different (posljednji pristup 1. ožujka 2024.). Tako i United Nations System, *op. cit.* u bilj. 119.
[143] United Nations System, *op. cit.* u bilj. 119, str. 23.

faktoringu, Zakona o tržištu kapitala, što pokazuje zastupljenost predmetne terminologije u hrvatskom pravnom sustavu.[144]

Strategija upravljanja rizicima općenit je plan na generalnoj razini koji ne sadržava tehničke detalje o upravljanju rizicima (engl. *high-level plan for risk management*).[145] Ona definira ciljeve koji se trebaju postići i načine njihova postizanja[146], ali na općenitoj razini u kontekstu načela.

Nadalje, strategija upravljanja rizicima može sadržavati informacije u vezi s tim koji se stupanj razvijenosti sustava upravljanja rizicima uspostavlja ili namjerava uspostaviti te vrijednosti koje će cjelokupnoj vrijednosti društva donijeti upravljanje rizicima.[147]

Strategija upravljanja rizicima može sadržavati terminologiju u vezi s rizicima koja služi uspostavi zajedničkog jezika za potrebe upravljanja rizicima, čime se postiže da svi dionici određenog društva dijele zajedničko shvaćanje pojma rizika. Naime, kako je navedeno, rizici se mogu promatrati samo kao opasnosti, ali i kao opasnosti i prilike. Stoga, strategija upravljanja rizicima može rasvijetliti stav/pristup društva s time u vezi. Je li kritični rizik isto što i rizik katastrofalne prirode, ovisit će o rječniku rizika koje upotrebljava pojedino društvo. Zajednički jezik odnosno rječnik rizika služi tomu da se omogući usklađeno prikupljanje podataka o rizicima.[148] Primjerice, uzmimo u obzir da tri osobe procjenjuju rizike u skladu s ljestvicom u okviru koje su ponuđene sljedeće kvalitativne vrijednosti: mali, srednji i umjeren rizik. Ako ne postoji konsenzus u vezi sa značenjima predmetnih pojmova, izgledno je da će se svaka od osoba voditi vlastitim shvaćanjem predmetnih pojmova (mali, srednji, visoki), što će u konačnici dovesti do toga da podatci koje prikuplja osoba zadužena za rizike budu neujednačeni, odnosno da potencijalni agregirani izvještaj o rizicima bude neusklađen.

Zamislimo situaciju društva koje zapošljava 50 zaposlenika u kojem je uprava društva od svojih zaposlenika zatražila identificiranje rizika društva. Može se dogoditi da jedan od zaposlenika pod pojmom rizika smatra isključivo rizike financijske prirode ne uzimajući u obzir rizike druge prirode poput reputacijskog rizika. Nadalje, neki od zaposlenika mogu

[144] Čl. 69., st. 2., toč. 1. Zakona o leasingu, čl. 64., st. 2., toč. 1. Zakona o faktoringu, čl. 30., st. 6. ZTK-a.
[145] Kampmann, A., *op. cit.* u bilj. 15, str. 83.
[146] *Ibid.*
[147] Hopkin, P.; Thompson, C., *op. cit.* u bilj. 16, str. 264.
[148] Kampmann, A., *op. cit.* u bilj. 15, str. 83.

smatrati da je potrebno identificirati samo one rizike za koje postoji relevantan stupanj ostvarenja u sljedećih godinu dana, ali ne i one rizike koji će se potencijalno ostvariti za tri ili više godina. Stoga, bez zajedničke terminologije u dijelu rizika upitno je u kojoj će mjeri sustav upravljanja rizicima biti efikasan.

Strategija upravljanja rizicima također služi kao sredstvo kojim se komunicira o namjeravanoj kulturi u vezi s rizicima koja se nastoji uspostaviti. Naime, ako strategija upravljanja rizicima sadržava odredbe koje naglašavaju važnost upravljanja rizicima, takva strategija smjerat će prema uspostavi kulture koju obilježava važnost svijesti o važnosti upravljanja rizicima. Strategija koja ističe važnost dijeljenja podataka i raspravu o rizicima utječe na uspostavu kulture slobodne komunikacije i transparentnosti. S time u vezi valja istaknuti da zapisana pravila koja se promatraju isključivo kao slova zapisana na papiru ne mogu stvoriti namjeravanu kulturu bez angažmana uprave i nadzornog odbora koji svojim ponašanjem šalju jasnu poruku da je upravljanje rizicima neizostavan dio određene korporativne kulture.[149]

O važnosti kulture rizika, a pogotovo u društvima koja djeluju u financijskoj industriji, govori tvrdnja da se slabosti u kulturi rizika često smatraju ključnim uzročnikom (engl. *root cause*) globalne financijske krize.[150]

4. OPĆI MODELI UPRAVLJANJA RIZICIMA

4.1. Uvod u opće modele

Jedno od sasvim praktičnih pitanja koja si društva mogu postaviti jest što ona moraju poduzeti kako bi organizacijski implementirala integrirano upravljanje raznim vrstama rizika te od kojih se etapa sastoji proces upravljanja rizicima. U razmišljanju o mogućnostima različitih vrsta implementacija upravljanja rizicima društva uzimaju u obzir procesne aspekte upravljanja rizicima, ali i organizacijske. To je sasvim logično zbog toga što proces upravljanja

[149] *Ibid.*, str. 87.
[150] Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture A Framework for Assessing Risk Culture, 2014., str. 1, dostupno na https://www.fsb.org/wp-content/uploads/140407.pdf (posljednji pristup 5. siječnja 2024.).

rizicima netko mora i obaviti/voditi/upravljati/nadzirati. Naravno, što manje zakonskih pravila o upravljanju rizicima postoji, to društva imaju veću „umjetničku“ slobodu kreiranja sustava upravljanja rizicima. Društva koja ne posluju u okviru financijske industrije imaju (naj)veću slobodu.

Na putu kreiranja i implementacije sustava upravljanja rizicima društva se susreću s mnoštvom tehničkih pitanja. Jedno od takvih može biti treba li društvo zaposliti glavnog menadžera rizika (osobu odgovornu za upravljanje rizicima), voditi registar rizika, na koji će način uprava i nadzorni odbor međusobno komunicirati o rizicima. „S obzirom na to da ne postoji jedinstveni stav kako provesti implementaciju integriranog upravljanja rizicima, sustavi integriranog upravljanja rizicima uvode se u različitim poduzećima na različite načine.“[151]

„Kako poduzeća ne bi lutala i kretala od nule prilikom uvođenja integriranog upravljanja rizicima, moguće je koristiti se standardima COSO ili ISO 31000, koji su osmišljeni kao neobavezne smjernice poduzećima koja žele uvesti integrirano upravljanje rizicima.“[152] Modeli COSO i ISO 31000 najčešće su korišteni modeli upravljanja rizicima prema svjetskoj anketi koju je provela Međunarodna organizacija za standardizaciju 2011. godine.[153] Oni su također jedan od najbolje uspostavljenih pristupa upravljanju rizicima.[154] Upravo se stoga u nastavku daje pregled COSO modela koji je objavljen 2004., a izmijenjen i dopunjen 2017. godine, te ISO standarda 31000 – Upravljanje rizicima – Smjernice[155] koji je izdan 2009., a izmijenjen i dopunjen 2018. godine. ISO 31000:2018 Smjernice o upravljanju rizicima objavila je međunarodna organizacija za standardizaciju, a COSO model organizacija *Committee of Sponsoring Organizations of the Treadway Commission* u okviru koje zajednički surađuju Američka knjigovodstvena asocijacija, Američki institut certificiranih javnih računovođa,

[151] Cit., Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 66.
[152] Cit., *ibid.*
[153] Str. 20, Giorgos, N., Diffusion of Enterprise Risk Management in Greek Companies, Piraeus, 2020., str. 20, dostupno na https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/13213/Nikas_1713.pdf?sequence=1 (posljednji pristup 2. veljače 2024.).
[154] Hopkin, P.; Thompson, C., *op. cit.* u bilj. 16, str. 56.
[155] Međunarona organizacija za standardizaciju izdala je četiri primarna izvora o upravljanju rizicima: ISO Guide 73:2009 Risk Management – Vocabulary, ISO 31000:2009 Risk Management – Principles and Guidelines (koji više nije na snazi), ISO /IEC 31010:2009 Risk Management – Risk Assessment Techiques, ISO 31000:2018 Risk Management – Guidelines.

Međunarodni financijski rukovoditelji, Institut upravljačkih računovođa i Institut internih revizora.[156]

4.2. Proces upravljanja rizicima prema COSO modelu

4.2.1. Faza identificiranja rizika

Jedan od koraka u procesu upravljanja rizicima jest faza identificiranja rizika.

Društvo identificira one rizike koji utječu na poslovne ciljeve društva i strategiju (plan kako ostvariti misiju, viziju i primijeniti temeljne vrijednosti)[157] te ih unosi u inventar rizika (engl. *inventory of risk*).[158]

Inventar rizika (mapa rizika / registar rizika) popis je rizika koji mogu utjecati na poslovanje društva.[159] Pojedinačno utvrđeni rizici mogu se grupirati u različite kategorije i potkategorije.[160] Inventar rizika može sadržavati i naznaku cilja na koji rizik utječe.[161] Naime, iz inventara rizika može biti vidljivo na koje poslovne ciljeve društva određeni rizik utječe.[162] Može se dogoditi da jedan rizik utječe na samo jedan poslovni cilj društva, a da neki drugi rizik utječe na više različitih poslovnih ciljeva društva.[163]

Pristupi su identificiranju rizika različiti.[164] Tako, primjerice, društvu stoji na raspolaganju raznovrstan asortiman alata koji će poslužiti identificiranju rizika. Za potrebe identificiranja rizika može se poslužiti umjetnom računalnom inteligencijom (engl. *cognitive computing*), zatim povijesnim podatcima (engl. *historical data tracking*) koji mogu poslužiti za predviđanje budućih događaja, intervjuima/razgovorima koji se provode s pojedincem ili skupinom ljudi, analizama procesa (raščlamba i grafički prikaz pojedinih etapa određenog

[156] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 69.
[157] COSO, *op. cit.* u bilj. 32, str. 67.
[158] *Ibid.*, str. 67.
[159] *Ibid.*, str. 68.
[160] *Ibid.*, str. 68.
[161] *Ibid.*, str. 68.
[162] *Ibid.*
[163] *Ibid.*
[164] *Ibid.*, str. 69.

procesa s kojima se povezuju pojedinačno identificirani rizici), skupnim radionicama na kojima sudjeluju različiti eksperti itd.[165]

Osim što je rizike potrebno navesti u inventar rizika u smislu popisati ih i naznačiti na koje poslovne ciljeve utječu, rizike je potrebno precizno opisati[166] koristeći se standardiziranim strukturama rečenica[167] za koje se sastavljač inventara rizika opredijelio. Drugim riječima, opisi moraju biti prezentirani na način da su razumljivi osobama koje će se njima služiti. Time se osigurava ujednačeno tumačenje značenja rizika zapisanih u inventaru rizika.

4.2.2. Faza procjene rizika

Nakon identifikacije rizika, u okviru procesa upravljanja rizicima, slijedi faza njegove procjene.[168] Procjena ozbiljnosti rizika provodi se uzimajući u obzir dva ključna elementa u vezi s rizicima: razina vjerojatnosti (engl. *likelihood*) da će se rizik ostvariti i jačina njegova utjecaja (engl. *impact*).[169] Utjecaj rizika na poslovne ciljeve društva može biti pozitivan ili negativan.[170] Navedena tvrdnja u skladu je sa spomenutim da se rizici mogu promatrati i kao prilike. Vjerojatnost ostvarenja rizika može se izraziti kvalitativno, kvantitativno i vremenski. Konkretno, tvrdnja da je vjerojatnost ostvarenja rizika mala/srednja/velika primjer je kvalitativnog prikazivanja vjerojatnosti ostvarenja rizika. Tvrdnja da je vjerojatnost ostvarenja rizika 70 % primjer je kvantitativnog izražavanja vjerojatnosti ostvarenja rizika. Tvrdnja da postoji mogućnost poplave pojedinog područja jedanput u tri godine vremenski je prikaz razine vjerojatnosti. Naravno, navedene mogućnosti izražavanja ozbiljnosti rizika mogu se i kombinirati.

U kontekstu procjene bitnosti rizika valja upozoriti na sljedeće.

Pogled sa 100, zatim 500, pa s 1000 te naposljetku 2000 metara nadmorske visine koji gleda u istom smjeru nije isti. Tako je i u kontekstu upravljanja rizicima. Uzmimo primjerice društvo koje proizvodi plastične čaše, a u isto vrijeme posluje kao hotel te pruža usluge

[165] *Ibid.*, str. 69 i 70.
[166] *Ibid.*, str. 70.
[167] *Ibid.*, str. 71.
[168] *Ibid.*, str. 72.
[169] *Ibid.*
[170] *Ibid.*, str. 74.

kemijskog čišćenja širokoj javnosti. Sve tri različite poslovne jedinice u svojem poslovanju susrest će se s nekim istim, ali i različitim rizicima. Rukovoditelji poslovanja tih triju različitih poslovnih jedinica, kada se ne preklapaju, imaju pregled rizika na poslovne ciljeve tih konkretnih poslovnih jedinica. Međutim, sasvim logično, nameće se pitanje kako će pojedinačni rizici svake pojedinačne jedinice, kada se svi oni uzmu zajednički u obzir, međusobno povezani, utjecati primjerice na cjelokupnost poslovanja društva na najvišoj razini, odnosno koja je razina ozbiljnosti pojedinih rizika na razini društva. Isto je primjenjivo u okviru odnosa između društava kćeri i majke koja čine istu skupinu. Naime, određeni rizik može biti prihvatljiv za svaku poslovnu jedinicu pojedinačno (ili društvo kći), ali kada se uzme u obzir njegova prisutnost u sve tri poslovne jedinice, na razini cjelokupnog poslovanja društva (ili društvo majku), takav rizik možda neće biti prihvatljiv.[171] Može se dogoditi i obratan slučaj. Za jednu poslovnu jedinicu možda će konkretan rizik biti neprihvatljiv, no na razini cjelokupnog društva rizik će ulaziti u granice sklonosti preuzimanju rizika.[172]

Prisjetimo se tvrdnje da pogled nije isti sa 100, 500, 1000 te 2000 metara nadmorske visine. Za potrebe ovog rada četiri različite nadmorske visine promatrat ćemo kao četiri različita „vidikovca rizika“ o kojima može ovisiti i procjena bitnosti/ozbiljnosti rizika. Najniži pregled rizika pregled je pojedinačnih rizika. Zatim slijedi pregled rizika koji se grupiraju. Treća je razina pregleda rizika povezivanje rizika s poslovnim ciljevima društva na koje rizici utječu. Četvrta razina promatra cjelokupnost rizika u njihovoj međusobnoj povezanosti. Takav pregled rizika, odnosno četvrta razina pregleda rizika, naziva se portfeljni pregled rizika (engl. *portfolio view*).[173] Postojanje portfeljnog pregleda rizika upravo je jedna od najčešće spominjanih karakteristika integriranog upravljanja rizicima kao višeg stupnja razvijenosti upravljanja rizicima u odnosu prema tradicionalnim modelima upravljanja rizicima utemeljenog na „silosima“.

4.2.3. Faza prioritizacije rizika

[171] *Ibid.*, str. 84.
[172] *Ibid.*
[173] *Ibid.*, str. 86.

Nakon utvrđenja rizika i procjene njegove ozbiljnosti slijedi faza prioritizacije rizika. Prioritizacija rizika znači odabir onih rizika kojima će se društvo najprije posvetiti na način da će na njih primijeniti odgovarajuće mjere iliti odgovore. Prioritizirati rizike znači odrediti redoslijed primjene odgovora/mjera. Kao i u svim sferama života u okviru kojih smo ograničeni i vremenskim i novčanim resursima, faza prioritizacije raščlamba je rizika redoslijedom planiranog utroška naših vremenskih i novčanih kapaciteta. Logično je pretpostaviti da će društvu, u kontekstu ograničenih vremenskih, novčanih kapaciteta te kapaciteta radnog osoblja, prioritetan biti onaj rizik čija je vjerojatnost ostvarenja iznimno visoka i čiji je utjecaj iznimno negativan za razliku od rizika čija je vjerojatnost ostvarivanja kao i potencijalno negativan učinak iznimno malena. I vremenska komponenta ostvarenja rizika ima važnu ulogu. Naime, ako će se određeni propis koji zahtijeva od društva prilagodbu određenih procesa početi primjenjivati za tri godine, konkretni rizik neusklađenosti s propisom možda i neće zahtijevati prioritetno rješavanje jer će se s time društvo možda „uhvatiti ukoštac“ sljedeće godine. Kapacitet za rizik kao maksimalna količina rizika koje je društvo sposobno apsorbirati u svom poslovanju također je kriterij za prioritizaciju rizika. Rizici čije vrijednosti prelaze kapacitet društva za rizik zasigurno zavređuju najveću prioritizaciju (žurno reagiranje) za razliku od rizika koji se nalaze u omjerima kapaciteta za rizik. Brzina kojom ostvareni rizik utječe na društvo (engl. *velocity*), zatim stupanj ustrajnosti utjecaja (engl. *persistence*) te mogućnost oporavka također su kriteriji koji se uzimaju u obzir za potrebe prioritizacije rizika.[174] Slijedom navedenog, rizik koji kada se ostvari iznimno brzo pogađa društvo, čiji negativni utjecaj traje dugo te je društvu teško vratiti se u normalan tijek ostvarivanja poslovnih ciljeva, zasigurno zaslužuje biti prioritiziran.

U prioritizaciji rizika uprava / visoko rukovodstvo društva uzimaju u obzir i sklonost društva preuzimanju rizika. Rizici koji se približavaju gornjim granicama sklonosti preuzimanju rizika, a pogotovo rizici koji prelaze tu gornju granicu, u pravilu bivaju prioritizirani.[175]

4.2.4. Faza odabira i provedbe odgovarajućeg odgovora na rizik

[174] *Ibid.*, str. 79.
[175] *Ibid.*, str. 80.

Odabir i provedba odgovarajućeg odgovora na rizik zadaća je uprave / višeg rukovodstva (engl. *management*).[176] U odabiru odgovora na rizik uzima se u obzir ozbiljnost rizika i njegova prioritizacija, odnosno utvrđenja koja proizlaze iz prethodnih faza procesa upravljanja rizicima.[177]

Reakcije odnosno odgovori na rizik mogu se podijeliti u sljedeće kategorije odgovora/reakcija na rizik: prihvaćanje (engl. *accept*), izbjegavanje (engl. *avoid*), praćenje (engl. *pursue*), smanjenje (engl. *reduce*) i dijeljenje (engl. *share*) rizika.[178]

Prihvatiti rizik znači da je društvo prihvatilo rizik a da nije pokušalo smanjiti, odnosno da nije planiralo smanjiti njegovu razinu ozbiljnosti.[179] U pravilu, prihvaćanje rizika bit će primjeren odgovor na rizik u onim situacijama kada je razina ozbiljnosti konkretnog rizika u okviru sklonosti za preuzimanje rizika. Uzmimo primjerice da društvo svoje poslovne partnere bonitetno ocjenjuje na način da ocjena 5 znači nizak rizik stečaja poslovnog partnera, ocjena 3 umjeren rizik stečaja, dok ocjena 1 znači iznimno visok rizik stečaja poslovnog partnera. Kada je sklonost preuzimanju rizika kod odabira poslovnih partnera obilježena umjerenim rizikom, društvo može poslovati s poslovnim partnerima koji su ocijenjeni bonitetnom ocjenom između 3 i 5. U takvim slučajevima društvo prihvaća rizike koji su u okviru granica sklonosti za preuzimanje rizika i nije dužno primijeniti posebne mjere da bi smanjilo bitnost/ozbiljnost rizika. U slučaju da je potencijalni poslovni partner ocijenjen ocjenom 1, a takva ocjena prelazi sklonost preuzimanju rizika, društvo bi trebalo izbjeći povećani rizik na način da ne posluje s takvim poslovnim partnerom (ako ne želi prijeći sklonost preuzimanju rizika). Alternativni pristup koji je dostupan društvu jest pokušaj smanjenja ozbiljnosti rizika koji je povezan s konkretnim potencijalnim poslovnim partnerom koji je ocijenjen krajnje rizičnim. Društvo bi smanjenje rizičnosti moglo postići traženjem određenog novčanog pologa, bjanko mjenice ili tomu sličnog instrumenta osiguranja. Naime, sredstvo osiguranja plaćanja zasigurno može smanjiti potencijalni negativni učinak rizika u slučaju da druga ugovorna strana ne ispuni svoje obveze ili upadne u financijske poteškoće. Sklapanje ugovora o osiguranju evidentan je primjer

[176] *Ibid.*, str. 81.
[177] *Ibid.*
[178] *Ibid.*
[179] *Ibid.*

dijeljenja rizika. Sklapanjem ugovora o osiguranju teret snošenja rizika više nije samo na društvu nego i na osiguravajućem društvu. U slučaju nastupanja osiguranog slučaja društvo može očekivati isplatu određenog novčanog iznosa.

Iako nije riječ o klasičnom tipu odgovora na rizik, društvo može, u slučaju da su određeni poslovni ciljevi (npr. povećanje dobiti za 80 % u odnosu na prošlu godinu lansiranjem i prodajom inovativnog proizvoda) povezani s razinom ozbiljnosti rizika na koje društvo načelno ne pristaje (očiti nerazmjer sa sklonošću preuzimanju rizika), revidirati odnosno ponovno razmotriti poslovne ciljeve. Naime, pretpostavka je da ako društvo u vrlo kratkom razdoblju planira povećati dobit društva za 80 % u odnosu na prijašnje usporedno razdoblje, da takav poslovni cilj najvjerojatnije neće biti moguće ostvariti bez preuzimanja „većih" rizika. To sugerira da je takav poslovni cilj povezan s većom sklonošću preuzimanju rizika. Ako takav poslovni cilj odredi društvo koje je potpuno nesklono preuzimanju rizika, jasno je vidljiva njihova međusobna neodrživost pa je potrebno mijenjati ili sklonost preuzimanju rizika ili poslovne ciljeve.[180] Naravno, u slučaju da društvo ostane pri agresivnijim poslovnim ciljevima koji zahtijevaju veću sklonost preuzimanju rizika, društvo bi trebalo s time uskladiti (povećati) svoju sklonost preuzimanju rizika.[181] Iz toga proizlazi nedvojbena međupovezanost između poslovnih ciljeva društva i sklonosti preuzimanju rizika.

Pojmove inherentni rizik (engl. *inherent risk*) i stvarni rezidualni rizik (engl. *actual residual risk*) najlakše je objasniti u kontekstu primjene odgovora na rizik. Inherentni je rizik onaj rizik na koji (još) nije primijenjena mjera kojom bi se njegova razina ozbiljnosti promijenila, odnosno razina rizika koja je postojala prije primjene odgovora na rizik.[182] Inherentni rizik može se promatrati kao izvorni, prirodni, početni rizik prije primjene mjera smanjenja rizika ili dijeljenja s drugom osobom (primjerice s osiguravajućim društvom). Kada je inherentni rizik u granicama sklonosti društva preuzimanju rizika, društvo može takav rizik prihvatiti. Kada inherentni rizik prelazi gornju granicu sklonosti preuzimanju rizika (te granicu prihvatljivog odstupanja tolerancije ako je ona određena), društvo će biti sklono smanjiti rizik u prihvatljive okvire sklonosti preuzimanju rizika. Primjerice, a referirajući se na navedeni

[180] *Ibid.*, str. 81.
[181] *Ibid.*
[182] *Ibid.*, str. 77.

primjer u vezi s bonitetnim ocjenjivanjem poslovnih partnera, društvo koje je ocijenilo potencijalnog partnera ocjenom 1, ocijenilo je da je inherentni rizik da poslovni partner neće ispuniti svoju obvezu iznimno visok. Ako se od poslovnog partnera unaprijed zatraži određeno sredstvo osiguranja njegove obveze, to će zasigurno umanjiti potencijalni negativni učinak rizika ako se ostvari, čime se zapravo konačna ocjena konkretnog rizika smanjuje na ocjenu bližu umjerenom riziku, čime se stvarni rezidualni rizik možebitno dovodi u granice sklonosti preuzimanju rizika. Iz toga se nazire pojašnjenje pojma „stvarni rezidualni rizik", a to je da je to onaj rizik koji preostaje nakon što je društvo poduzelo mjere da ga umanji.[183] Društvo će nastojati dovesti razinu rezidualnog rizika u okviru granica sklonosti društva za preuzimanje rizika.[184] U odlučivanju o odabiru najprikladnijeg odgovora na rizik uzimaju se u obzir i sljedeći faktori: poslovni kontekst, troškovi i koristi, očekivanja.[185] Uzmimo društvo čije su dionice uvrštene na uređenom tržištu, ili regulirani subjekt nadzora iz financijske industrije poput kreditne institucije ili investicijskog društva koji su u skladu s pravnim propisima Republike Hrvatske podvrgnuti nadzoru nadležnih nacionalnih nadzornih tijela (primjerice Hrvatske agencije za nadzor financijskih usluga i/ili Hrvatske narodne banke). Takvi subjekti nadzora, koji su u cijelosti ili u određenom dijelu poslovanja podvrgnuti specijalnim propisima financijskog sektora, svjesni su ovlasti nadležnih nacionalnih nadzornih tijela, mogućnosti provedbe neposrednih i posrednih nadzora te mogućnosti da budu, između ostalog, i novčano kažnjeni u slučaju utvrđenja povreda određenih obveza koje proizlaze iz propisa ili čak i da im odobrenje za rad bude oduzeto. Takav poslovni kontekst (normiranost te nadzor i mogućnost novčanog kažnjavanja) utječe na društvo tako da će predmetna društva (osim minimalnih zakonskih obveza) biti sklona investirati znatnija sredstva (primjerice zaposliti veći broj stručnjaka) kako bi (dodatno) smanjila rizik potencijalne neusklađenosti s propisima koji reguliraju financijsku industriju. Društva iz financijske industrije koja internacionalno posluju, primjerice istodobno u Hrvatskoj, Njemačkoj i Luksemburgu, usporedit će prakse nadležnih tijela iz Hrvatske, Njemačke i Luksemburga te u slučaju utvrđenja da je jedno nacionalno tijelo sklono kažnjavati iznimno visokim novčanim kaznama, a druga dva tijela iznimno niskim

[183] *Ibid.*
[184] *Ibid.,* str. 82.
[185] *Ibid.*

kaznama za povrede iste vrste, pretpostavka je da će društvo biti sklonije uložiti više sredstava u odgovore na rizik za poslovanje u onoj zemlji čije je nadležno nacionalno tijelo rigoroznije u kažnjavanju svojih subjekata nadzora. Iz navedenih primjera proizlazi da se poslovni kontekst kao faktor koji se uzima u obzir u odlučivanju o odabiru najprikladnijeg odgovora na rizik može razlikovati ovisno o tome kojom se vrstom djelatnosti društvo bavi, ali i o tome kakva je nadzorna praksa pojedine države (nadležnih nadzornih tijela), što je posebice relevantno u slučaju društava koja prekogranično posluju.

Odgovor na rizik košta. Da je tomu tako, najbolje je vidljivo u slučaju kada društvo na povećanu mogućnost poplava koje mogu naštetiti njegovu poslovanju (rizik) odgovori sklapanjem ugovora o osiguranju s osiguravajućim društvom (dijeljenje rizika). Sklapanje police osiguranja nije besplatno. U odlučivanju kako će se reagirati na rizik, društvo će zasigurno prije ugovaranja police osiguranja odvagnuti njezine troškove i potencijalne koristi koje će društvo imati (naknada štete) u slučaju da nastupi osigurani slučaj (rizik).

Iako se na prvu može činiti paradoksalno, odabrani odgovor na rizik sam po sebi stvara nove rizike. Tako je i s lijekovima koji se uzimaju u slučaju bolesti. Iako lijek liječi, on nosi sa sobom određeni rizik (određene nuspojave). Tako je i s odgovorom na rizik. Stoga, u odabiru odgovarajućeg odgovora na rizik društvo uzima u obzir kakve rizike povlači za sobom izabrani odgovor na rizik. Uzmimo primjerice ugovaranje police osiguranja od poplava. Novonastali je rizik u vezi sa sklopljenom policom osiguranja hoće li društvo moći isplaćivati premije osiguranja, odnosno hoće li rashodi zbog „skupe“ ugovorene police osiguranja biti otegotni za financijsku održivost poslovanja društva.[186]

Primjeri očekivanja kao faktor koji se može uzeti u obzir u odabiru odgovora na rizik jesu očekivanja zainteresiranih dionika. Očekivanja u vezi s razinom sklonosti društva za preuzimanjem rizika mogu proizlaziti od članova društva, ali i od ostale zainteresirane javnosti i nadležnih regulativnih tijela. Primjerice, pretpostavka je da će u razdobljima financijskih kriza i geopolitičkih razmirica očekivanja nadležnih nacionalnih tijela prema subjektima nadzora biti obilježena naglašenijom opreznošću i konzervativnošću u preuzimanju rizika (pogotovo u kontekstu investiranja i likvidnosti).

[186] Vidi više u *ibid.,* str. 83.

4.2.5. Kontinuirano praćenje i revizija

Vrijeme ne stoji, ono neprekidno teče te uvodi u živote ljudi te u „životne cikluse“ društava određene promjene. Kontrolni zdravstveni pregled fizičke osobe u pravilu se provodi svake godine jer zdravstvena slika možda više i ne odgovara aktualnom stanju na koje je utjecao protek vremena.

U tom je smislu sasvim razumljivo da rizici kojima je društvo izloženo na današnji datum sigurno nisu identični onima kojima je društvo bilo izloženo prije nekoliko godina niti će biti identični onima kojima će društvo biti izloženo za godinu dana. Naime, valja voditi računa o tome da društva posluju u dinamičnom okružju sklonom promjenama.[187] Rizici koje donosi rat u Ukrajini i Gazi (znatne promjene u geopolitičkoj sferi) uvelike su utjecali na pristup upravljanju geopolitičkim rizicima na način da je u trenutku pisanja ovog rada upravljanje njima važnije/relevantnije nego prije bitnih promjena na geopolitičkoj sceni. Sasvim je logično pretpostaviti da inventar rizika s vremena na vrijeme valja ažurirati te procijenjene rizike ponovno procjenjivati. Naime, protekom vremena događaju se promjene u društvu i izvan društva koje utječu na to da jedni rizici postaju manje relevantni, dok bitnost drugih raste.

Promjene koje dovode do nastanka novih bitnih rizika ili značajnih promjena u bitnosti postojećih rizika nazivaju se značajnim promjenama (engl. *substantial changes*).[188] Značajne promjene mogu biti interne ili eksterne.[189] Primjeri internih značajnih promjena jesu znatno širenje poslovanja (npr. preuzimanjem društva) te upotreba tehnoloških inovacija u poslovanju društva.[190] Značajne promjene koje proizlaze iz vanjskog okružja mogu biti povezane s regulativnim promjenama te promjenama u općem makroekonomskom okružju.[191] Primjena nove uredbe Europske unije koja zahtijeva od društva znatna usklađenja, investicije i operativne promjene bit će razlog radi kojeg će trebati napraviti novu ili ažurirati postojeću analizu rizika.

---

[187] Biolcheva, P., The place of artificial intelligence in the risk management process, SHS Web of Conferences 120, 02013 (2021), BUSINESS AND REGIONAL DEVELOPMENT, 2021.
[188] COSO, *op. cit.* u bilj. 32, str. 90.
[189] *Ibid.*
[190] *Ibid.*, str. 90.
[191] *Ibid.*, str. 91.

Nadalje, uvrštenje dionica društva na uređeno tržište Zagrebačke burze zahtijevat će od društva aktivniji pristup upravljanju rizicima usklađenosti koji proizlaze iz propisa koji uređuju postupanje s povlaštenim informacijama (obveza objavljivanja povlaštenih informacija, vođenje popisa upućenih osoba, primjena odredbi o zabrani zlouporabe tržišta) pa će društvo biti sklono u okviru svog sustava upravljanja rizicima implementirati preventivne kontrole provjere transakcija rukovoditelja, članova uprave i nadzornog odbora društva, ograničenja kruga osoba koje imaju pristup povlaštenim informacijama kako bi rizik nedopuštenih transakcija sveo na što manju mjeru. Preuzimanje novog društva (širenje poslovanja) tražit će od društva preuzimatelja aktivnije razmatranje utjecaja rizika kojima je izloženo preuzeto društvo u mjeri u kojoj takvi rizici utječu na društvo preuzimatelja, što će utjecati zasigurno na potrebu ažuriranja registra rizika.

Osim rizika, može se kontinuirano pratiti i revidirati i sam proces, odnosno sustav upravljanja rizicima.

Kontinuiranim praćenjem i revizijom pojedinih elemenata procesa upravljanja rizicima ili cjelokupnog procesa i/ili sustava upravljanja rizicima društvo zapravo kontinuirano utvrđuje mogućnosti poboljšanja upravljanja rizicima. To omogućuje da sustav (odnosno njegovi dijelovi) napreduje, razvija se i postaje zreliji.[192] Čak i društvo koje ima iznimno razvijen sustav upravljanja rizicima može ga unaprijediti, odnosno učiniti ga efikasnijim.[193] Ta je tvrdnja logična i u skladu je s konceptom cjeloživotnog učenja primjenjivog za fizičke osobe (ali i društva) u okviru kojeg pojedinac za vrijeme čitava svojeg života uči, stječe nova znanja te se konstantno profesionalno razvija. Kako pojedinci uče na vlastitim pogreškama, tako i društva uče na pogreškama iz prošlosti (engl. *historical shortcomings*).[194] Naime, pogreške iz prošlosti koje je društvo utvrdilo mogu biti iskorištene za unapređenje sustava upravljanja rizicima.[195]

Koliko i kako sustav upravljanja rizicima može sazreti, prikazuje se u nastavku.

Društvo koje se tek počelo upoznavati s modelima upravljanja rizicima, koje nema uspostavljen registar rizika, zaposlenog glavnog stručnjaka za rizike ni uspostavljene modele procjene bitnosti rizika kao ni uspostavljene linije obavještavanja o rizicima unutar društva,

[192] *Ibid.*, str. 95.
[193] *Ibid.*
[194] *Ibid.*
[195] *Ibid.*

takvo društvo ili nema razvijen sustav upravljanja rizicima ili je njegova razvijenost u poprilično niskoj, jednostavnoj i početnoj fazi uspostave upravljanja rizicima da je upitno može li se uopće tvrditi da je uspostavljen „sustav“ upravljanja rizicima. S druge strane, društvo u kojem se za članove nadzornog odbora, uprave i ostalog višeg rukovodstva traži da imaju napredna znanja u području upravljanja rizicima, svaki zaposlenik razumije i postupa u skladu s „kulturom“ društva u vezi s rizicima koju obilježava odgovornost svakog zaposlenika za preuzeti rizik, uspostavljene su linije izvještavanja o rizicima, pravodobno se identificiraju i procjenjuju rizici, postoje interni dokumenti koji propisuju sklonost preuzimanju rizika, uzimaju se u obzir sve vrste rizika relevantne za društvo (ne samo financijski rizici), pravodobno se ažuriraju registri rizika, takvo će društvo imati zasigurno zreliji/ razvijeniji sustav upravljanja rizicima. Hoće li određeno društvo imati manje ili više razvijeno upravljanje rizicima, ovisi o elementima/atributima/karakteristikama koje je društvo prihvatilo/implementiralo u okviru (sustava) upravljanja rizicima. Postojanje odbora za rizike i/ili posebnog stručnjaka zaduženog za rizike zasigurno je jedan od mogućih elemenata/atributa/karakteristika koji sugeriraju na viši stupanj zrelosti upravljanja rizicima. Prvi modeli koji služe za procjenu stupnja razvijenosti upravljanja rizicima počeli su se razvijati devedesetih godina prošlog stoljeća kada je prvi takav model razvio dr. David A. Hillson 1997. godine.[196, 197]

Viši stupanj zrelosti upravljanja rizicima evolucijsko je stanje koje je rezultat procesa njegova kontinuiranog poboljšanja. Kreiranje i korištenje modela za procjenu zrelosti (razine napretka) sustava upravljanja rizicima temeljeno je na pretpostavci da postoje predvidljive faze promjena u društvu koje su put od početnog stadija do potpune zrelosti. Modeli procjene stupnja razvijenosti upravljanja rizicima (engl. *risk management maturity models;* dalje u tekstu: RMMM) omogućuju utvrditi tehničku razinu i razvoj procesa upravljanja rizicima. Oni također omogućuju identificiranje područja konkretnog sustava upravljanja rizicima, odnosno pojedine etape procesa upravljanja rizicima kojima je potrebno poboljšanje.

[196] Bak, S.; Jedynak, P., Risk Management Maturity: A Multidimensional Model, Oxon, 2023., str. 1–24.
[197] Hillson, D. A., Towards a Risk Maturity Model, The international Journal of Project & Business Risk Management, Vol. 1, No. 1, 1997., str. 35–45, dostupno na https://risk-doctor.com/wp-content/uploads/2020/06/RMM-IJPBRM-Mar97.pdf (posljednji pristup 15. veljače 2024.).

Danas postoji mnoštvo različitih RMMM-ova koji funkcioniraju na način da svaki model ima propisane atribute za svaku razinu zrelosti upravljanja rizicima koja se procjenjuje.[198] Primjerice, ako konkretni RMMM za najvišu razinu zrelosti upravljanja rizicima zahtijeva ispunjavanje minimalno 45 određenih atributa od sveukupno 50, društvo koje ispunjava minimalno 45 atributa po predmetnom modelu nosit će najvišu razinu razvijenosti sustava upravljanja rizicima. Ti modeli dijele se na sveobuhvatne modele (engl. *comprehensive models*) i na funkcionalne modele (engl. *functional models*).[199] Sveobuhvatni modeli primjenjuju se kod procjene zrelosti općeg upravljanja rizicima (neovisno o vrsti rizika) za razliku od funkcionalnih modela za procjenu funkcionalnog upravljanja pojedinim vrstama rizika u okviru primjerice upravljanja kvalitetom, projektom, informacijskom sigurnošću itd.[200]

Ono što je zajedničko RMMM-ovima jest da sadržavaju setove atributa poput određenih karakteristika čije se postojanje treba procijeniti kako bi se utvrdila razina zrelosti sustava upravljanja rizicima.[201] Neki RMMM-ovi počivaju na samoprocjeni društva, a neki na angažmanu vanjskog stručnjaka (eksterna evaluacija) ili kombinaciji.[202] U većini modela[203] koristi se ljestvica od pet razina zrelosti upravljanja rizicima gdje razina 1 označava postojanje određenog, ali nespecifičnog i neformaliziranog pristupa upravljanju rizicima društva.[204] Najniža razina razvijenosti upravljanja rizicima zove se inicijalna, *ad hoc* ili naivna.[205] Najviša razina razvoja sustava upravljanja rizicima zove se optimizirana, vodeća, napredna, odlična, inteligentna, ambiciozna (engl. *aspirational*).[206] Da bi društvo poboljšalo trenutačnu razinu zrelosti sustava upravljanja rizicima i prešlo u višu razinu, društvo mora zadovoljiti sve kriterije više razine. U procjeni koliko je razvijen pojedini sustav upravljanja rizicima uzima se u obzir jesu li i u kojoj mjeri ispunjeni kriteriji, odnosno atributi u vezi s procesom upravljanja rizicima.[207] Proces upravljanja rizicima i komunikacija jedni su od najčešće korištenih kriterija za utvrđivanje razine zrelosti upravljanja rizicima. U kontekstu procesnih kriterija uzima se u

[198] Bak, S.; Jedynak, P., *op. cit.* u bilj. 196, str. 5.
[199] *Ibid.*, str. 11 i 12.
[200] *Ibid.*
[201] *Ibid.*, tablica 1.2., str. 14–17.
[202] *Ibid.*, str. 12.
[203] U odnosu na 34 modela koja su predmet analize u *ibid.*
[204] *Ibid.*, str. 18.
[205] *Ibid.*, tablica 1.3., str. 19 i 20.
[206] *Ibid.*
[207] *Ibid.*, tablica 1.2., str. 14.

obzir utvrđuje li društvo rizike, zatim analizira li ih / procjenjuje njihovu bitnost, kako se oni kontinuirano nadziru te kako se u vezi s njima komunicira. Prema nekim modelima, da bi se uopće moglo tvrditi da društvo upravlja rizicima na najnižoj inicijalnoj razini, potrebno je da postoji barem izvještaj o upravljanju rizicima.[208] Kako bi se moglo prijeći na drugu razinu zrelosti, uz izvještaje o rizicima, društvo treba imati kadar koji će biti zadužen za upravljanje rizicima te resurse (primjerice oprema, novac) namijenjene za upravljanje rizicima. Prema RMMM-u koji su razvili Proença, Estevens, Vieira i Borbinha, za treću razinu zrelosti sustava upravljanja rizicima uspostavljeno je 26 kriterija.[209] Neki su od kriterija da se aktivnosti u vezi s upravljanjem rizicima u pisanom obliku bilježe, društvo je definiralo sklonost preuzimanju rizika, rizici se identificiraju, opisuju i procjenjuju, postoji sustav prioritizacije rizika (u kontekstu odgovora na rizik), postoji procedura za utvrđivanje pozitivnih učinaka (prilika) koji proizlaze iz rizika, važu se troškovi/koristi namjeravanih odgovora na rizik, za svaki rizik utvrđena je odgovorna osoba, komunikacija i konzultacije implementirane su u sve aktivnosti upravljanja rizicima.[210]

U najvišem stupnju razvoja (razina 5) društvo je sposobno identificirati područja koja se mogu poboljšati te odabrati i implementirati poboljšanja.[211] Na takvoj visokoj razini razvijenosti društvo neprestano unapređuje i razvija proces upravljanja rizicima, čime zapravo znanstveno doprinosi razvoju upravljanja rizicima kao znanosti.[212] Visoka zrelost sustava upravljanja rizicima dovodi do povećanja vrijednosti društva.[213]

Prema mjeri razvijenosti sustava integriranog upravljanja rizicima u poduzećima (ERM indeks) koji su razvili Miloš Sprčić i suradnici, ovisno o ispunjavanju 14 karakteristika, ovisit će razina razvijenosti sustava integriranog upravljanja rizicima. Kriteriji su: „imenovanje glavnog menadžera rizika u poduzeću, postojanje zasebne organizacijske jedinice zadužene za upravljanje rizicima u poduzeću, postojanje službene politike i procedure upravljanja rizicima, jasno definiranje apetita prema riziku poduzeća, primjena COSO okvira za upravljanje

[208] Proença, D.; Estevens, J.; Vieira, R.; Borbinha, J., Risk Management: A Maturity Model Based on ISO 31000, 2017., *IEEE 19th Conference on Business Informatics (CBI)*, Thessaloniki, Grčka, 2017., 99–108.
[209] *Ibid.*
[210] *Ibid.*
[211] Bak, S.; Jedynak, P., *op. cit.* u bilj. 196, str. 54 i 55.
[212] *Ibid.*
[213] *Ibid.*

rizicima, primjena ISO 31000 okvira za upravljanje rizicima, primjena integrirane analize i integriranog upravljanja svim rizicima kojima je poduzeće izloženo, utvrđivanje korelacija među rizicima i zajedničkog učinka skupa rizika, utvrđivanje kvantitativnih učinaka koje rizici mogu imati na ključne pokazatelje rizika, održavanje radionica na kojima menadžeri raspravljaju o izloženosti rizicima i strategijama upravljanja rizicima, rangiranje rizika kojima je poduzeće izloženo u mapu rizika prema kriterijima pojavljivanja i značajnosti, postojanje plana odgovora na rizike za sve rizične događaje, barem jednom godišnje podnošenje formalnog izvještaja o upravljanju rizicima upravi i nadzornom odboru poduzeća, praćenje ključnih pokazatelja rizika, orijentiranih na rizike u nastajanju".[214]

Jedna od kritika koja se odnosi na RMMM-ove je ta da su oni „korak po korak recepti" (engl. *step-by-step recipes*) koji previše pojednostavnjuju (engl. *oversimplify*) stvarno stanje te se dovodi u pitanje njihova primjenjivost u praksi te korisnost.[215]

4.3. Usporedba procesa upravljanja rizicima po COSO modelu integriranog upravljanja rizicima i modelu ISO 31000:2018 upravljanja rizicima

Uzimajući u obzir da su COSO ERM i ISO 31000:2018 dva najzastupljenija modela upravljanja rizicima, s ciljem dobivanja spoznaja o procesu upravljanja rizicima potrebno ih je usporediti i utvrditi njihove sličnosti i razlike. Takav pristup omogućuje stvaranje zaključka o tome koje su faze upravljanja rizicima općenito prihvaćene, odnosno najzastupljenije u procesima upravljanja rizicima. S obzirom na to da se (kako će biti detaljnije i objašnjeno u nastavku) COSO ERM i ISO 31000:2018 u bitnim fazama procesa upravljanja rizicima poklapaju, u nastavku se odmah pristupa njihovoj usporedbi bez zasebna objašnjavanja modela ISO 31000:2018.

Faza identificiranja rizika i po COSO modelu i po ISO 31000 jedan je od stadija upravljanja rizicima. COSO model i ISO 31000 modeli su upravljanja rizicima koji se mogu primjenjivati na sve vrste rizika (opći modeli). Naime, ni COSO model ni ISO 31000 ne

[214] Cit., Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 240.
[215] Pöppelbuß, J.; Röglinger, M., What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management, 2011., ECIS (European Conference on Information Systems) 2011, rbr. 2.1.

ograničavaju se isključivo na pojedine vrste ili kategorije rizika. U njima ne postoji primjerice odredba da se oni odnose isključivo na rizike koji proizlaze iz upravljanja kvalitetom, ili isključivo na kibernetičke rizike, rizike usklađenosti ili rizike prijevara. Prema COSO modelu potrebno je identificirati sve rizike relevantne za poslovanje poduzeća i strategiju društva.[216] ISO 31000:2018 s time u vezi izričito navodi da on cit.: „pruža opći pristup upravljanju bilo kojom vrstom rizika i nije fokusiran na pojedinačnu industriju ili sektor".[217] Oba modela mogu se primijeniti na bilo koju organizaciju (društvo) neovisno o njezinoj veličini.[218] Također, oni nisu modeli za koje se izdaju certifikati usklađenosti.[219] Stoga je zajednička karakteristika da su i COSO i ISO opći modeli upravljanja rizicima jer nisu ograničeni ni na pojedine vrste rizika ni na društva određene industrije ili sektora. Fazu procjene rizika prema COSO modelu koja slijedi nakon identificiranja rizika, ISO 31000 naziva fazom analize rizika. Analizom rizika određuje se ozbiljnost rizika (vjerojatnost ostvarenja događaja i posljedice te jačina utjecaja), što se u bitnome poklapa s fazom procjene prema COSO modelu pa se pojmovi procjena / analiza bitnosti rizika mogu promatrati kao sinonimi.

ISO 31000 nakon analize rizika predviđa fazu evaluacije rizika. Evaluacija rizika služi tomu da društvu omogući donošenje odluka poput odluke o nepoduzimanju mjera (pasivnost), odabiru odgovora na rizik ili provedbi dodatnih analiza.[220] Uzimajući u obzir da evaluacija rizika društvu omogućuje odluku o tome treba li rizik tretirati, u svom bitnom sadržaju evaluacija rizika prema ISO 31000:2018 odgovara prioritizaciji rizika prema COSO ERM modelu. Stoga, neovisno o razlikama u nazivima predmetne faze, njezino je temeljno obilježje to da ona prethodi primjeni konkretne mjere i služi njezinu odabiru.

Neovisno o možebitnim odstupanjima u jezičnim nazivima pojedinih faza, identifikacija rizika, zatim procjena/analiza ozbiljnosti te prioritizacija/evaluacija, faze su u upravljanju rizicima koje su u bitnome jednake po COSO modelu i ISO 31000.

---

[216] Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, str. 81.
[217] ISO, *op. cit.* u bilj. 31, str. 1.
[218] Sison, L.; Doran, J.; Understanding the Differences between the COSO ERM Framework and ISO 31000 Risk Management Standards, dostupno na https://www.ajg.com/us/news-and-insights/2020/oct/coso-iso-3100-risk-management-plans/ (posljednji pristup 1. veljače 2024.),
COSO and ISO 31000 Risk Management Plans | Gallagher USA (ajg.com).
[219] *Ibid.*
[220] ISO, *op. cit.* u bilj. 31, str. 12.

Nakon toga slijedi implementacija odgovora na rizik (COSO ERM), odnosno faza tretmana rizika (ISO 31000:2018). Oba modela kao odgovor na rizik odnosno njegov tretman predviđaju izbjegavanje, prihvaćanje, praćenje i dijeljenje.[221]

Za razliku od COSO modela, ISO 31000 izričito navodi da odgovor na rizik može biti i cit.: „povećanje rizika kako bi se iskoristila prilika“ (engl. *increasing the risk in order to pursue an opportunity*).[222] Nadalje, ISO 31000 kao odgovor na rizik predviđa i promjenu vjerojatnosti rizika.[223]

Stvarni rezidualni rizik (COSO model) kao pojam prepoznat je i u ISO 31000 (rizik koji preostaje nakon tretmana).[224] ISO 31000 ističe važnost dokumentiranja takvih rizika.[225]

ISO 31000, za razliku od COSO modela, sadržava pravila o sadržaju planova za tretman rizika. Prema modelu ISO 31000 planovi za tretman rizika preciziraju kako će odabrani tretman (odgovor na rizik) biti proveden[226], čime se zapravo omogućuje posljedično i nadzor provedbe tretmana rizika.[227] Naime, ako postoji plan u okviru kojeg su navedeni koraci i vremenski okviri za primjenu odgovora na rizik, moći će se nadzirati ostvaruje li se i u kojoj mjeri predviđeni plan. Po ISO 31000 takav plan sadržava obrazloženje razloga zbog čega je odabran konkretni odgovor na rizik za pojedini rizik, tko je odgovoran i zadužen za odobravanje i implementaciju plana, koji su koraci primjene odgovora, potrebni resursi, kako će se mjeriti uspješnost odgovora na rizik (engl. *the performance measure*), nadzor i izvještavanje, rokove.[228]

Za razliku od COSO modela koji se izričito koristi pojmom „apetit za rizikom“ (engl. *risk appetite*), ISO 31000 navodi da društvo treba definirati kriterije u vezi s rizikom (engl. *defining risk criteria*). Jedan od primjera kriterija u vezi s rizikom po ISO 31000 koje treba definirati jest količina i vrsta rizika koja se smije ili ne smije prihvatiti.[229] Uzimajući u obzir da je zapravo u bitnome riječ o sklonosti društva za preuzimanje rizika, ISO 31000 prepoznaje

[221] *Ibid.*, str. 13 i 14.
[222] *Ibid.*, str. 13.
[223] *Ibid.*
[224] *Ibid.*, str. 14.
[225] *Ibid.*
[226] *Ibid.*
[227] *Ibid.*
[228] *Ibid.*
[229] *Ibid.*

predmetni koncept, ali ga ne naziva izričito apetitom za rizik, već se na njega referira u smislu pojma „kriteriji u vezi s rizikom“.[230]

Treba posebno istaknuti da oba modela ističu važnost integriranja upravljanja rizicima u procese donošenja odluka, što samim time uključuje i integriranje upravljanja rizicima i u procese donošenja poduzetničkih odluka uprave.[231]

Konkretno, ISO 31000 ističe da se uprava / više rukovodstvo (engl. *top management*) i nadzorni odbor / ostali nadzorni organi (engl. *oversight bodies*) trebaju kontinuirano posvetiti upravljanju rizicima, što uključuje i integriranje upravljanja rizicima u ključne poslovne aktivnosti i donošenje odluka (engl. *risk-based decision making*).[232] Prema ISO 31000 uprava / više rukovodstvo odgovorni su za upravljanje rizicima (engl. *top management*), s time da su nadzorni organi (engl. *oversight bodies*) poput nadzornog odbora odgovorni za nadzor upravljanja rizicima.[233]

Prema COSO modelu, upravni odbor (engl. *the board of directors*) ima primarnu odgovornost nadzora rizika, što uključuje i provedbu revizije u praksi upravljanja rizicima.[234] Upravni odbor određene zadatke može delegirati odboru za rizik.[235] Odgovornost dnevnog upravljanja rizicima počiva na upravi / višem rukovodstvu (engl. *management*).[236] Neovisno o strukturi, uobičajeno je internim aktima propisati podjelu odgovornosti.[237]

COSO model ističe da integriranje upravljanja rizicima u društvu poboljšava donošenje odluka društva.[238]

Uzimajući u obzir da predmetni modeli ne sadržavaju pravila koja bi bila međusobno proturječna, ne postoje zapreke da društva u svoje prakse uključe u isto vrijeme elemente obaju modela, odnosno da se njima inspiriraju. Faza kontinuiranog praćenja i revizije prisutna je u

[230] IRM, A Risk Practitioners Guide to ISO 31000:2018: Review of the 2018 version of the ISO 31 000 risk management guidelines and commentary on the use of this standard by risk professionals, 2018., London, str. 11.
[231] ISO 31000 vs. COSO: Comparing Risk Management Standards (techtarget.com)
[232] ISO, *op. cit.* u bilj. 31, str. 1, 4, 6, 8.
[233] *Ibid.*, str. 5.
[234] COSO, *op. cit.* u bilj. 32, str. 28 i 29.
[235] *Ibid.*
[236] *Ibid.*
[237] *Ibid.*
[238] *Ibid.*, str. 3.

oba modela, iz čega se može zaključiti da je ona također jedna od zajednički prepoznatih faza procesa (ključnih aktivnosti) upravljanja rizicima.[239]

Nadalje, ne postoji izričita zakonska zapreka propisana hrvatskim pravom da društva iz financijske industrije uspostave i implementiraju sustave upravljanja rizicima temeljene na navedenim modelima upravljanja rizicima (u mjeri u kojoj se to poklapa s odgovarajućim pravnim propisom koji regulira sustav upravljanja rizicima za pojedino društvo koje posluje u financijskom sektoru).

5. UPRAVLJANJE POJEDINIM VRSTAMA RIZIKA (engl. *specialist areas of risk management*)[240]

5.1. Posebna područja upravljanja rizicima

Uz opće modele upravljanja rizicima koji su primjenjivi na upravljanje bilo kojom vrstom rizika (primjerice COSO ERM i ISO 31000:2018), postoje međunarodni standardi koji propisuju posebnosti u vezi s upravljanjem pojedinim vrstama rizika. Tako primjerice standard ISO 9001:2015 propisuje posebnosti u vezi s upravljanjem rizicima kvalitete, ISO 21500:2012 propisuje posebnosti u vezi s upravljanjem rizicima projekta, ISO 37301:2021 propisuje posebnosti upravljanja rizicima usklađenosti. Osim međunarodnim standardima posebnosti, upravljanja pojedinim vrstama rizika mogu biti propisana i uredbama EU-a. Kao primjer takva slučaja navodi se Uredba DORA koja je propisala obveze za društva iz financijske industrije u vezi s upravljanjem ICT rizicima. S obzirom na pandemiju koronavirusa koja je uzrokovala mnoge promjene u organizaciji rada na daljinu, kao primjer upute o upravljanju rizicima rada na daljinu društava iz financijske industrije navodi se cirkular u vezi s radom na daljinu (engl. *teleworking*) luksemburškog nadzornog tijela za financijski sektor.

5.2. Upravljanje rizicima kvalitete u kontekstu upravljanja kvalitetom

[239] Vidi u Miloš Sprčić; Dvorski Lacković, *op. cit.* u bilj. 4, slika 2.10, str. 73.
[240] Vidi više u Hopkin, P.; Thompson, C., *op. cit.* u bilj. 16, str. 41.

Društvo koje je implementiralo sustav upravljanja kvalitetom sposobnije je kontinuirano proizvoditi / pružati usluge i proizvode na način da se poštuju zahtjevi u vezi sa standardom kvalitete te zadovoljiti zahtjeve, želje i očekivanja kupaca proizvoda / korisnika usluga.[241] Jedno od načela upravljanja kvalitetom proizvoda/usluga fokus je na kupca/korisnika.[242]

Standard ISO 9001:2015[243] propisuje pravila u vezi sa sustavom upravljanja kvalitetom kojim se osigurava da društvo proizvodi / pruža usluge i proizvode koji će odgovarati zahtjevima u vezi s kvalitetom koji proizlaze iz pravnih zahtjeva (primjerice zakona, podzakonskih akata, standarda društva, ugovora itd.) te da se poveća zadovoljstvo kupca / korisnika usluge.[244] ISO 9001:2015 ističe važnost održavanja komunikacije s klijentima koja obuhvaća pružanje relevantnih informacija u vezi s proizvodima/uslugama, postupanje s upitima klijenata, dobivanje povratnih informacija od klijenata o zadovoljstvu, uključujući i postupanje s pritužbama klijenata.[245] Jedna od etapa sustava upravljanja kvalitetom jest utvrđivanje zahtjeva u vezi s kvalitetom koje proizvodi/usluge moraju ispunjavati.[246] Prije nego što se proizvod/usluga isporuči/pruži, društvo će utvrditi ispunjenost svih zahtjeva u vezi s kvalitetom.[247] Jedno je od pravila upravljanja kvalitetom to da će društvo osigurati kontrole utvrđivanja neusklađenosti „outputa" kako bi se izbjeglo da društvo pruža uslugu, odnosno isporuči proizvod neodgovarajuće kvalitete (engl. *control of nonconforming outputs*). Ako je neki „output" neusklađen s kvalitetom, društvo može proizvod/uslugu popraviti, prestati s prodajom, informirati klijenta itd.[248] Kako bi društvo bilo usklađeno s ISO 9001:2015 (E), mora pratiti razinu percepcije klijenata o tome koliko su njihove potrebe i očekivanja ispunjeni, što znači da mora ustrojiti metode kako će pribaviti, pratiti i provjeravati takve informacije.[249]

S obzirom na to da je tema ovog rada upravljanje rizicima, sasvim logično postavlja se pitanje kakve veze ima upravljanje kvalitetom s upravljanjem rizicima.

---

[241] ISO, međunarodni standard 9001, Quality management systems — Requirements, 5. izdanje, Geneva, 2015., rbr. 01, str .VI.
[242] *Ibid.*, *op. cit.* u bilj. 241, rbr. 02, str. VII.
[243] ISO, *op. cit.* u bilj. 241.
[244] *Ibid.*, rbr. 1, str. 1.
[245] *Ibid.*, rbr. 8.2.1., str. 10.
[246] *Ibid.*, rbr. 8.2.2., str. 10.
[247] *Ibid.*, rbr. 8.6., str. 15 i 16.
[248] *Ibid.*, rbr. 8.7.2., str. 16.
[249] *Ibid.*, rbr. 9.1.2., str. 17.

Standard ISO 9001:2015 ističe da se implementiranjem sustava upravljanja kvalitetom omogućuje pravodobno reagiranje na rizike povezane s kontekstom i ciljevima koji su u vezi s kvalitetom proizvoda/usluge. Nadalje, predmetni standard ističe da „razmišljanje utemeljeno na rizicima“ (engl. *risk-based thinking*) omogućuje društvu identificiranje faktora koji negativno utječu na planirane ciljeve. ISO 9001:2015 ističe da je društvo odgovorno za implementiranje razmišljanja koje se temelji na rizicima te primjenu odgovora na rizik.

Kako bi društvo bilo usklađeno s ISO 9001:2015, mora planirati i biti sposobno provesti odgovore na rizik.[250] U kontekstu primjene odgovora na rizik, ISO 9001:2015 ističe obvezu prevencije, odnosno smanjenje neželjenih učinaka rizika.[251] Odgovori na rizik trebaju biti proporcionalni potencijalnom utjecaju na usklađenost proizvoda i usluga.[252] Kao potencijalne opcije odgovora na rizik navode se: izbjegavanje rizika, preuzimanje rizika, eliminiranje izvora rizika, mijenjanje vjerojatnosti ili posljedica, dijeljenje rizika.[253]

ISO 9001:2015 ističe da društva mogu odlučiti žele li razviti obuhvatniju metodologiju upravljanja rizicima u vezi s kvalitetom nego što je ona predviđena predmetnim standardom o upravljanju kvalitetom, primjerice upotrebljavajući i implementirajući druge standarde. ISO 31000 i COSO model primjeri su drugih standarda/modela koji se primjenjuju na upravljanje svim vrstama rizika, a kojim se društvo može koristiti kako bi uz zahtjeve iz ISO 9001:2015 u vezi s upravljanjem rizicima kvalitete implementiralo i druge zahtjeve u vezi s upravljanjem svim vrstama/skupinama rizika.

S obzirom na to da iz navedenoga proizlazi da je društvo prema ISO 9001:2015 dužno u kontekstu upravljanja kvalitetom utvrditi rizike u vezi s kvalitetom, ažurirati ih, planirati odgovore na rizik ovisno o njihovoj bitnosti te biti sposobno primijeniti odgovarajuće odgovore na rizike, a identificiranje rizika, procjena bitnosti i odgovor na rizike temeljni su općepriznati elementi upravljanja rizicima, zaključuje se da je proces upravljanja rizicima (kvalitete) integralan, bitan i neizostavan element upravljanja kvalitetom.

5.3. Upravljanje rizicima projekata u kontekstu upravljanja projektima

[250] *Ibid.*, rbr. 0.3.3., str. IX.
[251] *Ibid.*, rbr. 6.1.1., str. 4.
[252] *Ibid.*, rbr. 6.1.2., str. 5.
[253] *Ibid.*, rbr. 10.2.1., str. 19.

Međunarodni standard ISO 21500 iz 2012. sadržava smjernice o upravljanju projektima kojima se društva mogu koristiti za upravljanje projektima bez obzira na vrstu projekta, njegovu kompleksnost, veličinu ili trajanje. One sadržavaju opis koncepata i pojmova na generalnoj/općoj razini (engl. *high-level*) koji čine dobru praksu upravljanja projektima.[254]

Projekt se sastoji od procesa koje čine koordinirane i kontrolirane aktivnosti s datumom početka i završetka te čiji je cilj ostvarenje projektnih ciljeva. U pravilu, projekti su podijeljeni po fazama.[255] Posebnost projekata prema ISO 21500 jest ta da projekte provode posebni *ad hoc* timovi, ne ponavljaju se i njihov je proizvod poseban.[256] Jedan od koraka u upravljanju projektima jest izrada projektnog plana.[257] Projektni plan sadržava informacije o tome kako će se projekt provesti, popis zaduženja, podatke o troškovima i detalje kako će se plan provesti, kontrolirati i završiti. Jedna je od faza upravljanja projektom procjena trajanja pojedinih aktivnosti ili faza projekta.[258] Kontrola troškova projekta također je dio upravljanja projektom.[259] Logično je pretpostaviti da će društvo kontrolirati događa li se projekt u predviđenom vremenskom rasporedu i jesu li troškovi projekta premašili ili će premašiti novčana sredstva koja je društvo odredilo/izdvojilo/planiralo za potrebe konkretnog projekta. Rizik da projekt ili pojedina etapa projekta neće biti završeni u roku ili da će novčana sredstva za cjelokupni projekt premašiti planirana sredstva jedni su od (mnogih) rizika s kojima se društvo susreće u okviru upravljanja projektima. Uzimajući u obzir to da rizici mogu utjecati na ostvarenje projektnih ciljeva, a upravljanjem projektom žele se ostvariti projektni ciljevi, sasvim je logično da bez upravljanja rizicima u vezi s projektom nema uspješna upravljanja projektom.

Da je ISO 21500 o upravljanju projektom temeljen na upravljanju rizicima, vidljivo je iz toga što se u predmetnom standardu riječ „rizik“ spominje čak 88 puta.

U okviru upravljanja projektom društvo je dužno voditi registar rizika koji mogu utjecati na projekte koji sadržava informacije o identificiranim rizicima, njihovoj analizi te

[254] ISO, međunarodni standard 215000, Guidance on project management, 1. izdanje, Geneva, 2012., str. 1.
[255] *Ibid.*, rbr. 3.2., str. 3.
[256] *Ibid.*, rbr. 3.7., str. 6.
[257] *Ibid.*, rbr. 4.3.3., str. 12.
[258] *Ibid.*, rbr. 4.3.22., str. 22.
[259] *Ibid.*, rbr. 4.3.27., str. 24.

planiranim odgovorima na rizike.[260] Društvo uzima u obzir unutarnje i vanjske faktore/okolnosti iz kojih proizlazi rizik za projekt.[261] Upravljanje projektima uključuje izvještavanje i eskalaciju rizika, što upućuje na važnost komuniciranja o rizicima.[262] Osoblje uključeno u projekt mora imati kompetencije u vezi s upravljanjem projektima koje su potrebne kako bi se postigli ciljevi.[263] Svakom projektnom timu potrebni su stručni pojedinci koji su sposobni primijeniti svoja znanja i iskoristiti svoje iskustvo kako bi ispunili ciljeve projekta. Svaki utvrđeni nesklad/jaz između traženih kompetencija i stvarnog stanja članova projektnog tima potencijalni je rizik na koji treba reagirati.[264] Kompetencije u vezi s upravljanjem projektima mogu biti tehničke prirode poput znanja pojmova, koncepata i procesa upravljanja projektom.[265] Osobe koje upravljaju projektima susreću se s različitim ograničenjima projekta (engl. *project constraints*). Primjeri ograničenja projekta mogu biti kratak rok, ograničenost izvora njegova financiranja, ograničeni ljudski kapaciteti, potencijalno negativan učinak projekta na ekologiju.[266] Jedno je od ograničenja projekta i razina prihvatljive izloženosti rizicima (engl. *the level of acceptable risk exposure*), što je u biti sklonost preuzimanju rizika kod vođenja projekta. Procesi koji su sastavni dio upravljanja projektom jesu identifikacija, procjena, tretiranje i kontrola rizika.[267] ISO 21500:2012 ne gleda na rizike isključivo kao na događaje koji mogu negativno utjecati na projekt, nego uzima u obzir da osim prijetnje (engl. *threat*) rizik može biti i prilika (engl. *opportunity*), što je u skladu s poimanjem rizika da on nije uvijek „loš“. Svrha identificiranja rizika jest utvrditi događaje koji, ako se ostvare, mogu imati pozitivan ili negativan utjecaj na projektne ciljeve. To je ponavljajući postupak zbog toga što za vrijeme vođenja projekta mogu nastati rizici koji nisu postojali prije, mogu se utvrditi rizici koji su postojali prije, ali omaškom nisu utvrđeni te se ozbiljnost rizika s protekom vremena može mijenjati. To upućuje na važnost nadzora i revizije rizika u okviru procesa upravljanja rizicima. To je sasvim logično ako se uzme u obzir da neki kompleksniji projekti mogu trajati više godina. Preporuka je da više osoba sudjeluje u utvrđivanju rizika poput višeg

[260] *Ibid.*, rbr. 2.13., str. 2.
[261] *Ibid.*, rbr. 3.5.1., str. 5.
[262] *Ibid.*, rbr. 3.6., str. 6.
[263] *Ibid.*, rbr. 3.9., str. 7.
[264] *Ibid.*
[265] *Ibid.*, rbr. 3.9., str. 8.
[266] *Ibid.*, rbr. 3.11., str. 8.
[267] *Ibid.*, tablica 1., str. 10.

rukovodstva, stručnjaka za upravljanje rizicima, članova projektnog tima itd.[268] Nakon identificiranja rizika slijedi njegova procjena s obzirom na vjerojatnost ostvarenja rizika i posljedicu na projektne ciljeve. U skladu s procjenom rizika i drugim faktorima, rizici se prioritiziraju.[269] Tretiranjem rizika nastoje se osnažiti prilike i smanjiti opasnosti za projektne ciljeve. Odabir konkretnog odgovora na rizik / tretmana treba biti prikladan za rizik na koji se primjenjuje, troškovno učinkovit, pravodoban te razumljiv relevantnim dionicima. Tretmani uključuju mjere izbjegavanja rizika, smanjenja rizika, preusmjeravanja rizika i razvoj kriznih planova (engl. *contingency plans*) za slučajeve ostvarenja rizika. Primjerice, a u okviru upravljanja projektom, društvo može donijeti krizni plan za slučaj da osoba zadužena za upravljanje kompleksnim projektom napusti projekt prije njegova završetka. Nakon što je društvo odgovorilo/reagiralo na rizik, postavlja se pitanje je li tretman pravilno izvršen i je li rezultirao zadovoljavajućim učinkom. Praćenje napretka tretmana i procjena njegove efikasnosti dio su procesa kontrole rizika.

Slijedom navedenog razvidno je da je proces upravljanja rizicima neizostavan dio upravljanja kvalitetom.

5.4. Upravljanje rizicima usklađenosti

ISO 37301:2021[270] međunarodni je standard koji precizira zahtjeve i pruža smjernice za uspostavu, razvoj, implementiranje, evaluaciju, održavanje i poboljšavanje efikasnosti sustava upravljanja usklađenošću.[271]

ISO 37301:2021 definira općenito rizik kao učinak neizvjesnosti na ciljeve društva, pri čemu učinak može biti pozitivna ili negativna devijacija, iz čega proizlazi da učinak rizika može biti i pozitivnog karaktera (prilika).[272] Pojam rizika koristi se u kontekstu potencijalnog događaja, posljedica događaja te njihovih kombinacija.[273]

---

[268] *Ibid.*, rbr. 4.3.28., str. 25.
[269] *Ibid.*, rbr. 4.3.29., str. 26.
[270] ISO, međunarodni standard 37301, Compliance management systems — Requirements with guidance for use, 1. izdanje, Geneva, 2021.
[271] *Ibid.*, rbr. 1., str. 1.
[272] Ibid., rbr. 3.7., str. 1.
[273] *Ibid.*

Rizici usklađenosti mogu utjecati na različite ciljeve društva poput ciljeva u vezi s integritetom društva, kulturom društva, usklađenosti društva, reputacijom, vrijednošću, etikom poslovanja.[274]

Rizik usklađenosti (engl. *compliance risk*) definiran je kao vjerojatnost pojave i posljedice neusklađenosti s obvezama usklađenosti društva.[275] Obveze usklađenosti društva su obveze koje društvo obligatorno mora ispunjavati, ali i one koje je društvo dobrovoljno odabralo ispunjavati.[276] Jedan je od preduvjeta efikasnog upravljanja usklađenošću poznavanje pravnog i regulativnog konteksta. To posebice dolazi do izražaja u onim industrijama koje su iznimno regulirane i pod nadzorom posebnog nacionalnog tijela zaduženog za nadzor subjekta nadzora u okviru svojeg djelokruga. Kada je to odgovarajuće, a pogotovo u slučaju društava koja pružaju jednu od financijskih usluga, društvo bi trebalo uspostaviti i ažurirati jedinstveni dokument koji će sadržavati pregled svih obveza usklađenosti.[277]

Neizostavan je dio upravljanja usklađenošću procjena rizika usklađenosti koja je sastavni dio predmetnog međunarodnog standarda.[278] Prema ISO 37301:2021, u kontekstu procesa upravljanja rizicima, društvo mora identificirati, analizirati i procijeniti rizike usklađenosti, nadzirati ih i primjenjivati odgovarajuće mjere.[279] Rizici usklađenosti proizlaze iz aktivnosti društva, njegovih proizvoda, usluga.[280] Važno je istaknuti da rizici usklađenosti mogu proizići iz delegiranja poslova trećima.[281] Procjena rizika usklađenosti mora se provoditi redovito (engl. *periodically*) i uvijek kada je riječ o materijalnim promjenama.[282] Stupanje na snagu i primjena novog zakona ili uredbe Europske unije koji donose nove važne obveze za društvo zasigurno je razlog za ponovnu procjenu rizika usklađenosti s novim obvezama. Namjera pružanja novih usluga koje društvo dosad nije pružalo (a pogotovo u slučaju kada je

[274] *Ibid.*, str. VII.
[275] *Ibid.*, rbr. 3.24., str. 24.
[276] *Ibid.*, rbr. 3.25., str. 24.
[277] *Ibid.*, rbr. A.4.5, str. 23.
[278] *Ibid.*, rbr. 4.6., str. 6.
[279] I drugi modeli upravljanja rizicima usklađenosti predviđaju postojanje sljedećih etapa u procesu upravljanja rizicima u vezi s usklađenošću: identifikacija rizika, analiza, prioritizacija, tretman te evaluacija (uključujući i evaluaciju čitava procesa). O tome vidi više u European Commission, Compliance Risk Management in the Digital Era, European Commission, 2023., dostupno na https://taxation-customs.ec.europa.eu/system/files/2024-01/2023_CRM_Guide.pdf?trk=public_post_comment-text (posljednji pristup 3. ožujka 2024.).
[280] ISO, *op. cit.* u bilj. 270, rbr. 4.5., str. 6.
[281] *Ibid.*
[282] *Ibid.*

riječ o potrebi traženja prethodnog odobrenja nadležnog nacionalnog nadzornog tijela) također je primjer materijalnih promjena zbog kojih je potrebno provesti analizu rizika usklađenosti. Da bi društvo bilo usklađeno s predmetnim međunarodnim standardom, dužno je dokumentirati procjenu rizika usklađenosti te poduzete mjere upravljanja rizicima usklađenošću.[283]

Rizici usklađenosti uključuju inherentne rizike usklađenosti te rezidualne rizike usklađenosti. Inherentni rizici usklađenosti one su razine rizika prije primjene odgovora na rizike, a rezidualni rizik ona je razina rizika koja preostaje nakon primjena mjere kontrole/upravljanja rizicima.[284]

S obzirom na njegovu posljedicu, rizik usklađenosti može se podijeliti na različite potkategorije rizika u okviru skupnog pojma rizika usklađenosti: rizik integriteta poslovanja, poslovni rizik, reputacijski rizik, rizik financijskog gubitka, regulatorni rizik, pravni rizik, rizik sporova, interpretacijski rizik.[285] To implicira da identificiranje rizika usklađenosti i njegova kategorizacija ne ostaje samo na razini utvrđenja je li riječ o riziku usklađenosti, nego ga je u drugom koraku potrebno povezati s onom potkategorijom rizika usklađenosti na koju konkretni rizik usklađenosti ima učinak. Valja voditi računa o tome da su navedene potkategorije rizika usklađenosti ujedno i zasebne kategorije rizika. Primjerice, reputacijski rizik zasebna je kategorija rizika, ali može biti i potkategorija rizika usklađenosti ako je posljedica proizišla iz neusklađenosti.

U društvima u kojima postoji funkcija usklađenosti nositelji funkcije usklađenosti (jedna osoba ili skupina osoba) ovlašteni su i odgovorni za funkcioniranje sustava upravljanja usklađenošću. Uzimajući u obzir da se upravljanje usklađenošću sastoji i od upravljanja rizicima usklađenošću, zaključuje se da funkcija usklađenosti ima relevantnu ulogu u upravljanju rizicima usklađenosti koji mogu imati učinak na različite kategorije rizika (u tom kontekstu misli se na potkategorije rizika u okviru rizika usklađenosti). Stoga i ne začuđuje preporuka međunarodnog standarda ISO 37301:2021 da se politikom usklađenosti propiše suradnja/odnos između funkcije usklađenosti i funkcije nadležne za rizike kada je to

[283] *Ibid.*, rbr. 7.5., str. 14.
[284] *Ibid.*, rbr. A.4.6, str. 24.
[285] Vidi u Ramakrishna, S. P., Enterprise Compliance Risk Management: An Essential Toolkit for Banks and Financial Services, 2015., tablica 8.4., str. 213–239.

primjenjivo, odnosno kada te dvije funkcije postoje i nisu sjedinjene u jednoj osobi.[286] Jednostavno rečeno, upravljanje rizicima (usklađenosti) može biti u domeni osobe odgovorne za usklađenost, a koja nije ujedno zadužena za upravljanje rizicima.

5.5. Upravljanje rizicima u vezi s informacijskom i komunikacijskom tehnologijom

Ilustracije radi, zamislimo da se digitalnom aplikacijom kreditne institucije kojom se koristimo, između ostalog, za prijenos novčanih sredstava (mobilno bankarstvo) ne možemo koristiti tjedan dana zbog tehničkih smetnji koje onemogućuju rad aplikacije. Također, zamislimo da je haker ilegalno upao u IT sustav kreditne institucije i ostvario neovlašteni pristup podatcima u vezi s računom/računima koje imamo u kreditnoj instituciji (uključujući i osobne podatke) i neovlašteno izmijenio/ukrao podatke. Nadalje, zamislimo da operater uređenog tržišta na kojem se spajaju ponuda i potražnja za vrijednosnim papirima koji su uvršteni na predmetnom uređenom tržištu (burza) zbog kvara/uništenja hardvera ili softvera tjedan dana ne može upariti nijedan nalog za kupnjom ili prodajom vrijednosnog papira ili da ne može duže vrijeme zaprimiti naloge od intermedijara (npr. kreditnih institucija, investicijskih društava) koji imaju pristup, odnosno članovi su uređenog tržišta. Situacija u kojoj nakon incidenta određenom društvu treba mjesec dana da se operativno „oporavi“ i vrati u stanje kakvo je bilo prije incidenta i nastavi pružati usluge zasigurno nije primjer efikasnog upravljanja krizom. Jedan je primjer sistemskog katastrofalnog događaja situacija da su svi podatci o imateljima vrijednosnih papira i stanju vrijednosnih papira koji se vode u depozitoriju vrijednosnih papira uništeni jer je eksplozija uništila svu računalnu opremu središnjeg depozitorija u kojem su se vodili podatci, a središnji depozitorij vrijednosnih papira nije pohranio kopiju podataka (engl. *backup*) na nekom drugom (sigurnijem) mjestu.

Kako bi se postigla visoka zajednička razina digitalne operativne otpornosti, Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj

[286] ISO, *op. cit.* u bilj. 270, rbr. A.5.2., str. 27.

otpornosti za financijski sektor (dalje u tekstu: DORA)[287] uređena je materija sigurnosti mrežnih i informacijskih sustava kojima se podupiru poslovni procesi financijskih subjekata. Uredba o digitalnoj operativnoj otpornosti za financijski sektor (DORA) primjenjivat će se od 17. siječnja 2025.[288] Kao što njezino ime sugerira, ona se primjenjuje na društva koja posluju u financijskom sektoru poput kreditnih institucija, institucija za platni promet, investicijskih društava, društava za upravljanje investicijskim fondovima, društava za osiguranje.[289]

U kontekstu ovoga rada Uredbu o digitalnoj otpornosti za financijski sektor potrebno je posebno istaknuti jer je ona izričito propisala da financijski subjekti u sklopu svojeg općeg sustava za upravljanje rizicima moraju imati pouzdan, sveobuhvatan i dobro dokumentiran okvir za upravljanje rizicima informacijske i komunikacijske tehnologije (dalje u tekstu: IKT rizik), koji im omogućuje brzo, učinkovito i sveobuhvatno reagiranje na IKT rizik te osigurava visoku razinu digitalne operativne otpornosti.[290] Okvir za upravljanje IKT rizicima mora se sastojati barem od strategija, politika, postupaka te IKT protokola i alata.[291]

Financijski subjekti moraju kontinuirano utvrđivati sve izvore IKT rizika te provoditi procjenu rizika nakon svake bitne promjene u infrastrukturi mrežnog i informacijskog sustava.[292]

Okvir za upravljanje IKT rizicima mora se preispitivati najmanje jedanput godišnje te ga je potrebno kontinuirano poboljšavati.[293] Upravljanje IKT rizicima podliježe redovitoj unutarnjoj reviziji koju interni revizori provode u skladu s planom revizije financijskog subjekta.[294] U sklopu okvira za upravljanje IKT rizicima financijski subjekti izrađuju planove komunikacije u krizi kojima se osigurava odgovarajuća objava barem važnih IKT incidenata ili ranjivosti klijentima, partnerskim financijskim subjektima i javnosti, ovisno o slučaju.[295] Upravljanjem IKT rizicima nastoji se na najmanju moguću mjeru svesti rizik od oštećenja ili

[287] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (Tekst značajan za EGP).
[288] Čl. 64. DORA-e.
[289] O polju primjene detaljnije vidi čl. 2. DORA-e.
[290] Čl. 6., st. 1. DORA-e.
[291] Čl. 6., st. 2. DORA-e.
[292] Čl. 8., st. 2. i 3. DORA-e.
[293] Čl. 6., st. 5. DORA-e.
[294] Čl. 6., st. 6. DORA-e.
[295] Čl. 14., st. 2. DORA-e.

gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje.[296]

Financijski subjekti koji nisu mikropoduzeća odgovornost za upravljanje IKT rizicima i nadzor nad njima dodjeljuju kontrolnoj funkciji i osiguravaju odgovarajuću razinu neovisnosti takve kontrolne funkcije kako bi se izbjegli sukobi interesa. Predmetno pravilo u skladu je s modelom „triju crta obrane" (engl. *three lines of defence model*).[297] Naime, a u skladu s modelom triju crta obrane, zaposlenici koji rade na šalteru s klijentima bili bi prva crta obrane (engl. *day to day operations, direct labour*). Drugu liniju obrane čine kontrolne funkcije poput funkcije upravljanja rizicima i usklađenosti (npr. glavna osoba zadužena za nadzor rizika, glavna osoba zadužena za usklađenost, glavni službenik za sigurnost), a treću liniju čini interna revizija.[298]

5.6. Financijski sektor i upravljanje rizicima u vezi s radom na daljinu (engl. *telework*)

Komisija za nadzor financijskog sektora (dalje u tekstu: CSSF) nadležno je nacionalno tijelo u Luksemburgu za nadzor subjekata financijskog sektora i financijskih proizvoda u Luksemburgu.[299] Tako primjerice CSSF nadzire, između ostalog, kreditne institucije, investicijska društva, društva za upravljanje investicijskim fondovima, investicijske fondove u Luksemburgu. U ožujku 2022. CSSF izmijenio je i nadopunio okružnicu 21/769 o radu na daljinu.[300] Iako se ta okružnica ne primjenjuje u Republici Hrvatskoj, njezin sadržaj može poslužiti kao okvir za razumijevanje kojim sve rizicima u vezi s radom na daljinu može biti izloženo društvo iz Republike Hrvatske kod implementiranja rada na daljinu (pogotovo ono kojem pruža financijske usluge). Naime, utjecaj pandemije COVID-a na organizaciju rada, što uključuje i „cvjetanje" rada na daljinu koji se obavlja putem informacijsko-komunikacijske

[296] Čl. 9., st. 3., toč. b DORA-e.
[297] Čl. 6., st. 4. DORA-e.
[298] Vidi više u Sidewell, J.; Hlavnicka, P., Enhenced Enterprise Risk Management, New York, 1. izdanje, 2022.
[299] Vidi više o CSSF-u na https://www.cssf.lu/en/about-the-cssf/.
[300] CSSF, Circular CSSF 21/769 (as amended by Circular CSSF 22/804) Governance and security requirements for supervised entities to perform tasks or activities through telework, dostupno na https://www.cssf.lu/en/Document/circular-cssf-21-769/ (posljednji pristup 8. veljače 2024.).

tehnologije[301], nije zaobišao ni društva u Republici Hrvatskoj. Prema predmetnoj okružnici, nadzirani subjekti koji pružaju financijske usluge u Luksemburgu moraju identificirati i procijeniti inherentne rizike koji proizlaze iz rada na daljinu.[302] Od subjekata nadzora očekuje se uzeti u obzir operativne rizike, pravne, informacijsko-komunikacijsko-tehnološke, rizike usklađenosti i reputacijske u vezi s radom na daljinu.[303] Glede pravnih rizika, subjekti nadzora moraju uzeti u obzir rizike neusklađenosti s radnim pravom i poreznim propisima.[304] Također, prema okružnici društvo mora voditi računa o zaštiti profesionalne tajne, ali i zaštite/sigurnosti podataka.[305] Nadzirani subjekti moraju implementirati potrebne ublažavajuće mjere i kontrole putem kojih će se rezidualni rizik držati u okviru granica sklonosti društva preuzimanju rizika.[306] To je primjer iz kojeg je vidljiva važnost razumijevanja sklonosti preuzimanju rizika zbog toga što ona utječe na to kako će se odvijati proces upravljanja rizicima. Proces utvrđivanja rizika i primjene ublažavajućih mjera (odgovora na rizik) mora biti formaliziran.[307] Upravljanje rizicima u vezi s radom na daljinu mora biti redovito revidirano, što uključuje i reviziju primjene ublažavajućih mjera i kontrola.[308] Pri revidiranju modela upravljanja rizicima u vezi s radom na daljinu uzimaju se u obzir naučene lekcije iz prošlosti (engl. *lessons learned*), organizacijske promjene u društvu, vanjske promjene, promjene u internim procesima rada te trendovi poput kibernetičkog kriminala i mogućih kibernetičkih napada.[309] Kako bi zaposlenici društva bili svjesni rizika u vezi s radom na daljinu, oni trebaju biti o njima obaviješteni putem organiziranih treninga, različitih formi obavijesti (engl. *newsletters*) ili drugim vidom komunikacije.[310] To upućuje na to da je komunikacija o rizicima sastavni dio upravljanja rizicima u vezi s radom na daljinu.

6. KOMUNICIRANJE INFORMACIJA U VEZI S RIZICIMA

[301] Vidi više o radu na daljinu u čl. 17. Zakona o radu (NN, br. 93/14, 127/17, 98/19, 151/22, 64/23).
[302] CSSF, *op. cit.* u bilj. 300, rbr. 28., str. 8.
[303] *Ibid.*
[304] *Ibid.*, rbr. 29., str. 8.
[305] *Ibid.*
[306] *Ibid.*, rbr. 30., str. 8 i 9.
[307] *Ibid.*
[308] *Ibid.*, rbr. 31., str. 9.
[309] *Ibid.*
[310] *Ibid.*, rbr. 42., str. 11.

6.1. Općenito o komuniciranju kao sastavnom dijelu procesa upravljanja rizicima

Komuniciranje (bilo to usmeno ili pisano, interno ili eksterno) u vezi s rizicima smatra se jednim od ključnih elemenata efikasnog upravljanja rizicima.[311] Ono obuhvaća razgovore/rasprave / razmjenu mišljenja o rizicima (engl. *risk talks*), izvještaj o rizicima, različite metode prikazivanja rizika poput mape rizika.[312] Komunikacija o rizicima unutar društva (interna komunikacija) koja je usmjerena prema uspostavi određene korporativne kulture rizika treba biti razumljiva na način da kompleksni prikazi rizika (poput mnoštva brojeva, matrica, nabacanih statističkih podataka, korištenja iznimno kompleksnih termina pravno-ekonomske prirode) sadržajno i stilski budu prilagođeni namjeravanim korisnicima informacija.[313] Postoje kritike da svijest o važnosti upravljanja rizicima nije (u dovoljnoj mjeri) dio svijesti pojedinaca te da predmetna svijest (dovoljno) ne utječe na ponašanje pojedinaca i to upravo zbog neodgovarajućeg oblika/sadržaja komunikacije, odnosno kompleksnosti načina prikazivanja podataka o rizicima (npr. komunikacija isključivo u statističkom obliku bez nekih dodatnih pojašnjenja u kvalitativnom obliku).[314] Efikasna komunikacija o rizicima temelji se na taktikama/elementima/metodici/pristupima koji su usmjereni na postizanje četiri ključna cilja. Konkretno, efikasnom komunikacijom postiže se razumijevanje rizika, stvara se svijest o važnosti upravljanja rizicima, utječe se na to da se o rizicima razmišlja konstantno i posljedično se utječe na željenu/ciljanu/namjeravanu promjenu ponašanja u vezi s rizicima.[315] O važnosti komunikacije o rizicima govore i tvrdnje nekih autora da je jedan od primarnih razloga globalne financijske krize iz 2008. zapravo neuspjeh u domeni komunikacije o rizicima (engl. *communication failure*).[316] Jedna od poruka koja je proizišla iz globalne financijske krize jest ona o važnosti pravodobnog i efikasnog internog komuniciranja o rizicima i to pogotovo između rukovodstva i upravnog odbora, odnosno rukovodstva, uprave i nadzornog odbora

[311] Kampmann, A., *op. cit.* u bilj. 15, str. 20.
[312] *Ibid.*, str. 21 i 22.
[313] *Ibid.*, str. 23.
[314] *Ibid.*
[315] *Ibid.*
[316] Pirson, M.; Turnbull, S., Towards a More Humanistic Governance Model: Network Governance Structure, Journal of Business Ethics, Vol. 99, 2011., str. 101–114.

društva.[317] Financijska kriza pokazala je da je upravljanje rizicima (uključujući i komuniciranje o njima) podbacilo i da članovi upravnog odbora (odnosno uprave i nadzornog odbora) u većini slučajeva nisu imali saznanja o rizicima kojima je izloženo društvo.[318] Osim interne komunikacije o rizicima postoji i eksterna komunikacija.[319] Primjer su eksternog komuniciranja sve one informacije o rizicima / upravljanju rizicima koje su javno dostupne na korištenje (zainteresiranim dionicima određenog tržišta, odnosno relevantnoj javnosti). Izvještaj o rizicima koji se dostavlja isključivo članovima uprave i nadzornog odbora društva te koji se javno ne objavljuje primjer je internog komuniciranja, odnosno internog izvještavanja o rizicima. S druge strane, izvješće poslovodstva, bilješke uz financijske izvještaje, komentari poslovodstva i prospekti vrijednosnih papira koji se javno objavljuju i koji sadržavaju informacije o rizicima / upravljanju rizicima, odnosno procesu upravljanja rizicima eksterno su izvještavanje o rizicima / upravljanju rizicima zbog toga što su namijenjeni široko zainteresiranoj javnosti (npr. potencijalnim dioničarima).

Ilustrativni primjer internog tijeka informacija u smislu komunikacije o rizicima daje se u nastavku. Napomene radi, valja imati na umu da ne postoji jedan univerzalni pristup organizaciji sustava upravljanja rizicima (a time i organizaciji komuniciranja) te je svrha primjera prikazati samo primjer jedne od više potencijalnih organizacija sustava upravljanja rizicima na temelju koje je moguće pratiti komunikaciju o rizicima. Stoga, krenimo redom. Rizike najprije identificiraju operativne jedinice (engl. *operational units*). Operativne jedinice (odnosno pojedinci koji su zaposlenici u operativnim jedinicama) ispunjavaju obrazac o procjeni/analizi rizika (engl. *assessment form*) koji dostavljaju osobi zaduženoj za upravljanje rizicima (npr. rizik menadžeru). One najbolje poznaju pojedinačne rizike te imaju praktično znanje o mjerama koje se na njih mogu primijeniti, a sve u vezi s rizicima s kojima se susreću u okviru svoje poslovne jedinice. Obrazac o rizicima može sadržavati informacije poput opisa i vrste rizika, vjerojatnosti da će se rizik ostvariti, izvora uzročnika rizika (unutarnjih i vanjskih), predloženih mjera za upravljanje rizicima te mjera koje su već poduzete. U pravilu,

[317] *Ibid.*
[318] OECD, Corporate Governance and The financial Crisis: Key findings and main messages, 2009., str. 8 i 9, dostupno na https://www.oecd.org/corporate/ca/corporategovernanceprinciples/43056196.pdf (posljednji pristup 5. veljače 2024.).
[319] Kampmann, A., *op. cit.* u bilj. 15, str. 51.

obrazac sadržava kvalitativne i kvantitativne informacije o rizicima. Osoba zadužena za upravljanje rizicima agregirat će podatke iz svih ispunjenih obrazaca i kreirati opći izvještaj o svim rizicima (engl. *condensed / aggregated risk report*) temeljen na dodatnom unosu podataka osobe zadužene za upravljanje rizicima. Primarni je korisnik općeg izvještaja uprava. Međutim, izvještaj se može slati i operativnim odjelima, internoj reviziji, revizorima, ali i nadzornom odboru društva.[320] Kako bi se osigurala neovisnost i neizmijenjenost izvještaja o rizicima koji je sastavila glavna osoba zadužena za upravljanje rizicima, preporuka je da se (uz upravu) izvještaj šalje direktno istodobno i nadzornom odboru.[321] Važnost toga posebice je vidljiva u slučajevima kada nositelj funkcije upravljanja rizicima ne dijeli isto mišljenje s upravom.[322]

Uprava također sudjeluje u identificiranju znatnijih rizika (pogotovo znatnijih financijskih, operativnih i vanjskih rizika povezanih s ostvarenjem strategije i održavanjem aktivnosti društva)[323], što znači da je dužna sudjelovati u procesu upravljanja rizicima, a to uključuje i komuniciranje o rizicima u obliku redovitog izvještavanja nadzornog odbora o statusu znatnih rizika.[324]

Izvještaj o rizicima može biti standardni (regularni izvještaj koji se sastavlja u skladu s prethodno definiranim sadržajem i u prethodno određenom vremenskom okviru), ali i *ad hoc* koji se sastavlja zbog određenih iznenadnih promjena. Osim u formi formalnog izvještaja o rizicima, komunikacija se može odvijati u formi razgovora o rizicima (engl. *risk talks*) koji mogu poprimiti oblik službenih sastanaka (engl. *formal meetings*), ali i neformalnih razmjena mišljenja.

6.2. Izvješće poslovodstva

[320] *Ibid.*, str. 72.
[321] IIA Nordic Baltic cooperation project, Good practice guidelines for the enterprise risk management function, 2020., str. 6, dostupno na https://iia.no/product/good-practice-guidelines-for-the-enterprise-risk-management-function/ (posljednji pristup 19. siječnja 2024.).
[322] *Ibid.*, str. 38.
[323] HANFA, ZSE, *op. cit.* u bilj. 92, toč. 59., str. 25.
[324] *Ibid.*

Izvješće poslovodstva sadržava, uz objektivan pregled razvoja i rezultata poslovanja društva te njegova položaja, opis glavnih rizika i neizvjesnosti kojima je društvo izloženo.[325] Također, izvješće poslovodstva sadržava naznaku ciljeva i metoda upravljanja financijskim rizikom društva te izloženosti društva rizicima cijena, kreditnim rizicima, rizicima likvidnosti i rizicima novčanog tijeka.[326] Uobičajeno je da se u izvješću poslovodstva naglašavaju rizici kojima je društvo bilo ili će u budućnosti biti izloženo.[327] Pojednostavnjeno govoreći, u izvješću poslovodstva mogu se pronaći informacije o glavnim rizicima društva, pogotovo informacije o financijskim rizicima i upravljanje rizicima financijske prirode. Izvješće poslovodstva sastavni je dio godišnjeg izvješća.[328] ZTK, za razliku od Zakona o računovodstvu, izvješće poslovodstva naziva izvještajem rukovodstva (kao dio godišnjeg izvještavanja), odnosno međuizvještajem rukovodstva (kao dio polugodišnjeg ili kvartalnog izvještavanja). Isti je primjer komuniciranja o rizicima / upravljanju rizicima koje prelazi granice isključivo internog komuniciranja unutar društva. Izvješća poslovodstva, a pogotovo kada je riječ o izdavateljima vrijednosnih papira čiji su vrijednosni papiri uvršteni na uređeno tržište Zagrebačke burze, primjer su komunikacije o rizicima za potrebe svih zainteresiranih dionika tržišta kapitala uključujući i male buduće ulagatelje. Za neka društva propisan je dodatni sadržaj izvješća poslovodstva. Tako primjerice veliki poduzetnici koji su subjekti od javnog interesa i koji na datum bilance prelaze kriterij prosječnog broja od 500 radnika tijekom prethodne poslovne godine u svoje izvješće poslovodstva uključuju nefinancijsko izvješće[329] koje, između ostalog, u kontekstu izvješćivanja o održivosti sadržava opis glavnih rizika za poduzeće povezanih s pitanjima održivosti, uključujući opis glavnih ovisnosti poduzeća kada je riječ o tim pitanjima i način njegova upravljanja tim rizicima.[330] Tako propisani sadržaj izvješća poslovodstva pokazuje važnost upravljanja rizicima, odnosno izvještavanja o tome. S

[325] Čl. 19., st. 1. Direktive 2013/34/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o godišnjim financijskim izvještajima, konsolidiranim financijskim izvještajima i povezanim izvješćima za određene vrste poduzeća, o izmjeni Direktive 2006/43/EZ Europskog parlamenta i Vijeća i o stavljanju izvan snage direktiva Vijeća 78/660/EEZ i 83/349/EEZ (Tekst značajan za EGP) (dalje u tekstu: Direktiva 2013/34/EU).
[326] Čl. 19., st. 2., toč d. Direktive 2013/34/EU.
[327] Žager, K.; Tušek, B.; Sačer, I. M.; Mališ, S. S.; Žager, L., Računovodstvo 1: računovodstvo za neračunovođe, Zagreb, 2016., str. 78.
[328] Čl. 21., st. 2. Zakona o računovodstvu (NN, br. 78/15, 134/15, 120/16, 116/18, 42/20, 47/20, 114/22, 82/23; dalje u tekstu: ZR).
[329] Članak 21.a ZR-a.
[330] Članak 19.a Direktive 2013/34/EU.

time u vezi, vidljivo je da se fokus s financijskih rizika širi i na rizike održivosti, što je indikator njihove važnosti u suvremenom poslovanju i poslovnim trendovima.

6.3 Komentari poslovodstva

Poslovodstvo društva može u sklopu godišnjeg izvješća na dobrovoljnoj osnovi pružiti dodatne komentare koje smatra relevantnim.

Da je tomu tako, najbolje je vidljivo na temelju primjera dva godišnja izvješća, i to revidiranih konsolidiranih godišnjih izvješća za 2022. društava Span d. d. i Atlantic Grupe d. d.[331]

Društvo Span d. d. u sklopu godišnjeg izvješća za 2022., a uz sadržaj godišnjeg izvješća koje je propisano Zakonom o računovodstvu, na 118 A4 stranica pružilo je informacije o povijesti i razvoju grupe, organizacijskoj strukturi grupe, politici upravljanja sukobom interesa, trendovima u industriji, korporativnim događajima, pripajanjima i akvizicijama društava, poslovnim događajima i ostvarenjima, međunarodnom poslovanju, nagradama, priznanjima i postignućima, financijskim pokazateljima za 2022. godinu, ljudima i zajednici, zadržavanju zaposlenika, internoj i eksternoj komunikaciji itd.[332] Ti komentari također sadržavaju informacije o rizicima, financijskim rizicima, pravnim rizicima i rizicima povezanim s poslovanjem društva. Ti komentari pružaju detaljan opis rizika i upravljanja rizicima koji su specifični za društvo i grupu. Konkretno, riječ je o sljedećim skupinama rizika: financijskim, pravnim i vezanim uz poslovanje. U komentarima je navedeno da je društvo tijekom godine razvijalo transparentni sustav upravljanja rizicima u skladu s preporukama norme ISO 31000.[333] Prema komentarima poslovodstva Span je implementirao sustav upravljanja rizicima usklađen s preporukama norme ISO 31000.[334] Uz opći model upravljanja rizicima, društvo SPAN d. d. implementiralo je i ISO 37001[335] koji sadržava posebna pravila o upravljanju

[331] Dokumenti dostupni na internetskoj stranici Zagrebačke burze: https://eho.zse.hr/financijski-izvjestaji.
[332] Vidi u dokumentu naziva „SPAN d.d. (SPAN) – 2022, Godišnji izvještaj – Konsolidirano“, (revidirano) str. 3–118 prvog dijela dokumenta, dostupno na https://eho.zse.hr/financijski-izvjestaji.
[333] SPAN, *op. cit.* u bilj. 332, str. 8.
[334] *Ibid.*
[335] ISO, međunarodni standard 37301, Anti-bribery management systems — Requirements with guidance for use.

rizicima korupcije.[336] Nadalje, implementirana je politika upravljanja rizicima, definirani su apetiti rizika i kreirana je Metodologija upravljanja rizicima.[337] Svrha implementacije upravljanja rizicima transparentno je upravljanje rizicima u svim poslovnim domenama i procesima.[338] Ciljevi i rizici te plan njihove obrade prate se u vlastitoj aplikaciji za upravljanje rizicima.[339]

Što se tiče Atlantic Grupe, ona u godišnjem izvješću za 2022.[340] u komentarima poslovodstva navodi da je izložena brojnim eksternim i internim rizicima. Nadalje, kako bi spriječila i smanjila utjecaj tih rizika na poslovanje, prema komentarima poslovodstva, ona provodi proces integriranog upravljanja rizicima. Time se provodi identifikacija i kvantifikacija rizika. Kao koraci/faze procesa integriranog upravljanja rizicima navode se:

"1. Identifikacija potencijalnih rizika
2. Analiza i procjena utjecaja rizika te donošenje akcijskog plana za mitigaciju
3. Periodično monitoriranje provedbe akcijskog plana mitigiranja rizika
4. Godišnja revizija efikasnosti i provedbe donesenog akcijskog plana."[341]

Prema komentarima poslovodstva, ključni rizici koji mogu imati znatniji utjecaj na poslovni i financijski položaj jesu rizik poslovnog okružja (politički rizici, makroekonomski i socijalni rizici, rizici prirodnih nepogoda i zdravstvenih prijetnji), rizik industrije, rizik konkurencije, poslovni rizici (rizik ovisnosti o proizvodu i poslovnoj suradnji, rizik ovisnosti poslovanja o IT sustavima, rizik privlačenja i zadržavanja ključnih osoba) te financijski rizici (tržišni rizici, kreditni rizici, rizik likvidnosti).[342] Odgovorni odjeli, timovi ili zaposlenici na redovitim dnevnim/tjednim/mjesečnim osnovama prate, nadziru i aktivno upravljaju rizicima.[343]

[336] *Ibid.*
[337] *Ibid.*
[338] *Ibid.*
[339] *Ibid.*
[340] Vidi u dokumentu naziva „ATLANTIC GRUPA d.d. (ATGR) – 2022, Godišnji izvještaj – Konsolidirano" (revidirano) objavljenog 30. ožujka 2023. na internetskoj stranici Zagrebačke burze, str. 3–162.
[341] Cit., *op. cit.* u bilj. 340, str. 148.
[342] *Ibid.*
[343] *Ibid.*

Predmetni komentari poslovodstva (engl. *management commentary*) poznati su pod različitim nazivima poput rasprava i analiza poslovodstva (engl. *management's discussion and analysis* ili skraćeno engl. MD&A), pregled poslovanja i financijski pregled (engl. *operating and financial review*), strateški izvještaj (engl. *strategic report*).[344]

U komentarima poslovodstva društvo može iznijeti glavne rizike kojima je izloženo i opisati kako se ti rizici mijenjaju. Nadalje, društvo može iznijeti planove i strategije za preuzimanje i njihovo ublažavanje te navesti učinkovitost strategija upravljanja rizicima.[345] Takve informacije pomažu korisnicima procijeniti rizike društva i potencijalne ishode (engl. *outcomes*).[346] Poslovodstvo bi trebalo istaknuti glavne rizike i neizvjesnosti kojima je društvo izloženo umjesto objavljivanja svih mogućih rizika i neizvjesnosti.[347] Ako društvo u komentarima poslovodstva objavljuje informacije o nematerijalnim informacijama, one bi kao takve trebale biti označene kako bi se lako razlikovale od informacija o ključnim, odnosno materijalnim rizicima.[348] Prema neobvezujućim smjernicama poslovodstvo treba objaviti glavne strateške, tržišne, operativne i financijske rizike koji mogu utjecati na strategije i vrijednost društva, a opis glavnih rizika treba obuhvatiti moguće posljedice na stvaranje novčanih tokova i sposobnost stvaranja vrijednosti društva.

6.4. Bilješke uz financijske izvještaje

Bilanca, račun dobiti i gubitka, izvještaj o promjenama kapitala, izvještaj o novčanim tijekovima i bilješke uz financijske izvještaje temeljni su financijski izvještaji.[349] „Bilješke uz financijske izvještaje su dodatni, popratni iskazi koji dodatno pojašnjavaju strukturu, vrijednost i obilježja najvažnijih pozicija u ostalim temeljnim financijskim izvještajima".[350]

[344] International Accounting Standards Board (dalje: IASB), Exposure Draft ED/2021/16 Management Commentary, London, 2021., str. 45–47, dostupno na https://www.ifrs.org/content/dam/ifrs/project/management-commentary/ed-2021-6-management-commentary.pdf (posljednji pristup 5. ožujka 2024.).
[345] *Ibid.*
[346] *Ibid.*
[347] *Ibid.*
[348] *Ibid.*, rbr. 8.9., str. 47.
[349] Tintor, Ž., Analiza financijskih izvještaja u funkciji donošenja kvalitetnijih upravljačkih odluka, Obrazovanje za poduzetništvo – E4E: znanstveno stručni časopis o obrazovanju za poduzetništvo, Vol. 10, No. 1, 2020., str. 86.
[350] Definicija preuzeta s internetske stranice http://struna.ihjj.hr/naziv/biljeske-uz-financijske-izvjestaje/45006/.

Računovodstveni standardi propisuju što sve treba objaviti u bilješkama.[351] Primjerice, prema Odluci o objavljivanju Hrvatskih standarda financijskog izvještavanja poduzetnik treba objaviti informacije o ključnim pretpostavkama u vezi s budućnošću poslovanja te procjenu neizvjesnosti na datum bilance koje stvaraju veliki rizik.[352] Sastavljanje i prezentiranje dodatnih informacija u obliku bilješki pridonosi kvaliteti i razumljivosti računovodstvenih informacija zbog toga što one sadržavaju sve one informacije koje se direktno ne vide iz temeljnih financijskih izvještaja, a nužne su i korisne za njihovo razumijevanje i ocjenu kvalitete poslovanja.[353]

Postavlja se pitanje u kojoj su mjeri u praksi informacije o rizicima i njihovu upravljaju zastupljene u bilješkama uz financijske izvještaje na hrvatskom tržištu kapitala, odnosno u kojoj su mjeri takve informacije prepoznate kao dodatne informacije nužne za razumijevanje financijskih izvještaja i ocjenu kvalitete poslovanja društva.

Kako bi se dao odgovor na postavljeno pitanje, autor ovog rada analizirao je šest godišnjih izvješća za 2022. društava čiji su vrijednosni papiri (dionice ili obveznice) uvrštene na uređeno tržište Zagrebačke burze.[354] Od toga su dva godišnja izvješća društava iz bankarskog sektora, jedno iz IT sektora, dva iz prehrambene industrije / ugostiteljstva, jedno iz brodarskog sektora. Uzorak je izabran na način da se obuhvate društva koja posluju u različitim granama djelatnosti.

Za početak se analiziraju i uspoređuju bilješke uz financijske izvještaje godišnjih izvješća društava iz bankarskog sektora. U oba izvješća vidljivo je da bilješke sadržavaju informacije u vezi s upravljanjem rizicima. U jednom je izvješću veličina bilješke u vezi s upravljanjem rizicima otprilike pola jedne stranice, dok je u drugom 55 stranica A4 formata. U bilješci veličine 55 stranica mogu se pronaći sljedeći podatci u vezi s upravljanjem rizicima:

- politika i strategije upravljanja rizicima

[351] Vidi o tome više u Žager, K.; Tušek, B. i ostali u *op. cit.* u bilj. 327.
[352] Toč. 1.42. Odluke o objavljivanju Hrvatskih standarda financijskog izvještavanja (NN, br. 86/15).
[353] Žager, K.; Tušek, B. i ostali u *op. cit.* u bilj. 327, str. 75 i 76.
[354] Revidirani financijski izvještaji Grupe Zagrebačke banke za razdoblje od 01. siječnja do 31. prosinca 2022. godine, Godišnje izvješće za 2022. društva Span d. d., Godišnje izvješće društva Kraš d. d. za godinu koja je završila 31. prosinca 2022. godine, Konsolidirano godišnje izvješće za 2022. godinu zajedno s izvještajem neovisnog revizora za The Garden Brewery Grupu, Konsolidirano godišnje izvješće društva Jadroplov d. d. za godinu koja je završila 31. prosinca 2022. godine, Godišnje revidirano izvješće društva Erste & Steiermärkische Bank d. d. za godinu koja završava 31. prosinca 2022. Svi dokumenti dostupni su na internetskoj stranici Zagrebačke burze.

- organizacija upravljanja rizicima
- integrirano upravljanje rizicima društva
- sklonost preuzimanju rizika
- izjava o preuzimanju rizika
- procjena materijalnosti rizika
- kapacitet za preuzimanje rizika
- pregled i praćenje kreditnog rizika
- izloženost kreditnom riziku
- tržišni rizici
- metode i instrumenti mitigacije (ublažavanja) rizika
- rizik likvidnosti
- operativni rizik
- okvir i standardi upravljanja operativnim rizikom.

Bilješke uz financijske izvještaje društva iz IT sektora također sadržavaju informacije o upravljanju rizicima. One pružaju informaciju o tome tko i na koji način upravlja financijskim rizicima koji uključuju tržišni rizik, valutni rizik, rizik kamatne stope, cjenovni rizik, kreditni rizik i rizik likvidnosti. U konkretnom slučaju odjel financija društva upravlja financijskim rizikom. U dijelu odgovora ili tretmana rizika navedeno je da društvo ima zaključen okvirni ugovor o izvedenim financijskim instrumentima u cilju upravljanja kamatnim i valutnim rizikom te drugim rizicima koji nastaju ili mogu nastati zbog promjene cijena, vrijednosti ili nekih drugih veličina. Ugovaranjem „FX forward transakcija“ društvo upravlja tečajnim rizikom valuta USD i GBP. Kako bi smanjilo kreditni rizik, društvo je prihvatilo politiku poslovanja isključivo s kreditno sposobnim stranama i pribavljanja dostatnih instrumenata osiguranja naplate kako bi, prema potrebi, ublažila rizik financijskog gubitka zbog neispunjenja obveza. Bilješke dvaju društava iz prehrambene industrije / ugostiteljstva te društva iz brodarskog sektora također sadržavaju informacije o upravljanju financijskim rizicima što uključuje i opis financijskih rizika te procjenu njihove bitnosti. Društvo iz brodarskog sektora u svojim bilješkama uz financijske izvještaje navodi ciljeve upravljanja financijskim rizikom, upravljanja cjenovnim rizikom, opise kamatnog i kreditnog rizika, upravljanja valutnim rizikom i rizikom likvidnosti.

Društvo iz brodarske industrije navodi da „funkcija riznice“ prati financijske rizike i njima upravlja putem internih izvještaja o rizicima u kojima su izloženosti analizirane po stupnju i veličini rizika. U bilješkama brodarskog društva navodi se da krajnju odgovornost za upravljanje kreditnim rizikom snosi uprava, koja je postavila kvalitetan okvir za upravljanje rizikom likvidnosti po kratkim, srednjim i dugim pozicijama grupe i definirala zahtjeve koji se odnose na upravljanje likvidnošću.

Na temelju ispitanog uzorka evidentno je da bilješke uz financijske izvještaje kao dodatni i popratni iskazi sadržavaju informacije o rizicima i upravljanju rizicima. Naime, u svih šest godišnjih izvješća utvrđeno je da bilješke uz financijske izvještaje pružaju informacije o rizicima i njihovu upravljanju.

6.5. Prospekti vrijednosnih papira[355] kao izvor informacija o rizicima

Pri javnoj ponudi i/ili uvrštenju vrijednosnih papira na uređeno tržište sastavlja se prospekt vrijednosnih papira koji sadržava informacije koje služe ulagatelju da informirano odluči o (ne)ulaganju u vrijednosne papire.[356] Između ostalog, sadržaj prospekta vrijednosnih papira čine i informacije o rizicima kojima su izloženi izdavatelji vrijednosnih papira pri svojem poslovanju na određenom tržištu.[357] Prije objave prospekta vrijednosnih papira mora ga odobriti nadležno nacionalno tijelo.[358]

Takav prospekt vrijednosnih papira, osim što je primjer dokumenta koji sadržava informacije o rizicima, ujedno je i relevantan primjer dobrih praksi i primjene pravila (smjernica) o načinu na koji valja eksterno komunicirati o rizicima (ali i o njihovu upravljanju)

[355] Vidi više o prospektu vrijednosnih papira u Đurđenić, K.; Krunić, V.; Simić, S., Prospekt vrijednosnih papira – Gdje smo i kamo idemo, Pravo u gospodarstvu, 2016., 2, Zagreb.
[356] Čl. 1., st. 1. Uredbe (EU) 2017/1129 Europskog parlamenta i Vijeća od 14. lipnja 2017. o prospektu koji je potrebno objaviti prilikom javne ponude vrijednosnih papira ili prilikom uvrštavanja za trgovanje na uređenom tržištu te stavljanju izvan snage Direktive 2003/71/EZ (Tekst značajan za EGP) (dalje u tekstu: Uredba o prospektu).
[357] Čl. 16., st. 1. Uredbe o prospektu.
[358] Čl. 20., st. 1. Uredbe o prospektu.

kod obraćanja javnosti pri javnoj ponudi i/ili uvrštenju vrijednosnih papira na uređeno tržište.[359]

Kada potencijalni ulagatelj odlučuje o ulaganju u vrijednosne papire, on se nalazi u situaciji informacijske asimetrije pa ne iznenađuje važnost odgovarajućeg prezentiranja rizika društva u prospektu jer će informacije o rizicima (uz ostali sadržaj prospekta) ulagatelju omogućiti donošenje informirane investicijske odluke, odnosno omogućiti mu procjenu rizičnosti poslovanja društva koje izdaje vrijednosne papire koji su predmetom javne ponude i/ili uvrštenja na uređeno tržište.[360]

Od 2007. do 2016. u Europskom gospodarskom prostoru godišnje se odobrilo 4300 prospekata vrijednosnih papira.[361] Na hrvatskom tržištu kapitala prosječan broj odobrenih prospekata od 2021. do 2022. iznosio je prosječno 10 prospekata godišnje.[362] Ti brojevi pokazuju koliko postoji takvih dokumenata koji sadržavaju podatke o rizicima društva.

U Republici Hrvatskoj nadležno nacionalno tijelo za odobrenje prospekata vrijednosnih papira (uključujući i sadržaje informacija o rizicima i njihovu upravljanju) jest Hrvatska agencija za nadzor financijskih usluga.[363]

Rizici u vezi s izdavateljem (odnosno, rizici društva) koji se navode u prospektu moraju biti specifični za izdavatelja.[364] Kako bi prikaz rizika u prospektu bio odgovarajući, rizici koji se navode u prospektu moraju biti također bitni (ili značajni) te potkrijepljeni sadržajem cjelokupnog prospekta.[365] Specifični rizici sadržavaju jasnu i izravnu poveznicu s izdavateljem vrijednosnog papira.[366] „'Poveznicu' između rizika s jedne strane, te izdavatelja s druge strane, treba promatrati kao opipljive i jasne činjenične okolnosti u najširem smislu riječi, koje će

[359] Vidjeti više o prezentiranju rizika u prospektima vrijednosnih papira u Krunić, V., Prezentiranje rizika u prospektima vrijednosnih papira na europskom tržištu kapitala, Pravo u gospodarstvu, Vol. 62, No 3, Zagreb, 2023., str. 367–415.
[360] Krunić, V., *op. cit.* u bilj. 359, str. 370.
[361] ESMA, EU Prospectuses: ESMA Statistical Report 2022, Pariz, 2022., dostupno na https://www.esma.europa.eu/sites/default/files/library/esma50-165-2336_esma_statistical_report_-_eu_prospectuses.pdf (posljednji pristup 5. ožujka 2024.).
[362] Krunić, V., *op. cit.* u bilj. 359, str. 370.
[363] Čl. 405., st. 2. ZTK-a.
[364] Čl. 16., st. 1. Uredbe o prospektu.
[365] Čl. 16., st. 1. Uredbe o prospektu.
[366] ESMA, Smjernice o čimbenicima rizika u skladu s Uredbom o prospektu, 2019. (dalje u tekstu: Smjernice ESMA-e o rizicima), Smjernica 1, toč. i., dostupno na https://www.esma.europa.eu/sites/default/files/library/esma31-62-1293_guidelines_on_risk_factors_under_the_prospectus_regulation_hr.pdf (posljednji pristup 21. veljače 2024.).

očigledno opravdati navođenje konkretnog rizika u konkretnom slučaju za konkretnog izdavatelja i konkretni vrijednosni papir".[367]

Nadalje, prospekt ne smije sadržavati rizike koji su generički[368] u smislu da su potpuno općenite naravi.[369] Takvi rizici nisu prezentirani u prospektu na način da bi se stekao dojam da se oni odnose upravo na konkretnog izdavatelja.[370] Generički rizici ne sadržavaju dovoljno detalja koji bi čitatelju prospekta omogućili mentalno stvaranje slika rizika[371] te kao takvi ne smiju biti uključeni u prospekt.[372]

Također, prospekt vrijednosnih papira ne smije sadržavati rizike društva čija je namjera navođenja isključivo oslobođenje izdavatelja od odgovornosti.[373] Primjer takva navođenja rizika u prospektu je tvrdnja koja slijedi: „Izdavatelj ne može garantirati da se neće ostvariti rizik gubitka pravnih sporova te stoga nije odgovoran ako se konkretni rizik ostvari".[374]

„U situaciji kada izdavatelj u prospektu nije naveo nikakve druge informacije u vezi s rizikom gubitka pravnih sporova izuzev tvrdnje da ne može garantirati da se predmetni rizik neće ostvariti, takav nespecifičan rizik koji je izdavatelj naveo samo s namjerom da bude naveden u prospektu te da štiti izdavatelja od odgovornosti (u slučaju da izdavatelj izgubi pravne sporove, a ulagatelju primjerice padne vrijednost dionica) ne smije biti naveden u prospektu te ga je potrebno izmijeniti ili objasniti."[375] Bitni ili značajni rizici u vezi s izdavateljem oni su rizici čije bi nenavođenje ili pogrešno navođenje u prospektu drugačije utjecalo na odluku o ulaganju donesenu na temelju informacija u prospektu.[376]

Pri sastavljanju prospekta društvo koje izdaje vrijednosne papire i/ili traži uvrštenje za trgovanje na uređenom tržištu procjenjuje bitnost rizika na temelju vjerojatnosti njihova pojavljivanja te očekivanog opsega njihova negativnog utjecaja.[377] Stoga, a u kontekstu

[367] Cit., Krunić, V., *op. cit.* u bilj. 359, str. 377 i 378.
[368] Recital 54. Uredbe o prospektu.
[369] Krunić, V., *op. cit.* u bilj. 359, str. 379.
[370] *Ibid.*
[371] Arikan, O., The effect of boilerplate language on nonprofessional investors judgements, Accounting and Businsess Research, sv. 52, br. 4, London, 2021., str. 417–442.
[372] Vidjeti više o tome u Krunić, V., *op. cit.* u bilj. 359, str. 380.
[373] Recital 54. Uredbe o prospektu.
[374] Vidi Esma, Final Report – Prospectuse Peer Review, Pariz, 2022., rbr. 424.
[375] Cit., Krunić, V., *op. cit.* u bilj. 359, str. 380 i 381.
[376] Esma, CP on Guidelines o risk factors under the Prospectus Regulation, 2018., rbr. 28., str. 16.
[377] Članak 16., st. 2. Uredbe o prospektu.

navođenja rizika u prospektima, daje se naslutiti da su takvi rizici čisti, odnosno gledaju se u kontekstu prijetnje. U praksi se identificirani rizici mogu procijeniti i rangirati koristeći se mapom rizika (engl. *risk mapping*), što društvu može pomoći za sastavljanje prospekta.[378] Naime, društvo koje upravlja rizicima na način da je implementiralo proces upravljanja rizicima lakše će sastaviti prospekt u dijelu traženih informacija u vezi s rizicima. Odgovornost za procjenu rizika leži na izdavatelju te ako iz podataka u prospektu nije jasna bitnost rizika, nadležno tijelo za odobrenje prospekta trebalo bi od osoba odgovornih za sastavljanje prospekta zatražiti da se rizik jasnije obrazloži ili izmijeni.[379] Pretpostavka je da bi u redovitim okolnostima izdavatelj, odnosno njegova uprava, nadzorni odbor, rizik menadžer trebali najbolje znati rizike u vezi s poslovanjem društva.[380] Iako pravila o prospektu eksplicitno ne zahtijevaju od društava uključivanje u prospekt informacija o upravljanju rizicima (a samim time ni o procesu upravljanja rizicima), takve informacije zasigurno bi potencijalno mogle biti relevantan izvor informacija koje potencijalnim ulagateljima omogućuju donošenje informirane investicijske odluke.[381] „Iako razumni opisi politika upravljanja rizicima koji su prezentirani na primjeren način nisu sporni odnosno zabranjeni, dugački i detaljni opisi politika upravljanja rizicima koji bi mogli ograničiti ili narušiti dojam čitatelja o stvarnom opsegu negativnog utjecaja rizika ili o vjerojatnosti njegova nastanka u toj mjeri da čitatelju više nije jasno postoji li preostali značajan rizik predstavljaju primjer zabranjene prekomjerne i neprimjerene uporabe ublažavajućih izraza.“[382]

Prospektna regulativa izričito prepoznaje dvije temeljne kategorije rizika: rizike u vezi s izdavateljem vrijednosnog papira i u vezi s vrijednosnim papirom.[383] Rizici u vezi s izdavateljem mogli bi se podijeliti u sljedeće kategorije:

- rizici povezani s financijskim stanjem izdavatelja
- rizici povezani s poslovnim djelatnostima izdavatelja i granom industrije u kojoj posluje

[378] Miloš Sprčić, D., Upravljanje rizicima: Temeljni koncepti, strategije i instrumenti, Zagreb, 2013., str. 104.
[379] Smjernice ESMA-e o rizicima, Smjernica 3., str. 10.
[380] Krunić, V., *op. cit.* u bilj. 359, str. 388.
[381] Van Daelen, M., Risk management solutions in business law: Prospectus disclosure requirements, Tilburg 2008., str. 31.
[382] Cit., Krunić, V., *op. cit.* u bilj. 359, str. 391–393.
[383] *Ibid.*, str. 394 i 395.

- pravni i regulativni rizik
- rizik unutarnje kontrole
- ekološki, socijalni i upravljački rizici.[384]

Prospekt sadržava i sažetak u kojem se navode ključne informacije potrebne ulagateljima da bi, između ostalog, razumjeli karakteristike i rizike izdavatelja.[385] Iz toga proizlazi da sažetak prospekta sadržava ključne rizike za izdavatelja. Sasvim logično i opravdano postavlja se pitanje što znači „ključni" rizik.[386] Ključni je rizik bitan rizik koji je dostatno važan da ga se uključi u sažetak prospekta te je „ključnost" nadstandard uz pojam bitnosti.[387]

7. RIZIK U PODUZETNIČKOM KONTEKSTU

7.1. Poduzetničke odluke i načelo poduzetničke svrhovitosti

Iako ne postoji opća obveza prema ZTD-u da sva trgovačka društva moraju imati sustav upravljanja rizicima, to ne znači da društva, odnosno članovi uprave ne moraju u nekoj mjeri voditi računa o rizicima, odnosno upravljati rizicima u nekom obliku. To najbolje dolazi do izražaja kod donošenja poduzetničkih odluka i utvrđivanja postojanja/nepostojanja „prevelikih rizika".

Naime, kada uprava dioničkog društva ili društva s ograničenom odgovornošću (dalje u tekstu: društvo ili trgovačko društvo) donosi poduzetničke odluke, one se donose u uvjetima rizika. Nema posla bez preuzimanja nekog rizika.[388] Rijetke su situacije izvjesnosti kada je riječ o samo jednom jedinom ishodu, kada nema neizvjesnosti pa time ni rizika.[389] Poduzetničke odluke o tome hoće li jedno društvo preuzeti drugo društvo, lansirati dosad neviđeni inovativni proizvod, proširiti svoje poslovanje u drugu državu, (ne) uložiti u

[384] Smjernice ESMA-e o rizicima, toč. 35., str. 12.
[385] Vidi članak 7. Uredbe o prospektu.
[386] Krunić, V., *op. cit.* u bilj. 359, str. 404–407.
[387] *Ibid.*
[388] Barbić, J., Pravo društava, Knjiga druga, Društva kapitala, Svezak 1., Dioničko društvo, sedmo izmijenjeno i dopunjeno izdanje, Zagreb, 2020., str. 987.
[389] O donošenju odluka u uvjetima izvjesnosti vidi više u Miloš Sprčić, D., Upravljanje rizicima, str. 5.

vrijednosne papire, pristupiti zajedničkom pothvatu, otpustiti znatan broj radnika radi namjeravane uštede troškova, donose se u uvjetima rizika koji mogu utjecati (pozitivno ili negativno) na realizaciju ciljeva društva. Primjerice, cilj društva može biti kreiranje i komercijalno lansiranje izuma. Rizik je s time u vezi hoće li izum uistinu biti izumljen, hoće li se moći komercijalno proizvoditi, hoće li ga kupci prihvatiti, može li društvo financijski podnijeti dugogodišnje troškove koji bi mogli proizići iz istraživanja i razvoja. Međutim, netko mora donijeti poduzetničku odluku hoće li se, kada i na koji način krenuti u smjeru izuma, odnosno odustati od započetog smjera ako se ustanovi da su rizici povezani s nastavkom pothvata pretjerano visoki (npr. u očitom nerazmjeru s politikama preuzimanja rizika ili je iznimno velika vjerojatnost stečaja društva zbog troškova). Takve su poduzetničke odluke kompleksne i nisu jednostavne[390] te o njima uprava odlučuje na temelju poduzetničke svrhovitosti.

Je li nešto poduzetnički svrhovito, može se promatrati kroz prizmu odnosa između rizika (u smislu opasnosti) te potencijalnih prilika.[391] Razumno je pretpostaviti da poduzetnička odluka za koju se veže vrlo vjerojatno ostvariv rizik propasti društva, a koja donosi iznimno malu vjerojatnost minimalne zarade, zasigurno nije svrhovita poduzetnička odluka, odnosno odgovarajući odnos između potencijalnih opasnosti i prilika.

Konotacije koje se vežu uz poduzetnike u kontekstu donošenja poduzetničkih odluka jesu da su oni samopouzdani, specijalizirani / imaju iskustava u preuzimanju rizika te istančane sposobnosti upravljanja rizicima. Percepcije su da su poduzetnici skloniji preuzimati rizike nego drugi te da su kvalificirani donijeti prosudbu koje rizike valja preuzeti, a koje ne. Nadalje, poduzetnike se percipira kao nositelje/preuzimatelje rizika. Sve te konotacije u vezi s poduzetnicima potvrđuju da poduzetničke odluke uvelike obilježava njihovo donošenje u okružju rizika, odnosno da donošenje poduzetničkih odluka implicira (što svjesno ili nesvjesno, formalizirano ili ne) odlučivanje o preuzimanju rizika.[392]

S druge strane, nije riječ o poduzetničkim odlukama u slučajevima kada je uprava društva dužna ispuniti zakonom, statutom, poslovnikom o radu i ugovorom koji su članovi

[390] O razlici između jednostavnih i kompleksnih odluka vidi u Hillson, D., *op. cit.* u bilj. 2, str. 237.
[391] Keay, A.; Loughrey, J., The Concept of Business Judgment, Legal Studies, 39 (1), 2019., str. 36–55.
[392] *Ibid.*

sklopili s društvom propisanu obvezu pa zbog toga nema slobodnog odlučivanja uprave.[393] Obavješćivanje nadzornog odbora od uprave, briga o vođenju poslovnih knjiga, postupanje kako je zakonom propisano u slučaju gubitka, prezaduženosti ili nesposobnosti društva za plaćanje, davanje obavijesti dioničarima na način propisan zakonom nije donošenje poduzetničkih odluka.[394]

7.2. Primjerenost informacija o rizicima

ZTD-om je propisano da članovi uprave dioničkog društva moraju voditi poslove društva s pozornošću urednog i savjesnog gospodarstvenika.[395] To pravilo implicira da su članovi uprave dioničkog društva pri donošenju poduzetničke odluke dužni postupati s pozornošću urednog i savjesnog gospodarstvenika. Uredan i savjestan gospodarstvenik donosi one poduzetničke odluke za koje se pri njihovu donošenju smije na temelju primjerenih informacija razumno pretpostaviti da djeluje za dobrobit društva. Za društvo s ograničenom odgovornošću također je propisano da uprava vodi poslove društva te se na odgovornost članova uprave društva s ograničenom odgovornošću na odgovarajući način primjenjuju odredbe članka 252. o odgovornosti članova uprave dioničkog društva. Razumna pretpostavka o djelovanju za dobrobit trgovačkog društva ne smije biti utemeljena isključivo na (iracionalnoj) intuiciji člana uprave koja nema uporište u primjerenim informacijama u vezi s namjeravanom poduzetničkom odlukom.

U praktičnom smislu to znači da su pri donošenju poduzetničkih odluka članovi uprave društva kao uredni i savjesni gospodarstvenici dužni koristiti se / razmotriti / uzeti u obzir / raspitati se / pribaviti primjerene informacije na temelju kojih smiju razumno pretpostaviti djeluju li za dobrobiti društva. Drugim riječima, svaka poduzetnička odluka mora biti temeljena na dostatnoj činjeničnoj osnovi (engl. *sufficient factual basis*).[396] Sasvim opravdano postavlja se pitanje na što se takve informacije trebaju odnositi, odnosno s čime su one u vezi te koja je

[393] Barbić, J., *op. cit.* u bilj. 388, str. 988.
[394] Primjeri preuzeti iz *ibid.*
[395] Čl. 252., st. 1. ZTD-a.
[396] Grigoleit, H. C., Director's Liability and Enforcement Mechanism – General Structure and Key Issues – From the German Perspective, Conference on German and Asian Perspectives on Company Law u Hamburgu, 28. i 29. svibnja 2015., str. 5.

njihova priroda, kvaliteta i količina. Konkretno, a u kontekstu ovog rada, razmatra se obuhvaća li i u kojoj mjeri pojam primjerenih informacija primjerene informacije koje omogućuju identificirati i procijeniti „preveliku" rizičnost namjeravane poduzetničke odluke, odnosno može li razumna pretpostavka djelovanja za dobrobit društva postojati bez uzimanja u obzir okružja rizika koji su esencijalno obilježje habitata poduzetničke odluke.

Zamislimo situaciju da član uprave razmatra / premišlja se između donošenja triju iznimno bitnih strateških različitih poduzetničkih odluka (odluke A, B i C). Uzmimo primjerice da se član uprave odlučio za opciju B i da je poduzetnička odluka na kraju imala iznimno štetan utjecaj za društvo u financijskom smislu. Ako član uprave nije osobno izvršio zasebnu analizu rizika u vezi sa svakom mogućom poduzetničkom odlukom, nije zatražio ni od koga mišljenje s time u vezi (npr. angažirao vanjskog stručnjaka da izradi analizu rizičnosti za društvo) niti se s kim od zaposlenika u društvu s time u vezi interno konzultirao, u slučaju negativnih posljedica poduzetničke odluke za društvo za koju član uprave nije prikupio primjerene informacije u vezi s rizičnošću, a bila je riječ o strateškim poslovnim odlukama, takvu članu uprave zasigurno neće biti (kao tuženiku u parnici radi naknada štete društva) lako dokazati da je na temelju primjerenih informacija smio razumno pretpostaviti da djeluje za dobrobit društva. Prikupljanje „primjerenih" informacija koje će biti fond/baza informacija primjerenih za donošenje poduzetničke odluke pravni je standard koji ne zahtijeva prikupljanje „svih potencijalno dostupnih informacija" te će njegova procjena ovisiti o konkretnim okolnostima.[397] Primjerenost ovisi o konkretnoj namjeravanoj poduzetničkoj odluci od slučaja do slučaja.[398] U kontekstu spomenutog primjera donošenja iznimno bitne strateške poduzetničke odluke, uredan i savjestan gospodarstvenik morao bi pomno prikupiti informacije te njihovoj analizi posvetiti dovoljno vremena kako bi osvijestio razinu rizičnosti u vezi s konkretnom namjeravanom poduzetničkom odlukom.[399] U slučaju da član uprave ne može procijeniti rizik zbog toga što mora odlučiti u iznimno kratkom roku koji ni na koji način ne omogućuje pripremu i prikupljanje primjerenih informacija, on bi se trebao suzdržati od

[397] Winner, M., The Duty of Care and Business Judgment Rule in Austrian Company Law, AUC IURIDICA 68., Prag, 2022., str. 17.
[398] Grigoleit, H. C., *op. cit.* u bilj. 396, str. 6.
[399] Winner, M., *op. cit.* u bilj. 397, str. 17.

donošenja poduzetničke odluke.[400] Drugim riječima, određene faze procesa upravljanja rizicima poput utvrđivanja, procjene/analize i odgovora na „preveliki rizik“ sastavni su dio donošenja poduzetničkih odluka. Ako član uprave ne može procijeniti rizičnost poduzetničke odluke jer ne može samostalno ili putem zaposlenika društva prikupiti primjerene informacije koje će mu poslužiti kao baza za procjenu rizika, dužan je angažirati vanjskog stručnjaka.[401] Angažirati vanjskog stručnjaka potrebno je kada „dostupno“ znanje unutar društva nije dovoljno da se cit.: „procijeni problem“, odnosno izvaže rizik povezan s namjeravanom poduzetničkom odlukom.[402]

Nije naodmet istaknuti da je važno da se rizik ima u vidu u vrijeme donošenja poduzetničke odluke, da se u skladu s pravilima struke procijeni mogućnost njegova nastupanja, njegova veličina i utjecaj te da se poduzmu ili predvide buduće mjere za otklanjanje njegovih posljedica.[403]

7.3. *Business judgement rule* i zabrana preuzimanja prevelikog rizika

U vezi s pozornošću koju moraju pokazati članovi uprave, u pravu SAD-a razvio se *business judgement rule* po kojem nema sudske kontrole članova uprave ako se u svom poslu pridržavaju pretpostavki poslovne prosudbe.[404] To pravilo prihvaćeno je u njemačkoj sudskoj praksi, a sadržano je i u hrvatskom ZTD-u (čl. 252.).[405]

Prema stručnoj literaturi, pretpostavke su za primjenu pravila poslovne prosudbe sljedeće:

a) „mora se raditi o poduzetničkoj odluci,
b) uprava mora razumno pretpostaviti da djeluje za dobrobit društva,
c) ne smije biti riječ o prevelikom riziku,
d) odluka se mora donijeti na temelju primjerenih informacija,

[400] *Ibid.,* str. 18.
[401] *Ibid.*
[402] *Ibid.*
[403] Barbić, J., *op. cit.* u bilj. 388, str. 987.
[404] *Ibid.,* str. 985.
[405] *Ibid.*

e) ne smije postojati sukob interesa niti se smije djelovati pod utjecajem koji je nespojiv s onim što se poduzima,
f) mora se djelovati u dobroj vjeri.“[406]

Određeni elementi poput poduzetničke odluke i primjerenosti informacija objašnjeni su u radu.

Ako se ispune sve spomenute pretpostavke, nije riječ o povredi obveze člana uprave da djeluje kao savjestan i uredan gospodarstvenik.[407] Drugim riječima, iako stvari krenu po zlu, član uprave neće biti odgovoran za štetu koju je društvo pretrpjelo zbog negativna ishoda poduzetničke odluke.

Na temelju navedenih pretpostavki za primjenu pravila poslovne prosudbe, vidljivo je da je razina rizika povezanog s poduzetničkom odlukom (ne smije biti riječ o prevelikom riziku) element/kriterij koji se uzima u obzir pri procjeni djeluje li član uprave s pozornošću urednog i savjesnog gospodarstvenika. Taj kriterij uvelike je prihvaćen u praksi njemačkih sudova.[408] Razboriti član uprave koji je svjestan mogućnosti da će u slučaju spora radi naknade štete društvu morati dokazivati pretpostavke za primjenu poslovne prosudbe bit će sklon preventivno i pravodobno pisano dokumentirati i obrazložiti primjerene informacije koje su ga navele da zaključi da nije riječ o pretjerano velikom riziku za društvo. Razboriti član uprave dokumentirat će identifikaciju i procjenu rizika u vezi s namjeravanom poduzetničkom odlukom.

7.4. *Benchmark* (referentna točka, točka usporedbe) za procjenu prekomjernosti rizika

Uobičajeno je da članovi uprave u donošenju poduzetničkih odluka uime društva preuzimaju tržišne rizike. Oni svojim djelovanjem pokazuju poduzetnički žar (engl. *entrepreneurial flair*) te donose poduzetničke odluke s ciljem uspostave, povećanja i

[406] Cit., Barbić, J., *op. cit.* u bilj. 388, str. 985.
[407] *Ibid.*
[408] Yaru, C., The business of judging directors' business judgements in Singapore courts, Singapur, 2016., dostupno na https://law.nus.edu.sg/people/yaru-chia/ (posljednji put 9. siječnja 2024.).

održavanja profitabilnosti poslovanja društva.[409] Takve odluke moraju se donositi u „duhu“ društva (engl. *in a spirit of enterprise*).[410]

Pojedini stručnjaci ističu da je esencijalno pri donošenju poduzetničke odluke procijeniti odnos prijetnji i prilika koje proizlaze iz rizika te djelovati u okvirima racionalnosti.[411] Drugim riječima, rizik je potrebno analizirati/procijeniti, što je zapravo jedna od faza procesa upravljanja rizicima. Jedan od ciljeva postojanja pravila poslovne prosudbe jest zaštita članova uprave koji su spremni iskoristiti prilike koje proizlaze iz odgovornog preuzimanja rizika (engl. *responsible risk taking*).[412]

Iako je na prvi pogled sasvim razumljivo i nedvojbeno da uredni i savjesni gospodarstvenik ne smije preuzimati prevelike rizike, ipak je „preuzimanje prevelikih rizika“ kao izraz podložno različitim mogućnostima tumačenja. Granice između prihvatljivog rizika (engl. *acceptable risk*) koji društvo može odgovarajuće preuzeti i neprihvatljivog rizika koji bi bio povreda pravila poslovne prosudbe katkad nisu kristalno jasne.

S ciljem osvještavanja subjektivnosti percepcije što je malo, veliko, preveliko u kontekstu rizika, povucimo paralelu sa svakodnevnim životom. Prevelika porcija hrane prema subjektivnoj percepciji jedne osobe može biti sasvim standardna porcija prema subjektivnoj percepciji druge osobe. Stoga, a kako bi se izbjeglo lutanje u magli, potrebno je identificirati čvrste kriterije, odnosno *benchmark* iliti točke usporedbe koji mogu poslužiti za utvrđivanje je li što preveliko (primjerice rizik). U kontekstu prehrane kao *benchmark* mogao bi poslužiti neki općeprihvaćeni normativ ili gramaža/veličina porcije koja je uobičajena za prosječnu odraslu osobu. U kontekstu rizika, odgovor na pitanje što može biti *benchmark* baš nije jednostavan.

Primjeri prekomjernog rizika u stručnoj literaturi navode se kao „ulaganje viška novca u problematične vrijednosne papire, špekuliranje na burzi društva kome burzovni poslovi nisu u predmetu poslovanja, kreditiranje nekoga za koga je očito da mu prijeti stečaj ili obustava plaćanja, a da tražbine društva s tog naslova nisu valjano osigurane, sklapanje poslova u zemljama s problematičnom mogućnošću naplate tražbina, a da nije ugovoreno primjereno

[409] Keay, A.; Loughrey, J., *op. cit.* u bilj. 391, str. 44.
[410] *Ibid.*
[411] Joskova, L.,The Business Judgement rule in the Czech Republic, ACTA UNIVERSITATIS CAROLINAE – IURIDICA 3, Prag, 2022., str. 37–47.
[412] Varzaly, J. (2012). Protecting the Authority of Directors: An Empirical Analysis of the Statutory Business Judgment Rule, Journal of Corporate Law Studies, listopad 2012., str. 440.

osiguranje nekog pouzdanog izvan njih, ulaženje u poslove bez provjeravanja boniteta druge strane u poslu."[413]

Da katkad nisu granice između prihvatljivog i prekomjernog rizika (bez detaljnije analize) kristalno jasne, pokazat će se na primjeru ulaganja „viška" novca u problematične vrijednosne papire. Naime, višak novca društva sugerira da taj višak, ako se i izgubi, neće ugroziti kontinuitet poslovanja (jer inače ne bi bio višak). Stoga, ako je društvo uložilo određeni (manji) postotak viška novca (u odnosu na cjelokupni iznos viška) u problematične vrijednosne papire za koje se argumentirano smatra da mogu donijeti povećani prihod društvu, takva poduzetnička odluka koja ne riskira kontinuitet poslovanja, a potencijalno donosi priliku za visoku zaradu (veća razina prilika nego opasnosti), možda i ne bi trebala biti primjer prekomjernog rizika. S druge strane, ulaganje kompletnog iznosa svih raspoloživih sredstava (neovisno o tome je li riječ o „višku ili ne" zbog kojih iznos obrtnog kapitala društva postaje nedostatan) u problematične vrijednosne papire i to jednog izdavatelja (potpuna koncentracija ulaganja) snažan je indicij poduzetničke odluke koja bi itekako mogla biti prekomjerno rizična odluka, a pogotovo ako su usto prilike koje proizlaze iz rizika višestruko manje nego opasnosti (povreda načela poduzetničke svrhovitosti). Stoga, teško je *a priori* govoriti o prekomjernosti rizika bez uzimanja u obzir konteksta rizika koji se sastoji od relevantnih činjeničnih okolnosti i temeljnih koncepata koji proizlaze iz područja upravljanja rizicima.

U Njemačkoj je 2009. o problematici ekscesivnog rizika povezanog s ulaganjem u problematične vrijednosne papire odlučivao Visoki regionalni sud u Dusseldorfu u slučaju kreditne institucije IKB Deutsche Industribank.[414] Ta je banka zbog investiranja u određene problematične vrijednosne papire (dužničke vrijednosne papire sekuritizirane hipotekama u SAD-u) nakon globalne financijske krize podnijela iznimke gubitke (engl. *heavy losses*) te ju je njemačka vlada morala spasiti poduzimajući određene mjere (engl. *bail out*).[415] Njemački je sud odlučio da su članovi uprave i nadzornog odbora banke povrijedili dužnu pažnju. U konkretnom slučaju sud je smatrao da članovi uprave nisu postupali s dužnom pažnjom zbog

[413] Cit., Barbić, J., *op. cit.* u bilj. 388, str. 987.
[414] Gerner-Beuerle, C.; The duty of care and the business judgment rule: A case study in legal transplants and local narratives u knjizi Afsharipour, A.; Gelter, M., Comparative Corporate Governance, Cheltenham, 2012., str. 21.
[415] *Ibid.*, str. 22.

toga što su preuzeli rizike koji ako se ostvare mogu učiniti društvo insolventnim. Nadalje, ti su rizici bili povezani sa stranim, nepoznatim financijskim instrumentima koji se ne mogu kontrolirati. Uprava nije postupala s dužnom pažnjom jer je svjesno pristala na prekomjeran (između ostalog i koncentracijski) rizik. Naime, u jednom trenutku 47 % sveukupnog poslovnog volumena banke (engl. *total business volume*) bilo je izloženo „problematičnim" vrijednosnim papirima, a članovi uprave nisu vodili računa o upravljanju rizikom koncentracije. Prema njemačkoj presudi, članovi nadzornog odbora banke povrijedili su dužnu pažnju jer, između ostalog, nisu na odgovarajući način reagirali na neodgovarajuću izloženost rizicima.

Poruka koja proizlazi iz presude njemačkog suda jest da nije poželjno da članovi uprave društva preuzimaju prevelike rizike te su upravo stoga suočeni s povećanim rizikom osobne odgovornosti kako bi pozorno razmislili prije donošenja previše rizičnih poduzetničkih odluka.[416]

Izričaj pretpostavke „da ne smije biti riječ o prevelikom riziku" pravila poslovne prosudbe ne sadržava naznaku/identifikaciju/odabir/opis referentne točke s kojom će se uspoređivati je li riječ o prevelikom riziku. Ključno pitanje koje se postavlja jest u odnosu na što se procjenjuje je li namjeravana poduzetnička odluka preveliki odnosno prekomjerni rizik za društvo?

Primjer pravila koja sadržavaju referentnu točku za usporedbu prekomjernosti rizika jesu smjernice *Financial Stability Boarda* o nadzornoj interakciji s financijskim institucijama u vezi s kulturom rizika.[417] U njima je navedeno da „posljedice moraju biti jasno uspostavljene, artikulirane i primijenjene na bilo koga tko sudjeluje u preuzimanju rizika ili podupire preuzimanje rizika koje je ekscesivno u odnosu na izjavu financijske institucije u vezi sa sklonošću preuzimanju rizika, neovisno o tome što je to rezultiralo prihodom. U danom primjeru ekscesivnost rizika procjenjuje se u odnosu na izjavu o sklonosti preuzimanju rizika, što implicira da sklonost društva preuzimanju rizika (jedan od temeljnih koncepata) može poslužiti kao referentna točka za procjenu prekomjernosti rizika.

[416] Yaru, C., *op. cit.* u bilj. 408, str. 437.
[417] Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture, 2014., dostupno na https://www.fsb.org/wp-content/uploads/140407.pdf (posljednji pristup 7. ožujka 2024.).

Primjerice, društvo može imati politiku preuzimanja iznimno velikih rizika koji mogu imati i visokopozitivne utjecaje i visokonegativne utjecaje. O apetitu za rizikom u pravilu odlučuju uprava i nadzorni odbor. Stoga, ako je društvo sklono preuzimati iznimno velike rizike, za takvo društvo u kontekstu poduzetničkih odluka iznimno veliki rizici neće biti prekomjerni. S druge strane, ako je društvo sklono preuzimanju srednje umjerenih rizika i ima nultu toleranciju prema velikim i iznimno velikim rizicima, onda će iznimno veliki rizici za takvo društvo zasigurno biti preveliki odnosno prekomjerni. Ti primjeri idealno dočaravaju okružje u okviru kojeg procjena prevelikog rizika može varirati ovisno o sklonosti preuzimanju rizika.[418]

Drugi primjer moguće referentne točke za procjenu prekomjernosti rizika proizlazi iz pravila Kodeksa korporativnog upravljanja ZSE-a i HANFA-e. U skladu s Kodeksom, prekomjerni rizici su oni rizici koji nisu u skladu sa „strategijom". Napominje se da Kodeks ne definira pojam „strategije" pa nije razvidno odnosi li se strategija na strategiju upravljanja rizicima ili neku drugu strategiju društva.

Uzimajući u obzir da se u kontekstu procjene bitnosti/ozbiljnosti rizika analizira stupanj vjerojatnosti njegova ostvarenja te razina negativnog utjecaja (opasnosti), rizik čija je vjerojatnost ostvarenja iznimno velika i čiji bi utjecaj bio iznimno katastrofalan za ciljeve društva (npr. uzrokovanje stečaja) bio bi prekomjeran rizik. S druge strane, diskutabilno je bi li rizik stečaja čija je vjerojatnost ostvarenja iznimno malena bio prekomjerni rizik. U stručnoj literaturi postoje određene tvrdnje da preuzimanje rizika koje može ugroziti samo postojanje društva nije *per se* povreda pravila dužne pažnje sve dok rizik ima iznimno malu vjerojatnost ostvarenja.[419] „Neki autori čak i ističu da odbor (engl. *board*) ima dužnost preuzimanja rizika koji mogu ugroziti postojanje društva ako je to jedina mogućnost društva da 'preživi', što ide previše daleko (engl. *goes too far*)... jer potiče posebno riskantno ponašanje u blizini insolventnosti".[420]

[418] O rizicima koji su prekomjerni u odnosu na toleranciju prema rizicima koju je odredila uprava i nadzorni odbor vidi u Miller, R. T., Oversight Liability for Risk Management Failures at Financial Firms Southern California Law Review, Vol. 84, 2011., str. 47–123.
[419] Winner, M., *op. cit.* u bilj. 397, str. 20.
[420] *Ibid.*

Kriteriji koji mogu poslužiti za utvrđivanje prekomjernosti rizika, uz strategiju upravljanja rizicima i sklonosti društva preuzimanju rizika, jesu primjerice odnos stupnja vjerojatnosti ostvarenja rizika i razine negativnog utjecaja na društvo te razina prijetnje koja dovodi u pitanje vremensku neograničenost poslovanja (stečaj). Slijedom navedenog, prekomjerni rizici su oni rizici koji su obilježeni iracionalnošću preuzimanja zbog toga što se ne mogu racionalno opravdati u odnosu na *benchmarke* (kriterije) rizika.

Uzimajući u obzir kompleksnost materije, napominje se da predmetni kriteriji nisu zatvoren popis, već će ovisno o konkretnom slučaju trebati uzeti u obzir druge elemente. Primjeri *benchmarka* u ovom radu samo su jedan od mogućih pristupa analizi prekomjernosti rizika.

7.5. Geografski /povijesni/ kulturni kontekst rizika

Razlikovanje primjerenog od prekomjernog rizika provodi se različito u različitim kulturološkim kontekstima. „Lekcije naučene iz prošlog iskustva“ alat su koji oblikuje stav pojedine zemlje, odnosno kulturu određene nacije prema konceptu prekomjernog rizika.[421]

Države svijeta različito percipiraju te gledaju na sklonost preuzimanju rizika. Primjerice, poslovna kultura u Sjedinjenim Američkim Državama tradicionalno je bila povezana s preuzimanjem rizika, a sve s ciljem stjecanja veće dobiti. Naime, rizičniji poslovi, u pravilu, ako se uspješno obave, omogućuju veće zarade. S druge strane, tržište Njemačke (a pogotovo financijski sektori) ima averziju prema rizicima. Tako je primjerice njemački bankarski sektor još od dana hiperinflacije iz 1920. imao otpor prema riziku.[422] Gledajući kulturološki, vidljivo je da je kultura rizika Njemačke različita od one u Sjedinjenim Američkim Državama. Iz toga proizlazi da, osim što trgovačka društva svaka za sebe mogu imati različito poimanje toga što je za njih prekomjeran rizik (ovisno o internim politikama preuzimanja rizika), percepcija prekomjernosti može se razlikovati od države do države.[423]

[421] Kaal, W.; Painter, R., Initial Reflections on an Evolving Standard: Constraints on Risk Taking by Directors and Officers in Germany and the United States, *Seton Hall Law Review*: Vol. 40: Iss. 4, 2010., str. 1450.
[422] *Ibid.*
[423] *Ibid.*, str. 1452.

Pokušaj formiranja univerzalne definicije prevelikog ili prekomjernog rizika koja bi se primjenjivala na sva trgovačka društva, sve vrste rizika i koja bi bila prihvaćena na globalnoj (svjetskoj) razini iznimno je težak pothvat, ako ne i nemoguć. Naime, pojam prekomjernog rizika kontroverzan je pojam koji potiče mnogobrojne debate.[424]

Iako je Njemačka modelirala svoja pravila poslovne prosudbe po uzoru na pravila Sjedinjenih Američkih Država, a Republika Hrvatska preuzela njemački pristup, valja imati na umu da se njemački pristup pravilima poslovne prosudbe, a time i hrvatski pristup, dominantno razlikuju od američkog ponajviše u jednom pogledu. Naime, američki pristup izričito ne sadržava kriterij da uredan i savjestan gospodarstvenik ne smije preuzeti preveliki rizik.[425] Drugim riječima, američki pristup pravilu poslovne prosudbe izričito ne sadržava komponentu ekvivalentnu pretpostavci da ne smije biti riječ o prevelikom riziku.[426]

U kontekstu tvrdnje da zemlje mogu imati različit pristup percepciji rizika, u nastavku se daje pregled stavova SAD-a u vezi s rizicima. Tako je primjerice američki stav da nesposobnost predviđanja budućnosti i pogrešna procjena poslovnog rizika nisu povrede u postupanju članova uprave. [427] Naime, kako je i navedeno, američka kultura sklona je rizicima i ne koristi se pojmom prekomjernog rizika u smislu pretpostavki pravila poslovne procjene. Američka kultura smatra da je rizik inherentan poslovanju društva. Američki pristup razumijevanju ekonomskog i tehnološkog razvoja jest taj da je do njih došlo zbog hrabrog (engl. *bold*) preuzimanja rizika korporativnih inovatora.[428]

S druge strane, njemačka sudska praksa neće zaštititi člana uprave ako je poduzetnička odluka bila povezana s neprimjereno prekomjernim poslovnim rizikom (engl. *business risk was inappropriately excessive*), a što je sudska praksa od 1997. (što znači i prije globalne financijske krize iz 2008.)[429] U kontekstu kreditne i bankarske krize iz 2008. njemački komentatori zaključili su da cit.: „Član uprave ne postupa razumno u okviru pravila poslovne prosudbe ako on ili ona preuzima rizike u ime društva koje ako se ostvare dovode do propasti

[424] *Ibid.*, str. 1438.
[425] *Ibid.*, str. 1461.
[426] *Ibid.*, str. 1465.
[427] *Ibid.*, 1466.
[428] Rosenberg, D., Supplying the Adverb: The Future of Corporate Risk-Taking and the Business Judgment Rule, 2008., dostupno na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1266723 (posljednji pristup 7. ožujka 2024.).
[429] Kaal, W.; Painter, R., *op. cit.* u bilj. 421, str. 1467.

društva (engl. *no manager acts reasonably in terms of the business judgement rule if he or she takes risks on behalf of the corporation that, if realized, result in the demise of the corporation*).

8. ZAKLJUČAK

Neke su neizvjesnosti rizik, iz čega proizlazi da je pojam rizika specijalniji od pojma neizvjesnosti. Naime, rizik je ona neizvjesnost koja je mjerljiva, utječe na postizanje ciljeva (pozitivno i/ili negativno) društva te se njome može upravljati u okviru procesa upravljanja rizicima. Definicije upravljanja rizicima društva pristupaju upravljanju rizicima na različite načine definirajući upravljanje rizicima kao aktivnosti, kulturu, sposobnosti, prakse, procese, ali i kao sveobuhvatne i učinkovite sustave. Organizacija sustava upravljanja rizicima nije nužan dio operativnog ustrojstva poslovanja svih trgovačkih društava u Republici Hrvatskoj. Obveza uspostave sustava upravljanja rizicima tipična je i dominantna karakteristika za bankarski sektor, nebankarski financijski sektor, sektor osiguranja, ali i za infrastrukturu tržišta kapitala. Njemački je zakonodavac, za razliku od hrvatskog pristupa (forma preporuke), obvezu uspostave sustava upravljanja rizicima za dionička društva koja kotiraju na burzi propisao zakonom.

Koncept apetita društva za rizikom, koji je u zakonima i podzakonskim pravnim propisima Republike Hrvatske zastupljen izrazom „sklonost preuzimanju rizika“, obuhvaća rizike koje je društvo spremno preuzeti pri postizanju svojih ciljeva te se definira prema pojedinom riziku. Koncept kapaciteta za rizik, čija je istoznačnica u hrvatskom pravnom sustavu „sposobnost podnošenja rizika“, maksimalna je količina rizika koje je društvo sposobno apsorbirati u svom poslovanju. Profil rizičnosti, koji se smatra jednim od bitnih koncepata upravljanja rizicima, predstavlja sveukupnu izloženost pojedinačnim konkretnim rizicima ili skupini rizika u točno određenom trenutku.

U fokusu je procesnog pristupa definiranju upravljanja rizicima identificiranje onih aktivnosti/faza koje su zajedničke najvećem broju modela upravljanja rizicima. Proces upravljanja rizicima započinje fazom identificiranja rizika. Nakon identifikacije rizika, u okviru procesa upravljanja rizicima, slijedi faza procjene njegove ozbiljnosti koja se provodi uzimajući u obzir vjerojatnosti ostvarenja i jačinu njegova potencijalnog pozitivnog i/ili

negativnog utjecaja. Nakon utvrđenja rizika i procjene njegove ozbiljnosti slijedi faza prioritizacije rizika. Prioritizacija rizika znači odabir onih rizika kojima će se društvo najprije posvetiti na način da će na njih primijeniti odgovarajuće mjere iliti odgovore. Prihvaćanje, izbjegavanje, praćenje, smanjenje i dijeljenje moguće su reakcije odnosno odgovori na rizik. Kontinuiranim praćenjem i revizijom pojedinih elemenata ili cjelokupnog sustava upravljanja rizicima društvo kontinuirano utvrđuje mogućnosti poboljšanja sustava upravljanja rizicima, odnosno sustav napreduje, razvija se i postaje zreliji.

Uz opće modele upravljanja rizicima koji su primjenjivi na upravljanje bilo kojom vrstom rizika (primjerice COSO ERM i ISO 31000:2018) postoje međunarodni standardi, ali i uredbe EU-a (npr. DORA) koja propisuje posebnosti u vezi s upravljanjem pojedinim vrstama rizika. Bez upravljanja rizicima u vezi s projektom i kvalitetom nema uspješna upravljanja projektom/kvalitetom. Neizostavan je dio upravljanja usklađenošću upravljanje rizikom usklađenosti.

Komuniciranje je jedan od ključnih elemenata efikasnog procesa upravljanja rizicima. Osim interne komunikacije o rizicima postoji i eksterna komunikacija. Primjeri eksternog komuniciranja o rizicima i o upravljanju rizicima u praksi su: izvješće poslovodstva, komentari poslovodstva, bilješke uz financijske izvještaje te prospekti javne ponude i/ili uvrštenja vrijednosnih papira. Izvješće poslovodstva, kao sastavni dio godišnjeg izvješća, sadržava opis glavnih rizika kojima je društvo izloženo, naznaku ciljeva i metoda upravljanja financijskim rizikom društva. U određenim slučajevima ono sadržava i nefinancijsko izvješće koje, između ostalog, u kontekstu izvješćivanja o održivosti sadržava opis glavnih rizika za poduzeće povezanih s pitanjima održivosti, uključujući opis glavnih ovisnosti poduzeća kada je riječ o tim pitanjima i način njegova upravljanja tim rizicima. Poslovodstvo društva može u sklopu godišnjeg izvješća na dobrovoljnoj osnovi pružiti dodatne komentare koje smatra relevantnima. U komentarima poslovodstva društvo može iznijeti glavne rizike kojima je izloženo, opisati kako se ti rizici mijenjaju, iznijeti planove i strategije za nošenje s njima i njihovo ublažavanje te navesti učinkovitost strategija upravljanja rizicima. Bilješke uz financijske izvještaje kao dodatni i popratni iskazi sadržavaju informacije o rizicima i upravljanju rizicima. Prospekt vrijednosnih papira, osim što je primjer dokumenta koji sadržava informacije o rizicima, ujedno je i relevantan primjer primjene dobrih praksi i pravila

(smjernica) o načinu na koji valja eksterno komunicirati o rizicima kod obraćanja javnosti tijekom javne ponude i/ili uvrštenja vrijednosnih papira na uređeno tržište. Rizici u vezi s izdavateljem (odnosno rizici društva) koji se navode u prospektu moraju biti specifični za izdavatelja, bitni i potkrijepljeni sadržajem prospekta. Dugački i detaljni opisi politika upravljanja rizicima koji bi mogli ograničiti ili narušiti dojam čitatelja o stvarnom opsegu negativnog utjecaja rizika ili o vjerojatnosti njegova nastanka u toj mjeri da čitatelju više nije jasno postoji li preostali značajan rizik su zabranjeni.

Određene faze procesa upravljanja rizicima poput utvrđivanja, procjene/analize i odgovora na „preveliki rizik“ sastavni su dio donošenja poduzetničkih odluka u kontekstu primjene pravila poslovne prosudbe. Naime, kada uprava društva donosi poduzetničke odluke, one se donose u uvjetima rizika te o njima uprava odlučuje na temelju poduzetničke svrhovitosti. Je li nešto poduzetnički svrhovito, može se promatrati kroz prizmu odnosa između rizika (u smislu opasnosti) te potencijalnih prilika. U donošenju poduzetničkih odluka članovi uprave društva kao uredni i savjesni gospodarstvenici dužni su koristiti se / razmotriti / uzeti u obzir / raspitati se / pribaviti primjerene informacije na temelju kojih smiju razumno pretpostaviti djeluju li za dobrobit društva (svaka poduzetnička odluka mora se temeljiti na dostatnoj činjeničnoj osnovi). Ako član uprave ne može procijeniti rizičnost poduzetničke odluke, dužan je angažirati vanjskog stručnjaka. U slučaju da član uprave ne može procijeniti rizik zbog toga što mora odlučiti u iznimno kratkom roku koji ni na koji način ne omogućuje pripremu i prikupljanje primjerenih informacija, on se mora suzdržati od donošenja poduzetničke odluke. Kriteriji koji mogu poslužiti kao usporedna točka za utvrđivanje prekomjernosti rizika, uz strategiju upravljanja rizicima i sklonosti društva preuzimanju rizika, jesu stupanj vjerojatnosti ostvarenja rizika i razine negativnog utjecaja na društvo te razina prijetnje koja dovodi u pitanje vremensku neograničenost poslovanja (stečaj). Prekomjerni rizici su rizici obilježeni iracionalnošću preuzimanja zbog toga što se ne mogu racionalno opravdati u odnosu na *benchmarke* (točke usporedbe) rizika.