Upravljanje rizicima u gaming industriji na primjeru poduzeća Global Gaming Services d.o.o.

Čičko, Valentina

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka, Faculty of Tourism and Hospitality Management / Sveučilište u Rijeci, Fakultet za menadžment u turizmu i ugostiteljstvu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:191:647173

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni diplomski studij

VALENTINA ČIČKO

Upravljanje rizicima u gaming industriji na primjeru poduzeća Global Gaming Services d.o.o.

Riks Management in the Gaming Industry on the example of Global Gaming Services d.o.o.

Diplomski rad

Opatija, 2024.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni diplomski studij
Održivi razvoj turizma

Upravljanje rizicima u gaming industriji na primjeru poduzeća Global Gaming Services d.o.o.

Riks Management in the Gaming Industry on the example of Global Gaming Services d.o.o.

Diplomski rad

Kolegij:	**Menadžment rizika**	Student:	Valentina Čičko
Mentor:	Prof. dr. sc. **Goran Karanović**	Matični broj:	4020/DO23

Opatija, rujan 2024.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Valentina Čičko	4020/DO23
(ime i prezime studenta)	(matični broj studenta)

Upravljanje rizicima u gaming industriji na primjeru poduzeća Global Gaming Services d.o.o.
(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor diplomskog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog diplomskog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, 18.09.2024.

Potpis studenta

Sažetak

Gaming industrija je jedna od najbrže rastućih industrija na svijetu. Uz ekspanziju tehnologije i sve veću dostupnost interneta, videoigre (kasnije: igre) su postale dostupne široj publici, uključujući različite starosne i društvene grupe. Međutim, uz ovaj rapidan rast dolazi i niz rizika koji mogu ugroziti stabilnost i profitabilnost poduzeća u ovom sektoru. Upravljanje rizicima stoga postaje ključno za održavanje održivog poslovanja i zaštitu korisnika. U gaming industriji je upravljanje rizicima složen proces koji zahtjeva pažljivu strategiju i stalno prilagođavanje. Uz pravilno provođenje, gaming poduzeća mogu ne samo smanjiti potencijalne gubitke, već mogu i izgraditi dugoročno povjerenje korisnika i stabilnost na tržištu. Kroz efikasno upravljanje rizicima, gaming industrija može nastaviti svoj rast i inovaciju, pružajući korisnicima kvalitetne i sigurne proizvode. U ovom radu su teorijski objašnjeni ključni rizici u gaming industriji te načini kako se njima može upravljati. Također, identificirani su ključni rizici u poduzeću Global Gaming Services d.o.o. te je izrađena matrica rizika kao i prijedlozi za upravljanje identificiranim ključnim rizicima.

Ključne riječi: gaming industrija, rizik, upravljanje rizicima

Abstract

The gaming industry is one of the fastest-growing sectors in the world. With the expansion of technology and increasing internet accessibility, video games (hereafter referred to as games) have become available to a broader audience, including various age and social groups. However, this rapid growth also brings a range of risks that can jeopardize the stability and profitability of companies in this sector. Risk management, therefore, becomes crucial for maintaining sustainable business operations and protecting users. In the gaming industry, risk management is a complex process that requires careful strategy and continuous adaptation. When implemented properly, gaming companies can not only reduce potential losses but also build long-term user trust and market stability. Through effective risk management, the gaming industry can continue to grow and innovate, providing users with high-quality and safe products. This paper theoretically explores the key risks in the gaming industry and the methods for managing them. Additionally, the key risks within the company Global Gaming Services d.o.o. have been identified, along with a risk matrix and proposals for managing the identified key risks.

Keywords: gaming industry, risk, risk management

Sadržaj

1. Uvod

Tržište videoigara u svijetu i Europskoj uniji ostvaruje značajne prihode. Samo u "EU u 2022. godini prihodi tržišta videoigara iznosili su 23,48 milijadri €."[1]

Zbog povećanja potražnje posljednjih godina, produkcija videoigara, kako online tako i offline, iz godine u godinu raste. Zbog prirode poslovanja poduzeća koja izrađuju videoigre, te prikupljanja osobnih podataka, kao i brojnih drugih podataka koje prikupljaju, rizici poslovanja tih poduzeća su značajni.

Rast gaming industrije dovodi u središte poslovanja i rizike s kojima se poduzeća u ovoj industriji suočavaju.

1.1. Problem i predmet istraživanja

Poduzeća koja posluju u gaming industriji suočavaju se s brojnim rizicima koji se općenito mogu podijeliti u tehnološke rizike, rizike povezane s cyber[2] sigurnošću, pravne i regulatorne rizike, tržišne rizike, rizike povezane s intelektualnim vlasništvom te operativne rizike. Problem istraživanja je identifikacija utjecaja pojedinih rizika na gaming industriju te mogući načini upravljanja pojedinim skupinama rizika. Predmet istraživanja je analiza ključnih utjecajnih rizika u poduzeću Global Gaming Services d.o.o. i prijedlog poboljšanja upravljanja tim rizicima.

1.2. Svrha i ciljevi istraživanja

Svrha istraživanja je ukazati na važnost identifikacije i strateškog pristupa upravljanju rizicima u gaming industriji. Ciljevi istraživanja su:

- Pojmovno odrediti i utvrditi značajki rizika
- Pojmovno odrediti upravljanje rizicima u gaming industriji

[1] Understanding the Value of a European Video Games Society, Ecorys and KEA, DG Communications Networks, Content and Technology (DG CNECT), European Commission, 2023.

[2] Prvi element u riječima koji označava što vezano uza svijet prividne stvarnosti koji nastaje pomoću kompjutera [*cyberman*] https://hjp.znanje.hr/index.php?show=search

- Identificirati ciljeve upravljanja rizicima u gaming industriji
- Prikazati primjenjivost norme ISO 31000 na gaming industriju
- Analizirati rizike u poduzeću Global Gaming Services d.o.o.
- Predložiti poboljšanje upravljanja rizicima u poduzeću Global Gaming Services d.o.o.

1.3. Metodologija istraživanja

U pisanju teorijskog dijela rada korištene su metode analiza i sinteza, komparativna metoda, indukcija, dedukcija te povijesna metoda. Pomoću ovih metoda definirani su ključni pojmovi te su potom povezani u smislenu cjelinu. Također, uspoređene su pojedine definicije ključnih pojmova. U empirijskom dijelu rada korištena je statistička metoda i metoda intervjuiranja.

1.4. Struktura rada

Rad je podijeljen u pet poglavlja. Uvod u tematiku, predmet, problem, svrhu, ciljeve, metodologiju i strukturu rada nalazi se u prvom poglavlju. Prvo poglavlje također uključuje teorijsku osnovu koja pruža temelj za daljnju analizu istraživačkog problema. Pored toga, prvo poglavlje sadrži detaljan opis korištenih istraživačkih metoda i pristupa, što osigurava jasnu metodološku podlogu.

Opće značajke i definicije rizika objašnjene su u drugom poglavlju. Ovo poglavlje pruža temeljno razumijevanje pojma rizika, s naglaskom na njegovu neizbježnost i složenost u poslovnom svijetu. Također, detaljno razmatra načine na koje poduzeća mogu upravljati rizicima kako bi minimizirala njihove negativne učinke na poslovanje.

Treće poglavlje objašnjava upravljanje rizicima u gaming industriji te primjenjivost norme ISO 31000. U ovom poglavlju detaljno se razmatraju specifični rizici s kojima se suočavaju poduzeća u gaming industriji, uključujući tehnološke, pravne i tržišne rizike. Osim toga, poglavlje pruža uvid u ključne strategije za upravljanje tim rizicima, s posebnim naglaskom na implementaciju i održavanje učinkovitih kontrola kako bi se osiguralo dugoročno uspješno poslovanje.

Primjer rizika i njihovo upravljanje u poduzeću Global Gaming Sevices d.o.o. nalazi se u četvrtom poglavlju. Ovo poglavlje pruža detaljan uvid u specifične izazove s kojima se ovo poduzeće suočava, te načine na koje se rizicima upravlja u kontekstu gaming industrije. Analizirani su različiti aspekti poslovanja, uključujući tehnološke, pravne i tržišne rizike, te su prikazane strategije kojima poduzeće nastoji minimizirati njihove negativne učinke.

Posljednje poglavlje u radu je zaključak. U zaključku se sumiraju ključni aspekti upravljanja rizicima u gaming industriji, ističući važnost proaktivnog pristupa u suočavanju s izazovima. Poseban naglasak stavlja se na integraciju tehnologije i inovativnih alata kao ključnih elemenata u smanjenju rizika i osiguravanju stabilnog poslovanja. Zaključno, ističe se potreba za kontinuiranim praćenjem i prilagođavanjem strategija upravljanja rizicima kako bi se osigurao dugoročni uspjeh i održiv rast u ovoj dinamičnoj industriji.

2. Pojmovno određenje i značajke rizika

„Rizik kao fenomen postoji koliko i čovječanstvo. On je složena, stalna, neizbježna i neizvjesna pojava, koja čini dio našeg života... Kao sinonim riziku pojavljuje se naša neuvjerenost i nemogućnost da 100% predvidimo bilo koji događaj, čak i onaj najizvjesniji. Prirodno je da ljudi nastoje da izbjegnu rizik, ili da ga svedu na najmanju mjeru. Zbog toga se oni prilikom izbora između rizika i moguće koristi odlučuju za njihovu optimalnu kombinaciju (alternativu), pri čemu se podrazumijeva mogućnost mjerenja ili ocjene rizika.“[3] Temeljem navedenoga, u ovom dijelu rada objasnit će se i definirat rizik sa ekonomskog aspekta, ukazati će se na njegove karakteristike u poslovnim procesima te će se iznjeti metode za upravljanje rizicima.

Upravljanje rizicima igra ključnu ulogu u cjelokupnom poslovanju poduzeća, pružajući stratešku prednost u odnosu na konkurenciju. Iako ne zamjenjuje proces poslovnog upravljanja, čini ga transparentnijim i učinkovitijim. S obzirom na to da rizik odražava varijabilnost očekivanog budućeg povrata na uloženi kapital, njegova evaluacija može uključivati primjenu statističkih metoda vjerojatnosti kao potporu u donošenju odluka.

Jakša, Osmanagić-Bedenik i Iliopoulos naglašavaju da upravljanje rizicima ima ključnu ulogu u poslovanju poduzeća, osiguravajući stratešku prednost pred konkurencijom. Ovaj sustav ne zamjenjuje proces poslovnog upravljanja, već ga čini transparentnijim i učinkovitijim. Kroz redovite revizije politika i standarda, sustav upravljanja rizicima ne samo da potvrđuje svoju učinkovitost već i identificira prilike za unapređenje. Učinkovitost sustava mjeri se kroz postizanje željenih rezultata, što uključuje proaktivno prepoznavanje i upravljanje rizicima, uzimajući u obzir kako pozitivne tako i negativne aspekte rizika.[4] Sustav upravljanja rizicima u poduzeću temelji se na četiri ključne komponente:

1. **Proces upravljanja rizicima** – obuhvaća identifikaciju rizika, određivanje prioriteta, razvoj strategija za upravljanje rizicima i nadzor nad provedbom tih strategija.
2. **Organizacijska struktura** – uključuje formiranje odbora za rizike, imenovanje menadžera za rizike, povezivanje s drugim organizacijskim jedinicama te jasno definiranje uloga i odgovornosti.

[3] Radović, D. (2001) Rizik kao fenomen privređivanja i projekt menadžmenta, Montenegrin Journal of Economics, 1(9), str. 144.

[4] Jakša, T., Osmanagić-Bedenik, N., Iliopoulos F. (2008.): „Određivanje učinkovitosti sustava upravljanja rizicima u poduzećima elektroprivrede“, Energija, Vol.57., No.2., str. 156.

3. **Instrumenti, metodologije i sustavi** – odnosi se na alate za identifikaciju i mjerenje rizika, metodologije za izradu strategija te sustave izvještavanja i informacijske tehnologije.
4. **Znanje i vještine** – nužno je da osoblje ima potrebne vještine i znanja za učinkovito upravljanje rizicima.

Sustav upravljanja rizicima temelji se na općim načelima koja uključuju usklađenje strateških i operativnih ciljeva s misijom poduzeća te učinkovito korištenje resursa. Prema integriranim okvirnim načelima Organizacije za borbu protiv lažnih financijskih izvješća (COSO), proces upravljanja rizicima uključuje osam elemenata:

- Unutarnja okolina poduzeća
- Postavljanje ciljeva
- Identifikacija potencijalnih događaja
- Procjena rizika
- Odgovor na rizike
- Kontrolne aktivnosti
- Informiranje i komunikacija
- Nadzor i revizija.

Ranije su poduzeća, kako navode Jakša i Osmanagić-Bedenik, upravljala rizicima na tradicionalan način koji je bio reaktivan i fokusiran uglavnom na financijske rizike, poput kamatnih i valutnih rizika. Menadžeri su često bili skloni izbjegavanju rizika, a rizici su se promatrali pojedinačno, bez integriranog pristupa.[5] Takav pristup nije bio zadovoljavajući u postizanju željenih rezultata.

Današnji pristup upravljanju rizicima usmjeren je na proaktivno upravljanje rizicima, gdje se rizik promatra ne samo kao prijetnja, već i kao prilika. Fokus se proširuje na cijeli poslovni portfelj koji uključuje financijsku imovinu, kupce, zaposlenike i druge resurse poduzeća, poput strategije i brenda.

Moderna teorija portfelja omogućila je da se rizici promatraju holistički na razini poduzeća, čime se omogućuje suočavanje i neutraliziranje rizika. Ovaj cjeloviti pristup omogućuje

[5] Ibid., str. 156.

poduzećima da identificiraju i analiziraju međusobno povezane rizike te da ih učinkovito upravljaju u skladu s promjenama u poslovnom okruženju.

2.1. Definiranje rizika

Pojam rizik označava mogući negativni utjecaj na imovinu ili drugu vrijednost koja proizlazi iz trenutnog ili nekog budućeg događaja. Kada se termin rizik upotrebljava u svakodnevnom govoru, često je sinonim za vjerojatnost gubitka. Vjerojatni gubitak može biti nesiguran u određenim situacijama, dok u drugima postoji veća vjerojatnost za gubitak u grupi više događaja. Svaka ljudska odluka uz sebe veže i određeni rizik. Stoga je razmišljanje o riziku prisutno u svakodnevnim razmišljanjima i određivanjima konkretnih poslovnih aktivnosti. U svakom poslovnom sektoru, uključujući gaming industriju, rizik je neizbježan element poslovnih aktivnosti. Gaming industrija, kao jedna od najbrže rastućih i tehnološki najnaprednijih, suočava se s posebnim izazovima vezanim uz tehnološke promjene, sigurnosne prijetnje i promjenjive preferencije korisnika. Zbog toga je ključno da menadžment poduzeća u ovoj industriji sustavno procjenjuje rizike kako bi mogao pravovremeno poduzeti mjere za njihovo ublažavanje i obavijestiti rukovodeća tijela o potrebnim strategijama. Kvalitetno upravljanje rizicima omogućuje poduzećima predviđanje potencijalnih izazova i zadržavanje konkurentske prednosti u dinamičnom okruženju. Bitno je napomenuti da rizik nije nužno loš. On je zajednička karakteristika za sve poduzeća, što znači da sva poduzeća imaju određenu dozu neizvjesnosti s obzirom na pretpostavke i okruženje u kojem posluju. Iako rizici ne mogu biti potpuno otklonjeni, većina se može predvidjeti, što znači da se njima unaprijed može upravljati.

Osiguranje predstavlja neku vrstu oklade između osiguranika i osiguravatelja, u kojoj se osiguranik kladi da će se događaj dogoditi, a osiguravatelj se kladi da neće. Ako se događaj ne dogodi, osiguranik gubi uplaćenu premiju osiguranja, a ako se događaj dogodi osiguravatelj gubi dogovoreni iznos. Vjerojatnost da će se događaj dogoditi je vrlo mala, tako da uplaćena premija predstavlja gotovo siguran gubitak, međutim većina ljudi nesklona riziku radije prihvaća siguran mali gubitak nego da se izlaže mogućoj katastrofi.

„Rizik se sastoji od tri dijela: rizičnog događaja, njegove vjerojatnosti i utjecaja (štete), a moguće ga je prikazati slijedećom formulom:

Rizik = f (događaja, vjerojatnosti, štete)

gdje šteta može biti kašnjenje projekta, prekoračenje budžeta, smanjen obuhvat ili izvedba projekta“.[6]

Autor Van Well-Stam, D. rizik definira kao događaj koji se može ili ne mora pojaviti. Ako se pojavi, vodi prema većim troškovima, produljenju projekta, nemogućnosti da zadovolji specifične zahtjeve ili norme, zahtjeve za informacijama i organizacijske norme tvrtke.[7] Projektni se rizik razlikuje od poslovnog rizika. Izbor pravog projekta predstavlja poslovni rizik, a izvršenje projektnih ciljeva svih sudionika projekta ukazuje na projektni rizik.

Prema definiciji PMI u PMBOK-u**,** rizik projekta je nesiguran događaj ili stanje koje, ako se pojavi, ima pozitivan ili negativan utjecaj na barem jedan od ciljeva projekta (rokove, troškove, kvalitetu ilo predmet projekta). Rizik može imati jedan ili više uzroka, dok njegova pojava može imati jednu ili više posljedica.[8]

Poslovni rizik karakteriziraju tri osnovne osobine: neizvjesnost, potencijalni gubitak i vremenska komponenta. Neizvjesnost pojave različitih događaja nikad se ne može potpuno otkloniti. Rizik podrazumijeva mogućnost nekog oblika gubitka, pa čak i ako početni gubitak u konačnici može rezultirati dobitkom, rizik se promatra kao gubitak. Za planiranje odgovora na rizik značajna je vremenska komponenta rizika. Ove se komponente razmatraju kao kriterij za određivanje mogućnosti upravljanja rizikom.

Rizik se povećava s povećanjem izloženosti izvorima opasnosti, a smanjuje se učinkovitom zaštitom od njihovih nepovoljnih utjecaja. Da bi se rizicima uspješno upravljalo, potrebno je dobro poznavati osnovne komponente rizika:

- „Događaj – neželjenu situaciju ili slučaj koji bi mogao ugroziti ciljeve poduzeća
- Uzroke – moguće pokretače nastanka rizičnog događaja
- Utjecaj – učinke pojave rizičnog događaja na ciljeve poduzeća.“[9]

„O razini tolerancije na rizik ovisi način upravljanja rizikom. Menadžment poduzeća i drugi donositelji odluka u uvjetima neizvjesnosti i rizika, prema razini osobne tolerancije na

[6] Ibid.
[7] Van Well-Stam, D. i sur. (2004) Project Risk Management, Kogan Page Publishers, United Kingdom, str. 35-36.
[8] Project Management Institute (2004) *A Guide to the Body of Knowledge*, Third Edition, PMI, Pennsylvania, USA.
[9] Ramanathan, C., Narayanan, S. P., Idrus, A. B. (2012) Construction delays causing risks on time and cost - A critical review. Australasian Journal of Construction Economics and Building, 12(1), str. 37–57.

rizik, mogu se podijeliti u osnovne skupine.“[10] U prvoj su oni koji izbjegavaju rizik. Njihova tolerancija na rizik opada s porastom neizvjesnosti. Skloniji su sigurnim rezultatima te će za prihvaćanje rizika tražiti premiju. U drugu se skupinu ubrajaju oni skloniji riziku. Njihova tolerancija na rizik raste s porastom novca koji stavljaju na kocku. Spremni su preuzimati nesigurne poslove i plaćati penale. Treću skupinu čine rizično neutralni menadžeri kojima je tolerancija na rizik linearno zavisna o iznosu na kocki.

„Kako bi upravljanje rizicima bilo uspješno, potrebno je prethodno odabrati odgovarajući model rizika. Pomoću njega se može kvantificirati jačina rizika i usporediti s drugim mogućim rizicima kako bi se donijela odluka o načinu upravljanja rizikom.“[11] Modelom rizika se, također, prepoznaju uzroci njegovog nastanka, a to je preduvjet za učinkovito upravljanje rizicima.

2.2. Značajke i vrste rizika

„Rizike možemo podijeliti na interne i eksterne, a najvažnji interni su:

- „Ljudski resursi/zaposlenici,
- Tehnološki izvori,
- Informatički sustavi,
- Marketinški izvori
- Rizik kvalitete proizvoda.“[12]

Najvažniji eksterni rizici su:

- „Fiskalni izvori,
- Financijski rizici,
- Politički rizici,
- Rizici tržišta radne snage,
- Pravni izvori rizika,

[10] Kerzner, H. (2003) Project Management: A Systems Approach to Planning, Scheduling, and Controlling, Eighth Edition, John Wiley & Sons.
[11] Smith, P. G., Merritt, G. M. (2002) Proactive Risk Management, Productivity Press, SAD, str. 17.
[12] Klemetti, A. (2006) Risk management in construction project networks. Report 2006/2. Laboratory of Industrial Management, Helsinki University of Technology. Helsinki, Finland.

- Tehnološki izvori rizika.“[13]

„Tehnike za identifikaciju rizika mogu biti: brainstorming, upitnici/anketni listovi, poslovne studije koje se bave svakim poslovnim procesom ponaosob i opisuju podjednako unutarnje procese i vanjske čimbenike koji mogu utjecati na te procese, uspoređivanje s najboljom djelatnosti u nekoj dimenziji poslovanja (benchmarking), analiza scenarija, radionice na kojima se procjenjuje rizik, istraživanje incidentnih situacija, provođenje revizija i nadzora, studije opasnosti i operabilnosti Studies).“[14]

Budući da ne postoji jedinstvena podjela rizika, u nastavku (Tablica 1) je prikazana još jedna od mogućih podjela rizika. U tablici koja slijedi nabrojene su i opisane općenite vrste rizika, prema britanskoj Zelenoj knjizi Treasurya.

Tablica 1. Vrste rizika

VRSTA RIZIKA	OPIS RIZIKA
Rizik raspoloživosti	Rizik da će dobivena usluga kvantitetom biti manja od ugovorene
Poslovni rizik	Rizik da organizacija ne može ispuniti svoje poslovne obveze
Rizik građenja	Građevina nije završena na vrijeme, u okviru proračuna i prema ugovorenoj specifikaciji
Rizik pretakanja	Rizik prilagođavanja poslovanja prema potrebi premještanja zaposlenika/klijenata s jednog mjesta na drugo
Rizik zahtjeva	Zahtjev za uslugama ne odgovara planiranoj projektnoj ili procijenjenoj razini usluge
Rizik projektiranja	Projektant ne može isporučiti uslugu po traženim karakteristikama i standardima kvalitete
Ekonomski rizik	Kada je realizacija poslovanja osjetljiva na ekonomske utjecaje
Rizik okoline	Priroda poslovanja ima glavni utjecaj na neposredno okruženje i može postojati velika vjerojatnost od prigovora od strane javnosti
Rizik financiranja	Kada su kašnjenje poslovanja ili promjene obujma poslovanja posljedica neraspoloživosti financijskih sredstava
Pravni rizik	Promjene zakonodavstva povećavaju troškove
Rizik održavanja	Troškovi održavanja imovine premašuju proračun
Rizik korištenja	Troškovi korištenja premašuju proračun, kvaliteta odstupa od standarda
Rizik planiranja	Poslovanje nije uspješno zbog pogrešaka i propusta u planiranju

[13] Ibid.
[14] The Green Book (2003) Appraisal and Evaluation in Central Government, Treasury Guidance, London, str. 82-83.

Politički rizik	Političke promjene koje utječu na poslovanje
Rizik nabave	Nedovoljan kapacitet dobavljača, sporovi između ugovaratelja
Rizik informacija o poslovanju	Kvaliteta prikupljenih relevantnih informacija u fazi pokretanja poslovanja može dovesti do neočekivanih problema
Rizik reputacije	Loša percepcija javnosti I klijenata o poduzeću
Tehnološki rizik	Promjene u tehnologiju mogu dovesti do pružanja usluga koje ne uključuju optimalnu tehnologiju
Rizik obujma	Stvarna usluga varira od predviđene

Izvor: The Green Book (2003) Appraisal and Evaluation in Central Government, Treasury Guidance, London, str. 82-83.

2.3. Uzroci i posljedice rizika

Poslovni rizik povezan je s cjelokupnim poslovanjem poslovnog subjekta. To su stvari koje umanjuju njegovu sposobnost da ulagačima i dionicima pruži odgovarajuće povrate. Na primjer, voditelj poslovanja može donijeti određene odluke koje utječu na dobit poduzeća ili možda neće predvidjeti određene događaje u budućnosti, uzrokujući gubitke ili propast poslovanja. Na poslovni rizik utječe niz različitih čimbenika uključujući:

- „Preferencije potrošača, potražnju i količine prodaje
- Cijena po jedinici i ulazni troškovi
- Konkurencija
- Ukupna ekonomska klima
- Državni propisi.“[15]

Poduzeća su, također, izložena financijskom riziku, riziku likvidnosti, sustavnom riziku, tečajnom riziku i riziku specifičnom za zemlju. Zbog toga je sve važnije minimizirati poslovni rizik. Poduzeće s većom izloženošću poslovnim rizicima trebalo bi odabrati strukturu kapitala s nižim omjerom zaduženosti kako bi osiguralo da može u svakom trenutku ispuniti svoje financijske obveze. Ako prihodi padnu, poduzeće možda neće biti u mogućnosti podmiriti svoje obveze na vrijeme, što može dovesti do bankrota poduzeća. S druge strane, povećanje prihoda omogućava poduzeću veću dobit, čime se osigurava pravovremeno podmirivanje financijskih obveza. „Pozitivni rizici su događaji koji pozitivno utječu na ciljeve poslovanja. Za mnoge ljude

[15] Acquah, C. (2021) The impact of risk of businesses, dostupno na: https://www.researchgate.net/publication/350104154_THE_IMPACT_OF_RISK_ON_BUSINESSES (pristupljeno 17. 5. 2024.)

pojam rizik ima negativne konotacije. Suprotno uobičajenoj percepciji, rizik se ne definira niti kao dobra niti kao loša stvar. Rizik je jednostavno događaj koji ima potencijal utjecati na ciljeve poslovanja.“[16]

„Obično se organizacije usredotočuju na one rizike koji mogu rezultirati negativnim ishodom, kao što je šteta od požara, gubitak ključnog kupca ili pojava novog konkurenta. Međutim, treba uzeti u obzir i nepredvidive događaje, jer bi i oni mogli imati pozitivne ishode, poput vremena boljeg od prognoziranog, snažnijih trendova zadržavanja osoblja ili poboljšanih poreznih stopa. Nadalje, događaji koji su korisni za postizanje jednog cilja mogu u isto vrijeme predstavljati izazov za postizanje drugih ciljeva. Na primjer, lansiranje proizvoda s potražnjom većom od predviđene ima pozitivan učinak na financijsku izvedbu. Međutim, to također može povećati rizik za opskrbni lanac, što bi moglo rezultirati nezadovoljnim kupcima ako tvrtka ne može adekvatno zadovoljiti potražnju na tržištu.“[17]

Neki rizici imaju minimalan utjecaj na poduzeće dok drugi imaju veći utjecaj. Prakse upravljanja rizicima u poduzeću pomažu organizaciji identificirati, odrediti prioritete i usredotočiti se na rizike koji mogu spriječiti stvaranje, očuvanje i realizaciju vrijednosti ili koji mogu narušiti postojeću vrijednost. Međutim, jednako važno, to također pomaže organizaciji u potrazi za potencijalnim prilikama.

Stoga, poduzetnici moraju biti spremni preuzeti rizik kako bi vidjeli rezultate. Često rizik koji preuzimaju je ulaganje ušteđevine u novi posao ili pothvat. Ovi inovativni poduzetnici često mogu stvoriti veliku vrijednost za svoje poslovanje sve dok su njihove nove ideje za robu ili usluge usmjerene na kupca. Oni razumiju da postoji rizik od mogućeg neuspjeha ako se ideje ne pretvore u očekivanja, ali to ne znači da poduzeća neće riskirati.

„Primarni ciljevi organizacije uključuju maksimiziranje bogatstva dioničara, povećanje profita i tržišnog udjela. Rizici mogu utjecati na ove ključne ciljeve. Ako organizacija dopusti da se rizicima ne upravlja, može se suočiti s potencijalnim financijskim, operativnim, pravnim i reputacijskim gubicima.“[18]

Rizici utječu na poslovne aktivnosti, operacije, pa čak i financijsko izvješćivanje. Organizacije moraju prikladno reagirati na rizike prijevare ili sumnje na prijevare utvrđene tijekom ispitivanja financijskog sustava i procesa izvješćivanja. „To je potrebno jer umjetno

[16] Ibid.
[17] Financial Crime Academy (2024) Impact Of Risk On Organizations: Why Manage Risk?, dostupno na: https://financialcrimeacademy.org/impact-of-risk-on-organizations/ (pristupljeno 20. 5. 2024.)
[18] Ibid.

napuhani financijski rezultati ne znače da su organizacijski ciljevi postignuti, a bogatstvo dionika maksimizirano. Stoga su prakse i mjere upravljanja rizicima neophodne za postizanje ciljeva poduzeća. Uprava mora poduzeti odgovarajuće mjere za izgradnju potrebnog modela upravljanja rizikom u obliku politika, procedura i internih kontrola. Upravljanje rizikom također je odgovornost svakog zaposlenika organizacije jer svi rade zajedno u različitim ulogama, sa zajedničkim ciljem postizanja općih strateških ciljeva.“[19]

2.4. Metode za procjenu rizika

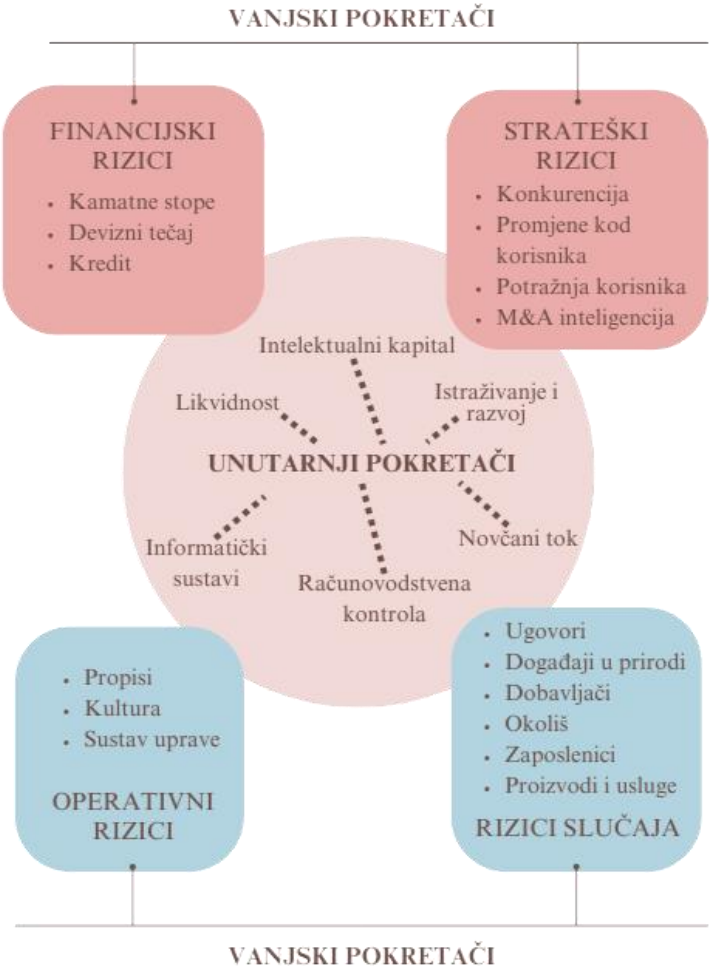
Zadatak analize rizika je prikazivanje svih identificiranih rizika u strukturiranom obliku, odnosno u tabelarnom obliku. Svaki se rizik drugačije odražava na poduzeća. Stoga je svakome od njih potrebno prići iz aspekta pojedinačnog poduzeća u kojem se pojavljuje. Rizici se analiziraju na slijedeće načine:

1) „Kvantitativna analiza rizika – koriste se točne numeričke vrijednosti za izračun identificiranih rizika. Vrijednosti se prikazuju u tabelarnom obliku i izražavaju se u jedinicama primjerenim i dogovorenim za konkretno poslovanje (novčane jedinice, vremenske jedinice, težinske jedinice itd.). Kvantitativnom analizom rizika procjenjuje se kakav će utjecaj identificirani fizici imati na poslovanje. Neke od kvantitativnih metoda analize rizika su:
    - Analiza osjetljivosti,
    - Matematički modeli,
    - Simulacije,
    - Račun vjerojatnosti.“[20]

Kod analize rizika važan je proračun vjerojatnosti neke pojave. “Jedna od tehnika određivanja vjerojatnosti je tehnika zvana Monte Carlo bazirana na eksperimentu i simulaciji. Upotrebljava se u situacijama u kojima bi bilo teško ili nemoguće rješenje u formi jednadžbe“[21]. Ova metoda podrazumijeva svaku tehniku statičkog uzroka kojom se aproksimira rješenje kvantitativnih problema.

[19] Ibid.
[20] Šegudović, H. (2006) Prednosti i nedostaci metoda za kvalitativnu analizu rizika, Infigo, Zagreb.
[21] Ibid.

2) Kvalitativna analiza rizika – ne koriste se apsolutne vrijednosti, nego se upotrebljavaju opisane vrijednosti do kojih se došlo na temelju iskustva, stručnosti i sposobnosti članova poslovnog tima koji sastavljaju kvalitativnu analizu. I kod ove vrste analize vrijednosti se izražavaju numerički, ali one su relativne. „Manjkavost ove vrste analize je subjektivnost koja je kasniji uzrok nepouzdanosti rezultata. Kako bi umanjili nepouzdanost rezultata važno je da analizu sa istim parametrima provede nekoliko kompetentnih osoba kako bi se dobilo na jednoznačnosti“.[22]



Ilustracija 1. Primjeri pokretača ključnih rizika

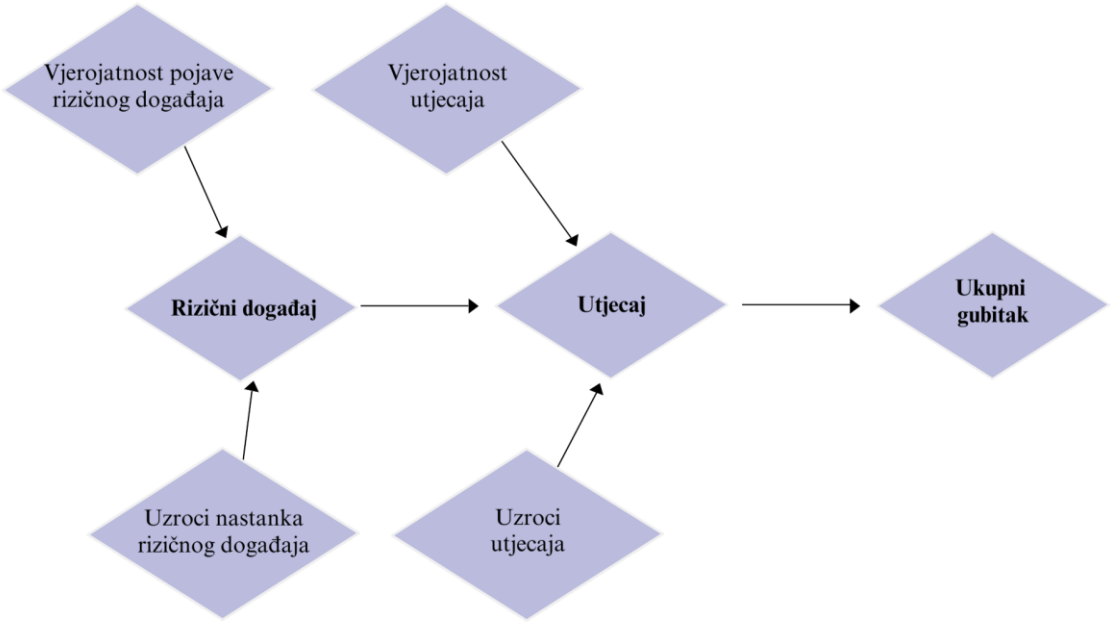
Izvor: Izrada autorice prama Šegudović, H. (2006) Prednosti i nedostaci metoda za kvalitativnu analizu rizika, Infigo, Zagreb, 2006.

[22] Ibid.

Neki od modela rizika su:

1. „Standardni model rizika (Slika 2) - je najčešće korištena tehnika za modeliranje rizika poslovanja. Prednosti ove tehnike su: jednostavna je za razumijevanje, obuhvaća bit poimanja rizika i prikazuje uzročno-posljedične odnose što je značajno za upravljanje rizicima.“[23] Komponente ovog modela su:
   - Rizični događaj – slučajni događaj ili stanje koje uzrokuje gubitak,
   - Uzrok rizičnog događaja – postoji razlog u okolini poduzeća zbog kojeg se vjeruje da bi se rizični događaj mogao dogoditi,
   - Vjerojatnost rizičnog događaja – vjerojatnost da će nastati rizični događaj,
   - Utjecaj rizika – posljedica ili potencijalni gubitak koji bi mogao nastati ako bi se dogodio rizični događaj,
   - Uzroci utjecaja – postoji razlog u okolini poduzeća zbog kojeg se vjeruje da bi se mogao pojaviti određeni utjecaj,
   - Vjerojatnost utjecaja – vjerojatnost da će nastati neki utjecaj od određenog rizičnog događaja,
   - Ukupni gubitak – veličina stvarne vrijednosti gubitka kada se dogodi rizični događaj.

[23] Smith, P.G., Merritt, G. M. (2002), op. cit., str. 19.



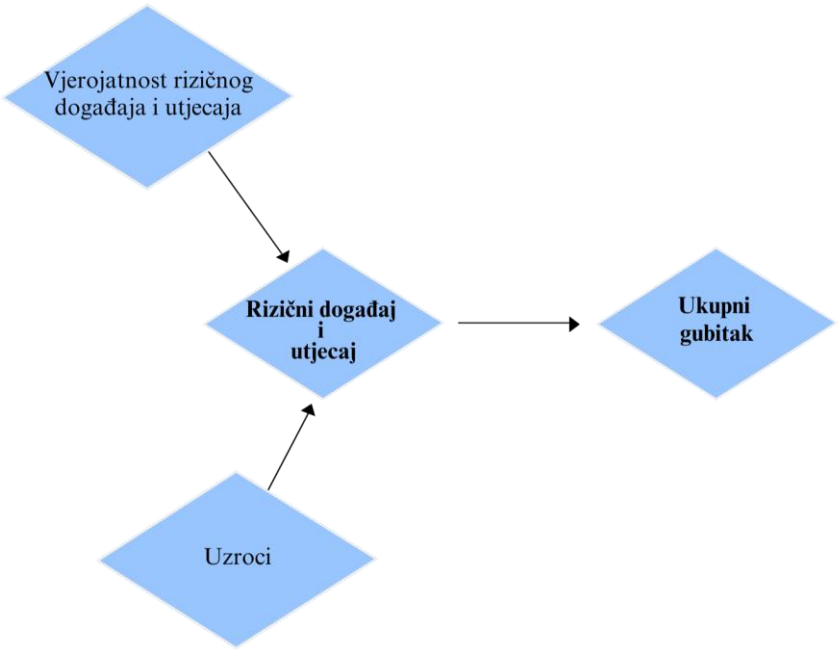
Ilustracija 2. Standardni model rizika

Izvor: Izrada autorice prema Smith, P.G., Merritt, G. M. (2002) *Proactive Risk Management*, Productivity Press, SAD, str. 19.

„Nedostatak ovog modela dolazi do izražaja kada neiskusni korisnici rizični događaj i njegov utjecaj formuliraju preopćenito. Za planiranje odgovora na rizik uzrok rizika je ključna informacija u ovom modelu. Poradi navedenog, ona mora biti što preciznija.“[24]

2. „Jednostavan model rizika (Slika 3) – povezuje rizični događaj i njegov utjecaj u jedinstvenu cjelinu, kao i vjerojatnost nastanka rizičnog događaja i vjerojatnost njegovog utjecaja. Prednost ovog modela je njegova jednostavnost, što ga čini pristupačnijim za korištenje.“ [25]

[24] Ibid.
[25] Ibid., str. 21.



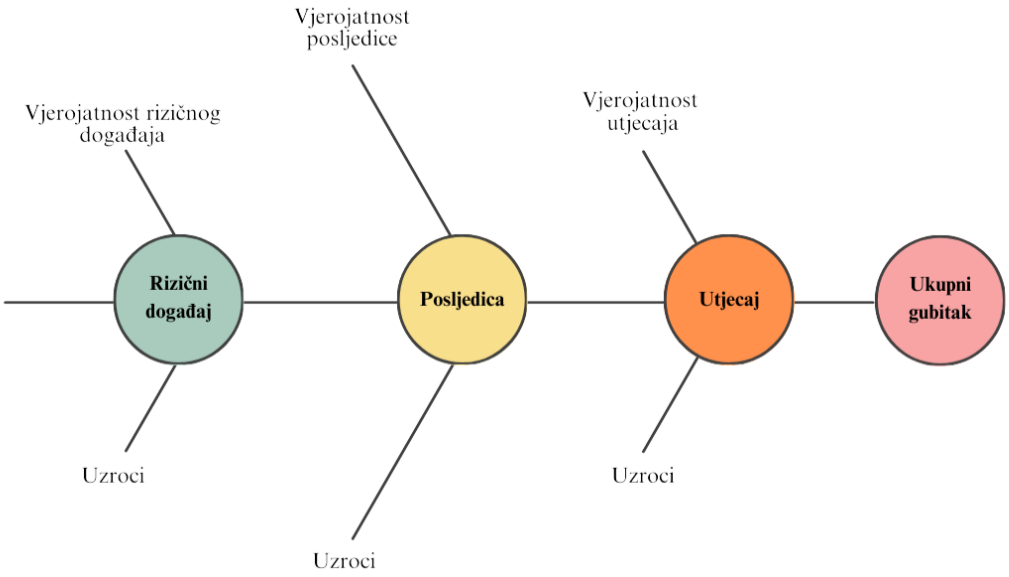
Ilustracija 3. Jednostavni model rizika

Izvor: Izrada autorice prema Smith, P.G., Merritt, G. M. (2002) *Proactive Risk Management*, Productivity Press, SAD, str. 21.

„Osnovna slabost ovog modela je što ne prikazuje potpunu prirodu rizika. U planiranju odgovora na rizik može doći do nedoumica jer se u ovom modelu ne razlikuju uzroci poradi koji bi moglo doći do rizika od uzroka zbog kojih bi ti rizici mogli imati određene posljedice.“[26]

3. Kaskadni model rizika (Slika 4) – ovim se modelom analiziraju rizici kroz više razina. „U najjednostavnijem modelu, koji se sastoji od tri razine, rizični događaj prethodi posljedici koja uzrokuje određeni utjecaj. Model se može sastojati od puno više događaja u kaskadnom slijedu. Gubitak koji otječe na poslovanje je rezultat niza kaskadnih događaja.“[27]

[26] Ibid.
[27] Ibid., str. 22.



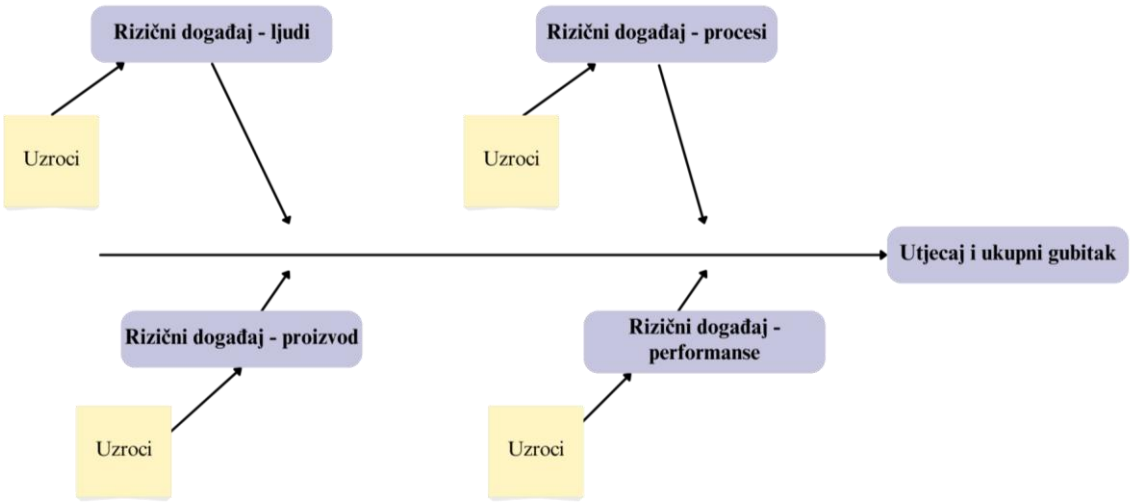
Ilustracija 4. Kaskadni model rizika

Izvor: Izrada autorice prema Smith, P.G., Merritt, G. M. (2002) *Proactive Risk Management*, Productivity Press, SAD, str. 22.

„Ovaj je model koristan za razumijevanje kompleksnih odnosa koji su zaslužni za katastrofične događaje i za analizu rizika za njegovo bolje razumijevanje. Kompleksnost i složeni postupak izračunavanja vjerojatnosti nastanka rizika spadaju među negativne strane ovog modela.“[28]

4. „Ishikawa model rizika (Slika 5) – poznat je i pod nazivom “riblja kost“. Ovaj model može prikazati mnogo uzroka nastanka rizičnih događaja i mnogo rizičnih događaja koji uzrokuju nastanak jednog jedinog utjecaja na gubitak u poslovanju. Rizični se događaji prikazuju u tipičnim kategorijama, primjerice, ljudi, procesi, proizvodi itd. Ovim se modelom na najbolji način može prikazati na koji se način pojavljuju stvarni gubici u poslovanju. Stoga je najprikladniji kao alat za analizu razloga već nastalog rizika.“[29]

[28] Ibid., str. 22.
[29] Ibid., str. 24.



Ilustracija 5. Ishikawa model rizika

Izvor: Izrada autorice prema Smith, P.G., Merritt, G. M. (2002) *Proactive Risk Management*, Productivity Press, SAD, str. 24.

Ishikawa model je vrlo složen, pa se zbog toga manje koristi u procesu planiranja rizika. „Osim toga, podjelom rizičnih događja u kategorije onemogućeno je precizno definiranje rizičnog događaja koji je rezultat interakcije različitih kategorija.“[30]

[30] Ibid., str. 24.

3. Upravljanje rizicima u gaming industriji

Posljednjih godina industrija videoigara značajno je porasla, postavši ključni segment kulturnih i kreativnih industrija. „Globalni prihodi dosegnuli su 179 milijardi eura u 2022. godini, dok je broj igrača dosegao više od 3 milijarde.“[31] Europsko tržište videoigara također je zabilježilo rast, ostvarivši 23,48 milijardi eura prihoda te dosegnuvši oko 220 milijuna korisnika. Iako je europsko tržište stabilno, očekuje se smanjenje udjela u globalnom tržištu „sa 8,7% na 7,3% do 2027. godine, zbog bržeg rasta konkurentskih tržišta izvan Europe.“[32]

Međutim, ova brza ekspanzija donosi i priličan udio rizika i izazove. Jedna od primarnih briga je nesigurnost tržišta. Dok je potražnja za igrama u porastu, predviđanje potrošačkih preferencija i trendova može biti težak zadatak. Nadalje, gaming industrija uvelike se oslanja na tehnološki napredak kako bi igračima pružila impresivna i privlačna iskustva. Međutim, praćenje brzog tempa tehnoloških inovacija može predstavljati značajan izazov. „Od grafike i procesorske snage do virtualne i proširene stvarnosti, programeri igara moraju se stalno prilagođavati i ulagati u najnovije tehnologije kako bi ostali konkurentni. Neuspjeh u tome može rezultirati zastarjelim igrama koje ne uspijevaju privući igrače.“[33]

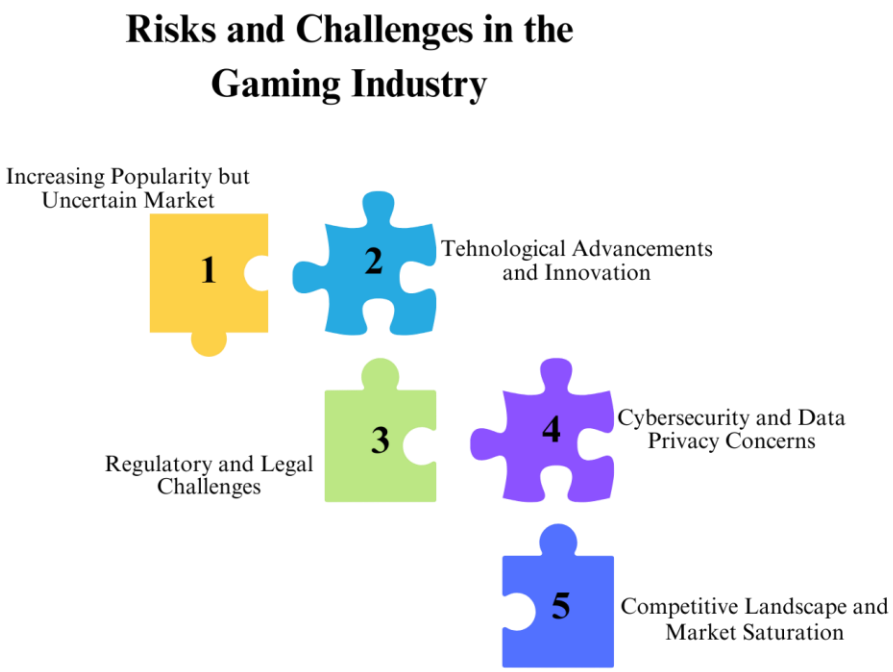
Gaming industrija djeluje unutar složenog regulatornog okvira koji se može značajno razlikovati od zemlje do zemlje. Ovo predstavlja izazov za programere i izdavače igara, budući da se moraju pridržavati raznih pravnih zahtjeva i dobiti licence za objavljivanje svojih igara u različitim regijama. Osim toga, industrija se također suočava s nadzorom u vezi s pitanjima kao što su kutije za plijen, mehanike slične kockanju i dobna ograničenja, što može dovesti do pravnih izazova i štete reputaciji.

Kako se industrija igara nastavlja razvijati, tako rastu i rizici povezani s kibersigurnošću i zaštitom osobnih podataka. „S porastom online igranja i sve većom integracijom društvenih značajki, osobni podaci igrača i financijski detalji u opasnosti su od hakiranja. Programeri igara moraju ulagati u snažne mjere kibernetičke sigurnosti kako bi zaštitili podatke svojih igrača od pokušaja hakiranja i kako bi osigurali sigurno okruženje za igranje. Štoviše, prikupljanje i

[31] Ecorys & KEA (2023.), Understanding the value of a European Video Games Society, Publications Office of the European Union, Luxembourg, dostupno na: https://digital-strategy.ec.europa.eu/en/library/study-european-video-games-sector (pristupljeno 24.08.2024.)
[32] Ibid.
[33] Faster Capital, Risks And Challenges In The Gaming Industry, dostupno na: https://fastercapital.com/topics/risks-and-challenges-in-the-gaming-industry.html (pristupljeno 1.6.2024.)

korištenje osobnih podataka za ciljano oglašavanje i mikrotransakcije izazvalo je zabrinutost oko privatnosti, što je dovelo do regulatornog nadzora i potencijalnih pravnih izazova.“[34]

Industrija igara uključuje brojne programere i izdavače igara koji se natječu za pozornost igrača. Ova zasićenost tržišta predstavlja izazov za nove sudionike i manja poduzeća za igre koja se pokušavaju probiti na tržište. Etablirani brendovi s dobro poznatim franšizama često dominiraju tržištem, što otežava novim poduzećima da steknu prednost.



Ilustracija 6. Rizici u gaming industriji

Izvor: Izrada autorice prema Faster Capital, Risks And Challenges In The Gaming Industry, dostupno na: https://fastercapital.com/topics/risks-and-challenges-in-the-gaming-industry.html (pristupljeno 1.6.2024.)

Iako gaming industrija nudi velike prilike za rast i ulaganja, nije bez rizika i izazova. „Od neizvjesnog tržišta i tehnološkog napretka do regulatornih prepreka i zabrinutosti oko kibernetičke sigurnosti, programeri igara i investitori moraju se pažljivo snaći u ovim preprekama. Održavanjem koraka s trendovima u industriji, poticanjem inovacija i davanjem prioriteta potrebama potrošača, dionici u gaming industriju mogu ublažiti rizike i iskoristiti rastuću potražnju za igrama.“[35] U svjetlu ovih izazova, europska industrija videoigara mora se osloniti na svoje kreativne potencijale i pronaći načine za povećanje konkurentnosti na

[34] Ibid.
[35] Ibid.

globalnom tržištu. „Jasna i usklađena strategija na razini EU-a mogla bi omogućiti sektor videoigara da i dalje bude izvor značajnih ekonomskih, društvenih i kulturnih koristi za Europu.“[36]

3.1. Pojmovno određenje upravljanja rizikom

Upravljanje rizikom je proces mjerenja ili procjenjivanja rizika i razvijanja strategija za upravljanje rizikom. Strategije koje se javljaju na tom području uključuju:

- Prijenos rizika drugoj strani,
- Izbjegavanje rizika ili smanjivanje negativnih utjecaja rizika i prihvaćanje nekih ili svih posljedica rizika.

Kada je riječ o tradicionalnom upravljanju rizikom, ono je usredotočeno na rizik koji proizlazi iz fizičkih ili legalnih slučajeva, primjerice, prirodne katastrofe ili požari, nesreće, smrti, sudske tužbe i sl. Financijsko se upravljanje rizikom usredotočuje na rizik kojim se može upravljati financijskim instrumentima. Kada je riječ o idealnom upravljanju rizikom, koriste se:

1. „Prioritet u kojemu se rizik s najvećim gubitkom i najvećom vjerojatnošću prvi obrađuje,
2. Rizik s manjom vjerojatnošću i manjim gubicima se obrađuje u padajućem redoslijedu.

Kod upravljanja rizikom javljaju se problemi oko određivanja rizika s većom vjerojatnošću i manjim gubicima te rizika s većim gubicima i manjom vjerojatnošću. Problemi se javljaju i prilikom alokacije resursa. Riječ je o ideji oportunitetnih troškova. Resursi koji se troše na upravljanje rizikom mogu biti potrošeni na neku isplativiju aktivnost. Idealno upravljanje rizikom podrazumijeva minimizirane troškove i maksimiziranje smanjivanja negativnih utjecaja rizika.“[37]

Ključ upravljanja rizicima leži u identificiranju faktora rizika povezanih s određenim poduzećem. Nakon toga treba uspostaviti plan upravljanja rizicima poradi minimalizacije vjerojatnosti pojave rizičnog događaja i njegovog negativnog utjecaja na samo poduzeće. Definiranje rizika ovisi o određenim uvjetima i situacijama.

[36] Ibid str. 9
[37] Krakar, Z. (2024) Upravljanje rizicima neusklađenosti, dostupno na: https://www.linkedin.com/pulse/upravljanje-rizicima-neuskla%C4%91enosti-zdravko-krakar/ (pristupljeno 15. 7. 2024.)

„Koraci u procesu upravljanja rizikom su:

1. Određivanje konteksta – određuje se planiranje procesa, grupiranje osnova po kojima će se procijeniti rizik, određivanje i grupiranje ciljeva dioničara i doseg upravljanja rizikom.
2. Identifikacija – nakon uspostavljenog konteksta, korak koji slijedi je identifikacija potencijalnih rizika. Rizik je povezan s događajima čijom realizacijom dolazi do problema. Identifikacija rizika može početi s uzrokom problema ili samim problemom.
3. Procjena – mora se procijeniti kolike gubitke može taj rizik nanijeti te kolika mu je vjerojatnost nastupanja.“[38]

Kada se rizik identificira i procijeni, sve metode za upravljanje rizikom mogu se razvrstati u četiri osnovne strategije: prihvaćanje, reagiranje, eliminacija i prijenos. Nakon što se rizici prepoznaju i svakoj se dodijeli odgovarajuća kvalitativna ocjena, važno je odlučiti hoće li se primijeniti kvantitativna procjena. To podrazumijeva da će rizik biti izražen u brojčanim vrijednostima, umjesto da se procjenjuje kao nizak, srednji ili visok. Kada se analizira skup rizika kako bi se utvrdio onaj s najznačajnijim utjecajem na poslovne aktivnosti, jedan od pristupa za prioritizaciju i kvantifikaciju rizika je dodjeljivanje brojčanih ocjena svakom riziku na sljedeći način:

- „V – vjerojatnost da će se rizik dogoditi,
- U – utjecaj na poduzeće ako se rizik dogodi. Ovo se područje dalje raščlanjuje na UT – utjecaj na trošak; Ur – utjecaj na rok; Urs – utjecaj na radne sate.“[39]

U prvom koraku upravljanja rizicima u gaming industriji bitno je identificirati i procijeniti potencijalne rizike koji mogu utjecati na poslovanje gaming industrije. To podrazumijeva provođenje sveobuhvatne analize rizika, korištenjem kvantitativnih i kvalitativnih metoda, kako bi se procijenila vjerojatnost i učinak različitih scenarija. Uobičajeni rizici koje poduzeća u gaming industriji trebaju uzeti u obzir uključuju kibernetičku sigurnost, prijevaru, usklađenost i probleme s korisnicima. „Rizici kibernetičke sigurnosti uključuju hakiranje, povrede podataka, zlonamjerni softver, napade uskraćivanjem usluge i druge kibernetičke prijetnje koje bi mogle ometati sustave i podatke. Rizici prijevare uključuju krađu identiteta, pranje novca, varanje, tajni dogovor i zlouporabu bonusa. Rizici usklađenosti

[38] Miloš Sprčić, D. i Dvorski Laxković, I. (2023) Upravljanje rizicima – teorijski koncepti i primjena u poslovnoj praksi, Naklada Slap, Zagreb.
[39] Ibid.

uključuju pridržavanje različitih propisa i zakona u različitim državama i na različitim tržištima. Rizici kupaca uključuju ispunjavanje očekivanja kupaca u pogledu kvalitete, raznolikosti i sigurnosti proizvoda i usluga u gaming industriji. Neuspjeh u rješavanju ovih rizika može rezultirati financijskim gubicima, štetom po ugledu, pravnim postupcima, novčanim kaznama i sankcijama.“[40]

Drugi korak u upravljanju rizikom je implementacija i praćenje odgovarajućih kontrola za ublažavanje i upravljanje identificiranim rizicima. To uključuje dizajniranje i provedbu strategija odgovora na rizik, kao što je izbjegavanje, smanjenje, prijenos ili prihvaćanje rizika, te uspostavljanje politika rizika, postupaka i standarda za usmjeravanje aktivnosti upravljanja rizikom. „Poduzeća u gaming industriji moraju usvojiti najbolje prakse i tehnologije za kibernetičku sigurnost, kao što su enkripcija, autentifikacija, vatrozidi, antivirusni programi, sigurnosno kopiranje i oporavak kako bi zaštitile sustave i podatke od neovlaštenog pristupa. Također bi trebale provoditi redovite sigurnosne revizije i testove kako bi otkrile i riješile ranjivosti ili incidente. Kako bi se spriječile prijevare, gaming poduzeća trebaju primijeniti mjere i alate za prevenciju, otkrivanje i odgovor kao što su provjera, šifriranje, praćenje, analitika i izvješćivanje.“[41]

Osim toga, trebale bi educirati osoblje i klijente o rizicima i politikama prijevare. Za gaming poduzeća važno je pratiti i pridržavati se promjenjivih propisa u industriji tako da budu informirana o novim ili revidiranim pravilima ili standardima. One, također, moraju komunicirati s relevantnim tijelima i dionicima kako bi pokazale svoj status usklađenosti i učinak. „Naposljetku, gaming poduzeća moraju pratiti iskustvo korisnika prikupljanjem povratnih informacija o preferencijama i ponašanju kako bi prilagodile proizvode i usluge. Također, moraju komunicirati s kupcima kako bi izgradile povjerenje i lojalnost.“[42]

Treći korak u upravljanju rizicima je poticanje i promicanje kulture rizika u organizacijama u gaming industriji. To znači stvaranje i održavanje svijesti, stava i ponašanja među osobljem, menadžmentom i kupcima koji podržavaju i omogućuju prakse upravljanja rizikom. „Više rukovodstvo i čelnici trebaju postaviti sustav za upravljanje rizikom definiranjem i komuniciranjem vizije, misije i vrijednosti, kao i raspodjelom resursa. Osoblje i

[40] Harris, C. i sur., What are the best risk management practices for the gaming industry?, dostupno na: https://www.linkedin.com/advice/0/what-best-risk-management-practices-gaming-industry-grebe (pristupljeno 20. 6. 2024.)
[41] Ibid.
[42] Ibid.

kupce treba educirati o upravljanju rizicima pružanjem relevantnih informacija, znanja i vještina. Dodatno, osoblje i kupce treba poticati uspostavljanjem pokazatelja učinka, mjera i ciljeva, kao i priznavanjem postignuća“.[43]

3.2. Ciljevi upravljanja rizicima

Jedan od glavnih ciljeva upravljanja rizicima u gaming industriji je osiguranje stablinosti razvojnih projekata. Izbor pokretača igre može imati značajan utjecaj na stabilnost i pouzdanost igre na svim platformama. Pogon za igre softverski je okvir koji pruža osnovne funkcije i alate za stvaranje i pokretanje igara. Neki sustavi za igre dizajnirani su da podržavaju više platformi, kao što su Unity, Unreal Engine ili Godot. „Ovi sustavi mogu pomoći programerima igara uštedjeti vrijeme i resurse dopuštajući im stvaranje jedne verzije igre i izvoz na različite platforme uz minimalne prilagodbe. Međutim, programeri igara također bi trebali biti svjesni ograničenja i kompromisa korištenja međuplatformskog sustava, kao što su problemi s performansama, problemi s kompatibilnošću ili naknade za licenciranje.“[44]

Testiranje i optimiziranje igre za različite platforme ključno je za osiguranje stabilnosti i pouzdanosti. Programeri igrica trebali bi testirati igru na različitim uređajima, operativnim sustavima i hardverskim konfiguracijama te identificirati i popraviti sve greške, kvarove ili padove koji se mogu pojaviti. „Testiranje bi također trebalo pokriti aspekte kao što su korisničko sučelje, metode unosa, grafika, zvuk, mreža i memorija. Optimiziranje igre znači prilagođavanje postavki i značajki igre kako bi odgovarale mogućnostima i specifikacijama svake platforme. Na primjer, programeri igara možda će morati smanjiti razlučivost, broj sličica u sekundi ili kvalitetu teksture igre za uređaje niže klase ili će trebati implementirati prilagodljivo skaliranje, dinamičko osvjetljenje ili kolanje sredstava za bolju izvedbu.“[45]

Svaka platforma ima vlastite smjernice i standarde koje programeri igara trebaju slijediti kako bi osigurali stabilnost i pouzdanost. Ove smjernice i standardi mogu uključivati tehničke zahtjeve, načela dizajna, kriterije osiguranja kvalitete ili procese certifikacije. Na primjer, programeri igara trebali bi slijediti smjernice i standarde platforme za aspekte kao što su

[43] Ibid.
[44] Sharma, S., How can game developers ensure stability and reliability across platforms?, dostupno na: https://www.linkedin.com/advice/1/how-can-game-developers-ensure-stability-reliability-yk0be (pristupljeno 1. 7. 2024.)
[45] Ibid.

veličina zaslona, orijentacija, razlučivost, omjer slike, unos dodirom, unos kontrolera, unos tipkovnicom, unos mišem, ikone, izbornici, dijalozi, obavijesti, dopuštenja, pohrana, sigurnosti ili monetizacije. „Praćenje smjernica i standarda platforme može pomoći razvojnim programerima igara da izbjegnu odbijanje, postupe u skladu s propisima i ispune očekivanja korisnika.[46] Cilj upravljanja rizicima u gaming industriji je i zaštita intelekturalnog vlasništva.

Registracija intelektualnog vlasništva omogućuje gaming poduzećima da zaštite svoje inovativne dizajne i tehnologije od nezakonite upotrebe ili kopiranja od strane drugih poduzeća. Time poduzeća mogu licencirati vlastitu tehnologiju i inovacije te im prodati drugim poduzećima što može biti dodatni izvor prihoda.

Registracija intelektualnog vlasništva važan je dio uspjeha poduzeća za razvoj igara u današnjoj gaming industriji. Pruža pravnu zaštitu patenta, inovacija i tehnologije te pomaže u stvaranju tržišne svijesti i komercijalnom iskorištavanju intelektualnog vlasništva. Postoji mnogo patenata u industriji igara koji se odnose na različite aspekte tehnologije, uređaja i metoda igara. „Primjeri patenata koji se odnose na industriju igara su:

- Patent pokretača igara: mnoga poduzeća za razvoj igara registriraju patente za svoje motore igara, koji su softverske platforme za stvaranje i pokretanje igara.
- Patenti uređaja za igranje: razni uređaji za igranje kao što su konzole, kontroleri i virtualne stvarnosti, također, mogu biti zaštićeni patentom.
- Patenti za metode i procese igre: gaming poduzeća, također, registriraju patente za jedinstvene metode igre, mehanike i procese koji igre čine jedinstvenima i inovativnima.
- Patenti hardvera uređaja za igranje: razne hardverske komponente koje se koriste u uređajima za igranje, kao što su grafički procesori, zvučni sustavi i dodirne podloge, mogu biti zaštićeni patentom.
- Patenti za dizajn igara i sučelja: programeri igara, također, mogu registrirati patente za jedinstvene dizajne igara i korisnička sučelja.“[47]

Upravljanje rizicima u gaming industriji odnosi se i na upravljanje reputacijskim rizicima. To se odnosi se na praksu praćenja, utjecaja i održavanja percepcije i ugleda gaming poduzeća. Uključuje aktivno upravljanje javnim mnijenjem, online reputacijom i prisutnošću brenda te načinom na koji drugi percipiraju subjekt i komuniciraju s njim. Upravljanje

[46] Ibid.
[47] Ibid.

reputacijom ključno je u današnjem digitalnom svijetu, gdje se informacije brzo šire i mogu značajno utjecati na uspjeh gaming poduzeća.

Jedan ključni aspekt strategije upravljanja reputacijom je održavanje pozitivne online prisutnosti. „To uključuje aktivno praćenje i odgovaranje na recenzije, komentare i povratne informacije na raznim internetskim platformama. Također, uključuje stvaranje i promicanje pozitivnog sadržaja, upravljanje računima na društvenim mrežama i brzo i profesionalno rješavanje svih štetnih informacija.“[48]

Još jedan važan aspekt je izgradnja i održavanje snažnih odnosa s kupcima, klijentima i dionicima. Dobar ugled može se održavati pružanjem izvrsne korisničke usluge, pružanjem visokokvalitetnih proizvoda ili usluga te održavanjem transparentnosti i integriteta u poslovnoj praksi. „Proaktivno praćenje brenda ključno je u upravljanju reputacijom. Redovito praćenje spominjanja brenda na mreži, praćenje trendova i novosti u gaming industriji te pravovremeno rješavanje problema ili glasina može spriječiti potencijalnu štetu reputaciji.“[49]

Za učinkovito upravljanje reputacijom važno je razviti jasnu strategiju, postaviti ciljeve te redovito procjenjivati i prilagođavati strategije na temelju povratnih informacija i rezultata. Upravljanje reputacijom je stalan proces koji zahtijeva predanost, brzo djelovanje i posvećenost održavanju pozitivnog imidža u očima dionika. „Predmetno je ključno za uspostavljanje povjerenja, izgradnju kredibiliteta i osiguravanje dugoročnog uspjeha. Gaming poduzeće može zaštititi svoj imidž i učinkovito se kretati digitalnim krajolikom aktivnim upravljanjem i zaštitom vlastitog ugleda.“[50]

Kako bi se zaštitili od kibernetičkih prijetnji, mjere kibernetičke sigurnosti bitne su i za igrače i za poduzeća koja se bave igrama. Ključne mjere kibernetičke sigurnosti koje se mogu primijeniti su:

- „Jake lozinke – gaming poduzeća trebaju poticati igrače da koriste jake, jedinstvene lozinke za svoje račune za igranje. Također je poželjna kombinacija velikih i malih slova, s brojevima i simbolima. Poduzeća moraju postaviti pravila zaporke koja su u skladu s minimalnim zahtjevima složenosti i povremenim promjenama zaporki.

[48] InternetReputation (2023) The Intersection of Online Gaming and Reputation Management, dostupno na: https://www.internetreputation.com/online-gaming-reputation-management/ (pristupljeno 22. 6. 2024.)
[49] Ibid.
[50] Ibid.

- Multifactor Authentication - poduzeća bi trebala omogućiti MFA za račune za igranje tako što će od korisnika zahtijevati dodatnu provjeru, kao što je kod koji se šalje na njihov mobilni uređaj uz lozinku, što dodaje dodatnu razinu sigurnosti.
- Sigurne mrežne veze – gaming poduzeća trebaju osigurati da se igrice igraju isključivo na sigurnim mrežama, na primjer kod kuće ili u bežičnom LAN-u te trebaju izbjegavati korištenje javnih ili nezaštićenih mreža. Tvrtke koje se bave igrama također bi trebale osigurati da su njihovi poslužitelji zaštićeni jakim vatrozidom i redovito ažuriranim sigurnosnim zakrpama.
- Obuka o sigurnosti – gaming poduzeća bi trebala educirati igrače i svoje zaposlenike o najboljim sigurnosnim praksama, kao što je kako prepoznati i izbjeći napade krađe identiteta, važnost čuvanja povjerljivosti podataka o računu prilikom preuzimanja ili korištenja alata za igranje.
- Robusna AntiMalware zaštita – gaming poduzeća bi trebala potaknuti igrače da instaliraju i održavaju najnovije verzije renomiranog sigurnosnog softvera na svojim računalima. Kako bi spriječili širenje zlonamjernog softvera koji bi mogao utjecati na račune igrača ili prekinuti igranje, tvrtke koje se bave igrama također bi trebale poduzeti odgovarajuće mjere na svojim poslužiteljima.
- Redovita ažuriranja softvera - igrači i gaming poduzeća trebaju osigurati da njihove platforme i uređaji za igranje uvijek pokreću najnovije verzije softvera. Kako bi se riješile ranjivosti koje mogu iskoristiti hakeri, obično se uključuju redovito ažurirane sigurnosne zakrpe.“[51]

3.3. Norma za upravljanje rizicima – ISO 31000

ISO 31000 predstavlja niz međunarodnih smjernica i načela koji omogućuju organizacijama sustavan i organiziran način za prepoznavanje, procjenu, tretiranje i praćenje rizika. Prvi put je objavljen 2009. godine, a posljednja revizija izvršena je 2018. godine. „Osnovna svrha ovog

[51] Course, E. R. (2024) Cyber security in the gaming industry, International Journal of Novel Research and Development, 9(3), str. 16-23.

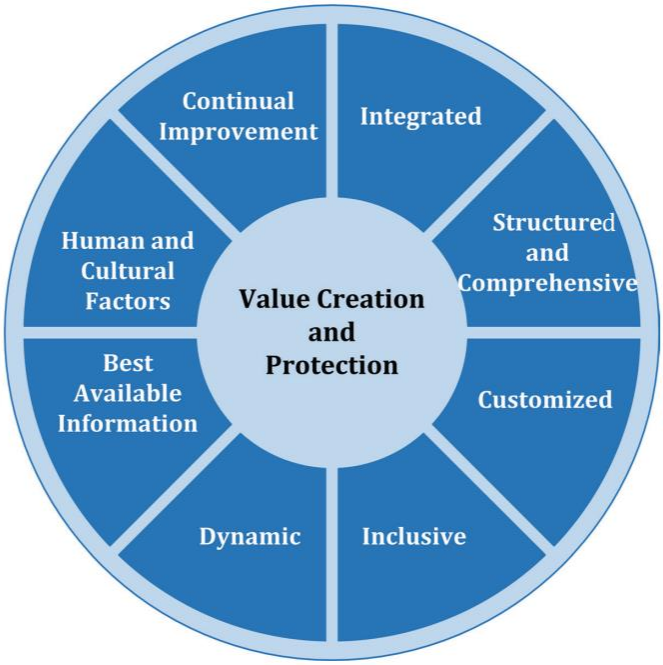
standarda je pružiti podršku organizacijama u zaštiti njihove imovine, postizanju ciljeva i unapređenju procesa donošenja odluka.“[52]

Upravljanje rizikom temelji se na načelima, okviru i procesu. „Ove komponente već postoje u cijelosti ili djelomično unutar gaming poduzeća, međutim, u nekim slučajevima ih treba prilagoditi ili poboljšati kako bi upravljanje rizikom bilo učinkovitije.“[53]

3.3.1. Principi norme ISO 31000

Cilj upravljanja rizicima je očuvanje i povećanje vrijednosti unutar gaming industrije. Kroz poboljšanje poslovnih rezultata, poticanje inovacija i pružanje podrške u ostvarivanju postavljenih ciljeva, upravljanje rizicima ima ključnu ulogu. Principi prikazani na Slici 8 služe kao smjernice za uspješno i učinkovito upravljanje rizikom, naglašavajući njegovu važnost i jasno definirajući njegovu svrhu i ciljeve. „Ovi principi predstavljaju temelj za uspostavu okvira i procesa za upravljanje rizicima u gaming industriji, a njihova primjena trebala bi pomoći poduzećima u suočavanju s neizvjesnostima koje mogu utjecati na ostvarenje njihovih ciljeva.“[54]

[52] GlobalSuite (2023) What is ISO 31000 standard and what is its purpose? Discover the importance of risk management in your organization, dostupno na: https://www.globalsuitesolutions.com/what-is-iso-31000-standard-and-what-is-its-purpose/ (pristupljeno 5. 7. 2024.)
[53] hahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12. 6. 2024.)
[54] Ibid.



Ilustracija 7. Principi

Izvor: Shahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12.6.2024.)

Prema International Organization for Standardization (2018), učinkovito upravljanje rizicima podrazumijeva sljedeće ključne elemente:

- Upravljanje rizicima mora biti integrirano u sve organizacijske aktivnosti, postajući neizostavan dio svakodnevnog poslovanja.
- Strukturiran i sveobuhvatan pristup osigurava dosljedne i usporedive rezultate u upravljanju rizicima.
- Okviri i procesi upravljanja rizicima trebaju biti prilagođeni specifičnom vanjskom i unutarnjem kontekstu organizacije te povezani s njezinim ciljevima.
- Uključivanje dionika na odgovarajući i pravovremen način omogućava uvažavanje njihovih znanja, stavova i percepcija, čime se poboljšava svijest i kvalitetnije upravljanje rizicima.
- Rizici se mogu pojaviti, promijeniti ili nestati s promjenom organizacijskog okruženja, stoga je važno pravovremeno predvidjeti, identificirati, potvrditi i reagirati na te promjene.

- Odluke o upravljanju rizicima oslanjaju se na povijesne, trenutne i buduće informacije, uzimajući u obzir ograničenja i neizvjesnosti povezanih s tim podacima. Informacije moraju biti jasne, pravovremene i dostupne dionicima.
- Ljudsko ponašanje i organizacijska kultura značajno utječu na svaki aspekt upravljanja rizicima, na svim razinama i u svim fazama.
- Kontinuirano unaprjeđivanje upravljanja rizicima temelji se na iskustvima i učenju kroz praksu.[55]

3.3.2. Okvir norme ISO 31000

Prema Gillisu (2024), osnovna svrha okvira za upravljanje rizikom je osigurati da organizacija uspješno uklopi upravljanje rizicima u svoje ključne aktivnosti i funkcije. Učinkovitost ovog procesa u velikoj mjeri ovisi o tome koliko je upravljanje rizikom integrirano u cjelokupno poslovanje i donošenje odluka unutar organizacije. Ovaj proces zahtijeva aktivnu podršku dionika, posebice vrhovnog rukovodstva u gaming industriji. Razvoj takvog okvira uključuje faze integracije, dizajna, implementacije, procjene i stalnog unaprjeđenja upravljanja rizicima na razini cijele organizacije. Na slici 9 prikazane su glavne komponente ovog okvira.[56]

[55] Shahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12.6.2024.)
[56] Gillis, A. S., ISO 31000 Risk Management, dostupno na: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management (pristupljeno 12.6.2024.)

Ilustracija 8. Komponente okvira

Izvor: Shahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12.6.2024.)

Organizacija bi trebala procijeniti svoje postojeće prakse i procese upravljanja rizikom, procijeniti sve nedostatke i riješiti te nedostatke unutar okvira. Komponente okvira i način na koji rade zajedno trebaju biti prilagođeni potrebama gaming poduzeća. Najviše rukovodstvo i nadzorna tijela trebaju osigurati da je upravljanje rizikom integrirano u sve organizacijske aktivnosti i trebaju odražavati predanost:

- „prilagođavanjem i implementacijom svih komponenti okvira
- davanje izjave ili politike kojom se uspostavlja pristup, plan ili postupak upravljanja rizikom
- osiguranje da su potrebni resursi dodijeljeni upravljanju rizikom
- dodjeljivanje ovlasti i odgovornosti na odgovarajućim razinama unutar organizacije.

To će pomoći organizaciji da:

- uskladi upravljanje rizikom sa svojim ciljevima, strategijom i kulturom
- prepozna i ispuni sve obveze
- utvrdi količinu i vrstu rizika koji se mora uzeti u obzir za usmjeravanje razvoja kriterija rizika, osiguravajući da su oni priopćeni organizaciji i njezinim dionicima

- prenese vrijednost upravljanja rizikom organizaciji i njezinim dionicima
- promiče sustavno praćenje rizika
- osigura da okvir upravljanja rizikom ostane primjeren kontekstu organizacije.“[57]

Prema International Organization for Standardization (2018), uspješna integracija upravljanja rizicima temelji se na detaljnom razumijevanju struktura i specifičnog konteksta organizacije. Te strukture variraju u skladu s namjenom, ciljevima i složenošću svakog gaming poduzeća. Upravljanje rizicima mora biti prisutno u svim dijelovima organizacijske strukture, gdje svaki pojedinac snosi određeni dio odgovornosti za ovaj proces. Upravljanje oblikuje smjer organizacije, odnose unutar i izvan nje, kao i potrebne procese, prakse i pravila koja omogućuju ostvarivanje ciljeva. Upravljačke strukture pretvaraju ovaj smjer u strategije i povezane ciljeve, što je ključno za postizanje održivog učinka i dugoročne stabilnosti. Ključni aspekti uključuju dodjelu odgovornosti za upravljanje rizicima i definiranje nadzornih uloga unutar organizacije. Integracija upravljanja rizicima nije jednokratan zadatak, već kontinuirani proces koji se mora prilagoditi specifičnim potrebama i kulturi gaming poduzeća. Upravljanje rizicima mora biti neodvojivi dio organizacijske svrhe, vođenja, strategije i operacija, a ne zasebna funkcija.[58]

Prilikom dizajniranja okvira za upravljanje rizikom gaming poduzeće treba ispitati i razumjeti svoj vanjski i unutarnji kontekst. Ispitivanje vanjskog konteksta organizacije uključuje:

- „društvene, kulturne, političke, pravne, regulatorne, financijske, tehnološke, i ekonomske čimbenike, bilo međunarodne, nacionalne, regionalne ili lokalne
- ključne pokretače i trendove koji utječu na ciljeve organizacije
- odnose, percepcije, vrijednosti, potrebe i očekivanja vanjskih dionika
- ugovorne odnose i obveze
- složenost mreža i ovisnosti.“[59]

Ispitivanje unutarnjeg konteksta gaming poduzeća uključuje:

- „viziju, misiju i vrijednosti
- upravljanje, organizacijsku strukturu, uloge i odgovornosti
- strategiju, ciljeve i politike
- kulture organizacije

[57] Shahr Development (2018), op. citr.
[58] Ibid.
[59] Ibid.

- standarde, smjernice i modele koje je usvojila organizacija
- sposobnosti, shvaćene u smislu resursa i znanja (npr. kapital, vrijeme, ljudi, intelektualno vlasništvo, procesi, sustavi i tehnologije)
- podatke, informacijske sustave i tokove informacija
- odnose s internim dionicima, uzimajući u obzir njihove percepcije i vrijednosti
- ugovorne odnose i obveze
- međuovisnosti i međupovezanosti.“[60]

Najviše rukovodstvo i nadzorna tijela trebaju pokazati i artikulirati svoju stalnu predanost upravljanju rizikom putem politike, izjave ili drugih oblika koji jasno prenose ciljeve organizacije i predanost upravljanju rizikom. Obveza bi trebala uključivati:

- „svrhu organizacije za upravljanje rizikom i veze s njezinim ciljevima i drugim politikama
- jačanje potrebe za integracijom upravljanja rizikom u cjelokupnu kulturu organizacije
- uvođenje integracije upravljanja rizicima u osnovne poslovne aktivnosti i donošenje odluka
- ovlasti i odgovornosti
- stavljanje na raspolaganje potrebnih resursa
- način na koji se rješavaju sukobljeni ciljevi
- mjerenje i izvješćivanje unutar pokazatelja uspješnosti organizacije.“[61]

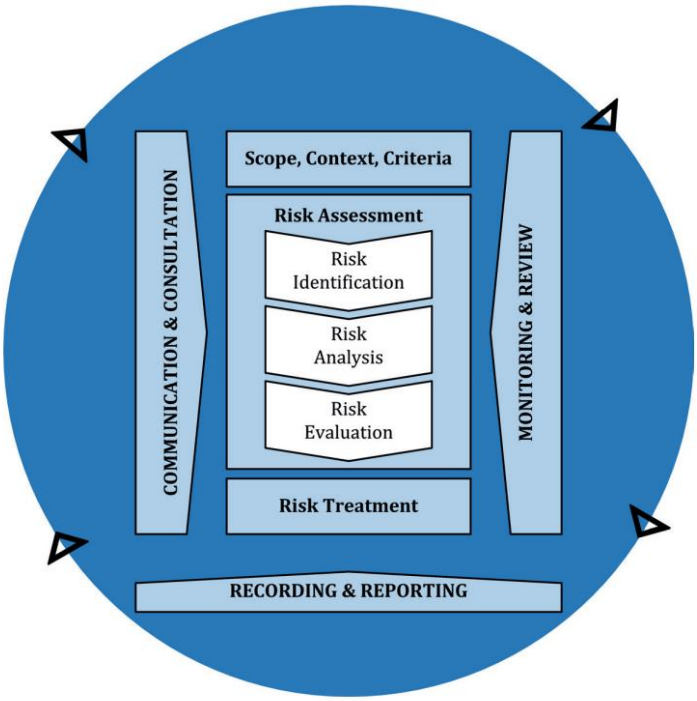
Gaming poduzeće bi trebalo implementirati okvir upravljanja rizikom:

- „razvojem odgovarajućeg plana uključujući vrijeme i resurse
- utvrđivanjem gdje, kada i kako se donose različite vrste odluka u cijeloj organizaciji i tko ih donosi
- izmjenom primjenjivih procesa donošenja odluka prema potrebi
- osiguravanjem da se aranžmani organizacije za upravljanje rizikom jasno razumiju i prakticiraju.“[62]

[60] Ibid.
[61] Ibid.
[62] Ibid.

3.3.3. Proces norme ISO 31000

Proces upravljanja rizikom uključuje sustavnu primjenu politika, postupaka i praksi na aktivnosti komuniciranja i savjetovanja, uspostavljanja konteksta i procjene, tretiranja, praćenja, pregleda, bilježenja i izvješćivanja o riziku. Ovaj proces je ilustriran na Slici 10.



Ilustracija 9. Proces

Izvor: Shahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12.6.2024.)

Prema Institute of Risk Managementu (2018), proces upravljanja rizikom trebao bi biti ključni dio upravljačkih aktivnosti i donošenja odluka unutar gaming poduzeća, te integriran u njegove strukture, operacije i procese. Ovaj proces može biti primijenjen na različitim razinama, uključujući stratešku, operativnu, programsku ili projektnu razinu. Postoji mogućnost različitih primjena unutar organizacije, koje su prilagođene ciljevima i specifičnim vanjskim i unutarnjim uvjetima. Uz to, treba uzeti u obzir promjenjivu prirodu ljudskog ponašanja i organizacijske kulture tijekom cijelog procesa upravljanja rizicima. Iako se često prikazuje kao

linearan proces, upravljanje rizicima je zapravo iterativno u praksi, što znači da se kontinuirano ponavlja i prilagođava novim okolnostima.[63]

Svrha komunikacije i savjetovanja je omogućiti relevantnim dionicima da razumiju rizike, temelje na kojima se donose odluke te razloge zbog kojih su određene radnje nužne. Komunikacija ima za cilj podići svijest i razumijevanje rizika, dok konzultacije uključuju prikupljanje povratnih informacija i informacija koje podržavaju proces donošenja odluka. Uska koordinacija između komunikacije i savjetovanja trebala bi osigurati razmjenu informacija koja je pravovremena, točna, relevantna, jasna i pouzdana, uz poštivanje povjerljivosti, integriteta informacija i prava na privatnost. Komunikacija i savjetovanje s vanjskim i unutarnjim dionicima trebali bi se odvijati tijekom svih faza procesa upravljanja rizicima. Njihova glavna svrha je:

- „spojiti različita područja stručnosti za svaki korak procesa upravljanja rizikom
- osigurati da se različita gledišta na odgovarajući način uzmu u obzir pri definiranju kriterija rizika i pri ocjenjivanju rizika
- pružiti dovoljno informacija za olakšavanje nadzora rizika i donošenja odluka
- izgraditi osjećaj uključenosti i vlasništva među onima koji su pogođeni rizikom.“[64]

Svrha definiranja opsega, konteksta i kriterija je prilagoditi proces upravljanja rizicima kako bi omogućio učinkovitu procjenu i tretman rizika. To podrazumijeva jasno određivanje opsega procesa, kao i razumijevanje vanjskih i unutarnjih faktora koji utječu na organizaciju. Gaming poduzeće mora precizno definirati opseg svojih aktivnosti vezanih uz upravljanje rizicima. Budući da se ovaj proces može primijeniti na različitim razinama, poput strateške, operativne, programske, projektne ili druge, ključno je imati jasan uvid u područje koje se razmatra, kao i ciljeve koje treba postići te njihovu povezanost s organizacijskim ciljevima. Prilikom planiranja pristupa važno je razmotriti:

- „ciljeve i odluke koje je potrebno donijeti
- ishode koji se očekuju od koraka koje treba poduzeti u procesu
- vrijeme, mjesto, posebna uključivanja i isključenja
- odgovarajuće alate i tehnike za procjenu rizika

[63] IRM (2018) A Risk Practitioners Guide to ISO 31000: 2018, dostupno na: https://www.demarcheiso17025.com/document/A%20Risk%20Practitioners%20Guide%20to%20ISO%2031000%20%96%202018.pdf (pristupljeno 2.7.2024.)
[64] Ibid.

- potrebne resurse, odgovornosti i evidencije koje treba voditi
- odnose s drugim projektima, procesima i aktivnostima.“[65]

Procjena rizika obuhvaća cijeli postupak identifikacije, analize i procjene rizika. Taj proces treba biti sustavan, ponavljajući i suradnički, uz korištenje stručnosti i mišljenja svih relevantnih dionika. Važno je osloniti se na najkvalitetnije dostupne informacije, uz provođenje dodatnih istraživanja po potrebi. Glavni cilj tretmana rizika je odabrati i primijeniti odgovarajuće mjere za njihovo rješavanje. Tretman rizika provodi se kroz iterativni postupak koji uključuje:

- „formuliranja i odabira opcija tretmana rizika
- planiranje i provedbu tretmana rizika
- procjenu učinkovitosti tog tretmana
- odlučivanje je li preostali rizik prihvatljiv
- ako nije prihvatljivo, daljnje mjere.“[66]

Svrha nadzora i evaluacije je osigurati i unaprijediti kvalitetu i učinkovitost dizajna, implementacije i rezultata procesa. Kontinuirano praćenje te periodično ocjenjivanje procesa upravljanja rizicima i njegovih rezultata trebali bi biti integrirani u planiranje procesa upravljanja rizicima, s jasno definiranim odgovornostima. Praćenje i evaluacija trebaju biti prisutni u svim fazama procesa, uključujući planiranje, prikupljanje i analizu podataka, bilježenje rezultata te pružanje povratnih informacija. Dobiveni rezultati nadzora i pregleda trebali bi se koristiti kao dio aktivnosti organizacije vezanih uz upravljanje učinkom, mjerenje i izvještavanje.

Proces upravljanja rizikom i njegovi ishodi trebaju biti dokumentirani i o njima treba izvješćivati putem odgovarajućih mehanizama. Bilježenje i izvješćivanje ima za cilj:

- „priopćiti aktivnosti upravljanja rizikom i rezultate u cijeloj organizaciji
- pružiti informacije za donošenje odluka
- poboljšati aktivnosti upravljanja rizicima
- pomoći u interakciji s dionicima, uključujući one s odgovornošću za aktivnosti upravljanja rizikom.“[67]

[65] Ibid.
[66] Ibid.
[67] Ibid.

3.4. Važnost upravljanja rizikom

Sigurnosna usklađenost je proces kojim se osigurava da se gaming poduzeća pridržavaju industrijskih standarda i propisa kada je u pitanju zaštita podataka njihovih klijenata. To uključuje osiguravanje sigurnosti njihovih sustava, korištenje najnovijih sigurnosnih protokola i pridržavanje najboljih praksi u vezi s pohranjivanjem i zaštitom podataka.

Prema Bhattiju (2023), dva ključna standarda u sigurnosnoj usklađenosti su ISO 27001 i PCI-DSS. ISO 27001 predstavlja sustav za upravljanje informacijskom sigurnošću, koji postavlja smjernice za identifikaciju, praćenje i unapređenje sigurnosnih rizika. S druge strane, PCI-DSS (Standard sigurnosti podataka industrije platnih kartica) postavljen je od strane Vijeća za sigurnosne standarde industrije platnih kartica i odnosi se na tvrtke koje posluju s kreditnim, prepaid i debitnim karticama, bankomat karticama, POS uređajima i e-novčanicima. Primarni cilj PCI-DSS-a je smanjenje rizika od prijevara kroz kontrolu i zaštitu podataka o vlasnicima kartica.[68]

Sigurnosna usklađenost prema Bhattiju (2023), igra ključnu ulogu u zaštiti podataka igrača od neovlaštenog pristupa, kao i u osiguravanju da gaming poduzeća poduzimaju odgovarajuće mjere za očuvanje sigurnosti svojih sustava. Nedostatak usklađenosti s propisima može dovesti do sigurnosnih proboja, što može rezultirati financijskim gubicima i narušavanjem reputacije tvrtke. Kako bi osigurala usklađenost, gaming poduzeća trebaju prvo procijeniti svoje postojeće sigurnosne protokole te identificirati područja koja zahtijevaju unaprjeđenje. Na temelju toga, potrebno je razviti sigurnosnu politiku koja detaljno opisuje korake za postizanje usklađenosti. Ova politika trebala bi uključivati mjere poput šifriranja podataka, primjene dvofaktorske autentifikacije i redovitog ažuriranja softverskih sustava. Usklađivanje s propisima donosi brojne prednosti za gaming poduzeća, uključujući povećanje povjerenja korisnika, bolju sigurnost i smanjenje rizika od povreda podataka. Također, doprinosi jačanju lojalnosti kupaca i poboljšanju korisničke usluge, dok pozitivno utječe na javnu percepciju brenda, povećavajući povjerenje i vjernost korisnika. Kako bi učinkovito zaštitila podatke igrača, gaming poduzeća trebaju primjenjivati snažne metode šifriranja, redovito ažurirati softver i koristiti dvofaktorsku autentifikaciju. Uz to, sustavi trebaju biti

[68] Bhatti, K. (2023) The Importance of Security Compliance in the Gaming Industry, dostupno na: https://www.linkedin.com/pulse/importance-security-compliance-gaming-industry-kaushik-bhatti-/ (pristupljeno 3.7.2024.)

kontinuirano nadzirani, a poduzeća moraju imati spreman plan za odgovor na eventualne sigurnosne incidente.[69]

[69] Ibid.

4. Analiza upravljanja rizicima na primjeru poduzeća Global Gaming Services d.o.o.

U ovom poglavlju prikazani su osnovni podaci o poduzeću Global Gaming Services d.o.o., zajedno s analizom čimbenika i vrsta rizika s kojima se ovo poduzeće suočava, kao i utjecajem tih rizika na poslovanje. Analiza je provedena korištenjem metode intervjua s menadžmentom svih odjela unutar poduzeća, čime su prikupljene ključne informacije iz različitih perspektiva unutar organizacije.

Rezultati intervjua omogućili su detaljnu identifikaciju i procjenu rizika u različitim segmentima poslovanja, uključujući tehničke, operativne, financijske i pravne rizike. Na temelju prikupljenih podataka izrađene su preporuke za unapređenje sustava upravljanja rizicima u poduzeću, koje će se implementirati s ciljem smanjenja potencijalnih negativnih učinaka na poslovanje i osiguranja dugoročne stabilnosti i uspjeha poduzeća.

4.1. Opći podaci i poslovanje poduzeća Global Gaming Services d.o.o.

Global Gaming Services d.o.o. je malo poduzeće koje posluje kao društvo s ograničenom odgovornošću (d.o.o.). Poduzeće posluje u skladu s odredbama Zakona o trgovačkim društvima. Tablica 1 prikazuje opće informacije o poduzeću Global Gaming Services d.o.o.

Tablica 1. Opći podaci o poduzeću Global Gaming Services d.o.o.

Global Gaming Services d.o.o.
OIB: 54073250643
Ulica i kućni broj: Strmec Stubički 124
Općina/grad: Stubičke Toplice
Poštanski broj: 49240
Država: Republika Hrvatska
Internetska stranica: https://gameboost.com/
Naziv registracijskog tijela: Trgovački sud u Zagrebu
Datum upisa u matični registar: 28.02.2022.
Registarski broj: 081421549
Osnivači/članovi društva:

- Kristijan Salijević, Strmec Stubički, Strmec Stubički 124, član društva
- Fil Rouge Capital, Croatia Partners SCSp, Luksemburg, Côte D'eich 1, član društva
- FeelsGood Capital Partners društvo s ograničenom odgovornošću za upravljanje alternativnim investicijskim fondovima, Zagreb, Jurišićeva ulica 3, član društva

Izvor: Izrada autora

Vizija poduzeća Global Gaming Services d.o.o. je postati globalno relevantno poduzeće s izrazitom namjerom širenja na međunarodno tržište, koje postavlja nove standarde izvrsnosti u svim područjima svoga djelovanja, odnosno na području rada u gaming industriji.

Misija poduzeća Global Gaming Servcies d.o.o. je omogućiti sigurne, cjenovno pristupačne gaming usluge za klijente u cijelom svijetu te pružiti optimalni softver i web stranicu za potrebe klijenata na globalnoj razini.

Dugoročni cilj poduzeća Global Gaming Services d.o.o. je postati poznato i vodeće ime na globalnom tržištu za gaming usluge i esports. Za pet do deset godina poduzeće se vidi s barem 50 zaposlenika i primjerenim poslovnim prostorom u svojem vlasništvu.

Trenutno u poduzeću ima 27 stalno zaposlenih radnika, a predviđa se da će se taj broj povećati do kraja godine. Uz stalne zaposlenike, poduzeće surađuje s više od 500 freelancera iz cijelog svijeta, koji putem platforme GameBoost pružaju online digitalne usluge i online digitalne proizvode. Određene poslovne funkcije obavljaju se putem vanjskih suradnika; primjerice, računovodstvene usluge su povjerene vanjskom knjigovodstvenom servisu, dok se pravna podrška pruža kroz eksterno pravno savjetovanje. Također, marketinške aktivnosti su djelomično povjerene vanjskoj marketinškoj agenciji s kojom poduzeće surađuje.

Poduzeće posluje kroz platformu GameBoost (https://gameboost.com/), koja djeluje kao posrednik između korisnika (kupaca) i pružatelja usluga u svijetu online igara. Platforma osigurava sigurnost za sve uključene strane i podržava niz popularnih igara, uključujući League of Legends, Valorant, Overwatch 2, LoL: Wild Rift, World of Warcraft te mnoge druge. Poduzeće trenutno posluje na globalnom tržištu, na kojem se namjerava i zadržati, uz kontinuirano povećanje broja usluga, ali i unapređenje kvalitete. Tržište poduzeća je tržište gaming usluga, što su zapravo online digitalne usluge. Ovo tržište je u svijetu još uvijek jako novo i nerazvijeno te kao takvo daje mogućnost širenja već postojećim i novim poduzećima.

Iako poduzeće trenutno ima ured (sjedište) samo u Republici Hrvatskoj, cilj je otvaranje novih ureda u Sjedinjenim Američkim Državama, Njemačkoj i drugim ključnim tržištima.

Očekivani rast poslovanja kroz godine, s izrazito realnim pristupom, kreće se do cca 1 milijun eura mjesečno, odnosno do iznosa od cca 12 milijuna eura godišnje, a navedeno se očekuje već kroz sljedećih tri do pet godina.

Kvaliteta usluga koju poduzeće nudi, njegova fleksibilnost, rokovi isporuke, odnosno odgovora te posvećenost svakom klijentu bez obzira na njegovu snagu, veličinu i platežnu moć, glavne su reference i preporuke koje poduzeću omogućuju da trenutno posluje s mnogobrojnim zadovoljnim klijentima iz cijelog svijeta.

Pronalazak i obradu novih tržišta i klijenata poduzeće ostvaruje samostalno te pomoću suradnika, čija se umreženost u ovoj vrsti djelatnosti često koristi kao poveznica za buduću suradnju. Široke mogućnosti i postojeći portfelj usluga tvrtki pritom olakšavaju ugovaranje novih poslova. Postojeći klijenti nerijetko imaju potrebu i želju za nastavkom suradnje, a pošto su u velikoj većini slučajeva fizičke osobe, tvrtka zbog svoje veličine i fleksibilnosti ima mogućnost brze prilagodbe promjenama tržišnog potencijala.

Poslovanje poduzeća Global Gaming Services d.o.o. usmjereno je ponajviše na realizaciju vlastitih ideja i inovacija te pretvaranje navedenih u konkretne usluge, zatim omogućavanje samih usluga i na kraju marketing i plasman usluga na domaće te ponajviše na strano tržište.

U poslovanju poduzeća Global Gaming Services d.o.o. postoji značajan prostor za razvoj i napredovanje. U tehničko-tehnološkom smislu razvoj je moguć kroz kontinuiranu nabavu novih tehnologija i inovacije te na tome utemeljenom proširenju ponude. U prodajno marketinškom smislu osnova za razvoj je osvajanje novih tržišta, podržano maksimalnom usmjerenošću na klijenta i fleksibilnošću u ispunjenju njihovih potreba.

4.2. Čimbenici i vrste rizika poduzeća Global Gaming Services d.o.o.

Na poslovanje poduzeća Global Gaming Services d.o.o. (kasnije – GGS) najviše utječu sljedeće vrste rizika: tehnološki rizici, rizici povezani s cyber sigurnošću, pravni i regulatorni rizici, tržišni rizici, rizici povezani s intelektualnim vlasništvom te operativni rizici. Jedna od

tehnoloških rizika koji utječe na poduzeće GGS je ograničenje engine[70] i platforme[71]. Naime, odabir pravog engine i razvojne platforme ima značajnu ulogu na području poslovanja ovog poduzeća. Loš odabir engine i platforme može ograničiti značajke koje se mogu implementirati, ciljne platforme (PC, konzole, mobilne) koje se mogu dosegnuti ili se može odraziti na ukupnu izvedbu pojedine igre.

Kako bi smanjilo pojavnost i utjecaj rizika ograničenja engine i platforme na svoje poslovanje, poduzeće GGS koristi nekoliko strategija upravljanja ovim rizikom. Poduzeće prije odabira engine i platforme detaljno analizira zahtjeve projekta. To uključuje procjenu veličine igre, željenih grafičkih detalja, mrežnih funkcionalnosti te drugih specifičnih potreba. Na temelju zahtjeva projekta uspoređuje različite engine i platforme i u tom kontekstu obraća pažnju na njihove snage i slabosti, dostupnost alata i zajednice te na cijenu. Važan segment strateškog pristupa upravljanju predmetnim rizikom su i konzultacije s iskusnim developerima.

Streteški pristup uključuje i optimizaciju. Redovito profiliranje performansi igre omogućuje identifikaciju uskih grla i područja gdje je potrebna optimizacija. Svaki engine i platforma imaju svoje specifične optimizacijske tehnike. Korištenje middleware-a[72] pomaže u automatizaciji nekih optimizacijskih zadataka i ubrzava razvoj.

Brzi razvoj tehnologije može učiniti zastarjelim softver i hardver koji se koriste za održavanje i unapređenje platforme, što zahtijeva stalna ulaganja u nove alate i vještine. Upravljanje rizikom brzog razvoja tehnologije u gaming poduzeću GGS je ključno za ostanak konkurentnim na tržištu koje se stalno mijenja. Strateški pristup poduzeća GGS na ovom području uključuje stalno praćenje trendova, ulaganje u istraživanje i razvoj, fleksibilne razvojne procese, partnerstva s tehnološkim poduzećima, edukaciju zaposlenika te prilagođavanje novim tehnologijama kako bi se osigurao kontinuirani razvoj platforme i zadržala konkurentska prednost na tržištu.

[70] *inform.* osnovni dio programa oko kojega se grade ostale funkcije i mogućnosti programskog paketa [*3D engine*]; jezgra

[71] Preuzeto iz engleskog jezika (eng. *platform*), način komunikacije ili zabave, poput televizije, radija ili interneta: "Trenutno objavljujemo oglase na nekoliko različitih platformi - webu, mobilnim telefonima s pristupom internetu i u različitim dijelovima novina."

[72] Preuzeto iz engleskog jezika (eng. *Middleware),* softver koji se nalazi između operativnog sustava i aplikacija koje se na njemu pokreću. Djelujući kao skriveni prevoditeljski sloj, middleware omogućuje komunikaciju i upravljanje podacima za distribuirane aplikacije

Ključni rizici na području cyber sigurnosti za poduzeće GGS su brojni i kompleksni te predstavljaju stalnu prijetnju za poslovanje ovog poduzeća. Oni se mogu podijeliti u sljedeća područja: Cyber napadi, ranjivosti u igrama i na unutarnje prijetnje.

Cyber napadi koji predstavljaju najznačajnije rizike za poduzeće GGS su: DDoS napadi, krađa identiteta, malware, ransomware i social engineering. DDoS napadi imaju za cilj onemogućiti pristup serverima i uslugama te predmetno može dovesti do prekida u igrama te posljedično i do gubitka korisnika. Hakeri mogu ukrasti osobne podatke igrača, financijske informacije i druge osjetljive podatke što može značajno negativno utjecati na poslovanje poduzeća GGS. Malware, kao što je zlonamjerni softver, može se infiltrirati u sustave i oštetiti podatke. Ransomware je vrsta malware-a koja šifrira podatke te traži otkupninu za njihovo dešifriranje te u slučaju realizacije ovog rizika, poduzeće GGS bi se suočilo sa značajnim financijskim gubicima. Uz navedeno, hakeri često koriste socijalne inženjering tehnike kako bi prevarili zaposlenike ili igrače, odnosno kako bi od njih dobili osjetljive informacije.

Ranjivnosti u igrama uključuju exploite[73] i botnete[74]. Ranjivosti u kodu igre mogu omogućiti hakerima da preuzmu kontrolu nad igračevim računom, da manipuliraju igrom ili da pristupe osjetljivim podacima. Botneti se mogu koristiti za izvršavanje različitih vrsta napada, uključujući DDoS napade, krađu podataka i manipulaciju igrom.

Unutarnje prijetnje na području sigurnosti s kojima se suočava poduzeće GGS uključuju nezadovoljne zaposlenike i ljudske pogreške. Zaposlenici koji su nezadovoljni svojim poslom mogu nanijeti štetu poduzeću na području sigurnosti. Ljudske pogreške, kao što su slabe lozinke ili otvaranje phishing e-poruka, mogu dovesti do sigurnosnih incidenata koji se mogu vrlo negativno odraziti na poslovanje poduzeća GGS.

U upravljanju cyber rizicima poduzeće GGS koristi sveobuhvatan pristup koji obuhvaća tehnološke, organizacijske i ljudske aspekte. Jedan od tehnološki pristupa podrazumijeva redovne sigunosne provjere (provođenje penetracijskih testiranja, skeniranja ranjivosti i drugih vrsta provjera kako bi se identificirale i uklonile sigurnosne smetnje). Koriste se i snažne lozinke te autentifikacija u dva faktora. Uz navedeno, poduzeće GGS redovito stvara sigurnosne kopije podataka. Redovito se provode i ažuriranja softvera i hardvera kako bi se uklonile

[73] Preuzeto iz engleskog jezika (eng. *Exploit*), iskoristiti nešto na način koji vam pomaže: iskoristiti svoje resurse
[74] Preuzeto iz engleskog jezika (eng. *Botnet*), skupina računala koja su pod kontrolom softvera s ugrađenim štetnim programima, bez znanja njihovih korisnika

njihove ranjivosti. Poduzeće je, također, implementiralo firewall i sustav za detekciju upada kako bi se zaštitili mrežni resursi. Podaci se šifriraju kako bi se poduzeće zaštitilo od neovlaštenog pristupa u slučaju krađe uređaja ili podataka. Na području sigurnosti radi se i kroz podjelu mreže na manje segmente da bi se ograničila šteta u slučaju incidenta.

Organizacijske strategije uključuju politike sigurnosti, edukaciju zaposlenika, upravljanje incidentima, suradnju s pružateljima usluga i osiguranje. Uspostavljene su jasne i detaljne politike sigurnosti koje se odnose na sve zaposlenike i suradnike. Provodi se redovita edukacija zaposlenika o cyber sigurnosti kako bi zaposlenici bolje shvatili potencijalne prijetnje te kako bi se pravovremeno i adekvatno zaštitili. Poduzeće, uz navedeno, ima izrađen plan za upravljanje incidentima koji može omogućiti brzo i učinkovito reagiranje u slučaju sigurnosnog incidenta. Suradnja s pružateljima usluga u oblaku, na području hostinga i drugih usluga osigurava poduzeću visoku razinu sigurnosti. Poduzeće je, također, osigurano od cyber rizika.

Poduzeće GGS potiče kulturu sigurnosti među zaposlenicima kako bi svi zaposlenici bili aktivno uključeni u zaštitu podataka. Provjerava se i pozadina svih zaposlenika koji imaju pristup osjetljivim podacima. Provodi se i nagrađivanje zaposlenika koji prijave sigurnosne probleme ili se u svojem radu pridržavaju sigurnosnih politika.

Rizici koji mogu utjecati na poduzeće GGS su i oni koji se odnose na pravno i regulatorno područje. To se odnosi na promjene zakonodavstva i poreza na nacionalnoj i međunarodnoj razini kao i na poznavanje zakonodavnih i poreznih sustava na međunarodnim tržištima na kojima poduzeće GGS posluje. Nedovoljno poznavanje zakonodavstva i poreznih sustava na nacionalnoj i međunarodnoj razini može značajno negativno utjecati na poslovanje poduzeća GGS. Kako bi se smanjila pojavnost ovih rizika, poduzeće trenutno koristi usluge računovodstva i pravnih usluga u Republici Hrvatskoj. S planom širenja poslovanja u Sjedinjene Američke Države i Njemačku, poduzeće će također angažirati stručnjake za računovodstvene i pravne usluge specijalizirane za ta tržišta.

Tržišni rizici se ponajviše odnose na promjene u preferencijama igrača, prekomjernu zasićenost tržišta, piraciju, promjene u poslovnom modelu, povećane troškove razvoja, ovisnost o platformama, snaga velikih brendova, kulturološke razlike na globalnom tržištu i dr. Na sve navedene tržišne rizike posebno mogu biti ranjiva mala poduzeća koja posluju u gaming industriji.

Poduzeće GGS tržišnim rizicima upravlja primjenom nekoliko strategija. Jedan od strateških pristupa odnosi se na istraživanje tržišta. Redovitim istraživanjem tržišta poduzeće dobiva uvid o kretanjima na tržištu, preferencijama potrošača, različitim potrebama potrošača na pojedinim tržištima i dr. Upravljanje tržišnim rizicima poduzeće GGS provodi i kroz diverzifikaciju. Bitan čimbenik na ovom području je i agilnost u poslovanju kao i uspostavljanje partnerstva s drugim poduzećima u gaming industriji. Naglasak se stavlja i na praćenje poslovanja konkurencije kao i na razvijanje inovativnih rješenja na području gaming industrije.

Ključni rizici vezani uz intelektualno vlasništvo s kojima se suočava poduzeće GGS su: kršenje autorskih prava, kršenje žigova, krađa poslovnih tajni i piratstvo. Da bi poduzeće smanjilo potencijal realizacije ovih rizika, koristi odobrenja za korištenje tuđih autorskih prava te provodi registraciju vlastitog intelektualnog vlasništva. Također, potpisuje ugovore o partnerstvu s vanjskim suradnicima.

Operativni rizici kojima je izloženo poduzeće GGS uključuju prekoračenje budžeta u sloku projekata koje poduzeće provodi, nedostatak kvalitete, promjene u dizajnu igre, loše upravljanje projektima i dr. Realizacija ovih rizika mogla bi se značajno negativno odraziti na kvalitetu proizvoda i usluga ovog poduzeća kao i na njegove financijske rezultate te tržišni ugled. Da bi poduzeća smanjilo pojavnost ovih rizika, strateški im pristupa.

Poduzeće sve projekte planira te planira način na koji će realizirati upravljanje projektima. Također, u sklopu svakog projekta provodi procjenu rizika i na temelju iste razrađuje mjere vezane uz upravljanje rizicima. Uz navedeno, prije nego što se plasiraju određeni proizvodi na tržište, provodi se njihovo testiranje te se otklanjaju uočeni nedostaci i slabosti.

4.3. Matrica rizika i budući razvoj upravljanja rizikom u poduzeću Global Gaming Services

Matrica procjene rizika je alat koji pomaže u identifikaciji, analizi i vrednovanju potencijalnih rizika s kojima se poduzeće može suočiti. Omogućuje razumjeti vjerojatnost nastanka određenog rizika i njegov potencijalni utjecaj na poslovanje. Elementi matrice su:

- Rizik: kratak opis rizika.

- Vjerojatnost: procjena koliko je vjerojatno da će se rizik dogoditi (niska, srednja, visoka).
- Utjecaj: procjena koliki bi bio utjecaj rizika na poslovanje u slučaju da se dogodi (mali, srednji, veliki).
- Prioritet: kombinacija vjerojatnosti i utjecaja, koja određuje koliko je hitno poduzeti mjere za upravljanje rizikom (nizak, srednji, visok).
- Mjere ublažavanja: predložene aktivnosti za smanjenje vjerojatnosti nastanka rizika ili ublažavanje njegovog utjecaja.

Matrica rizika izrađena je kroz strukturirani proces koji je uključivao intervjue s ključnim članovima menadžmenta i vanjskim suradnicima poduzeća Global Gaming Services. Ovaj postupak uključivao je razgovore s voditeljima odjela, uključujući voditelja operacija, voditelja development tima, voditelja financija, te vanjskim partnerima kao što su knjigovodstveni servis i pravnik s kojim poduzeće redovno surađuje. Cilj ovih intervjua bio je identificirati ključne rizike koji mogu utjecati na poslovanje poduzeća te procijeniti njihovu vjerojatnost i potencijalne posljedice.

Vjerojatnost i posljedice svakog rizika ocijenjene su na skali od 1 do 5. Na temelju tih ocjena, rizici su rangirani u različite razrede, od niskog do ekstremnog rizika. Točnije:

1) Vjerojatnost:
    - Gotovo nevjerojatno: 1
    - Malo vjerojatno: 2
    - Vjerojatno: 3
    - Vrlo vjerojatno: 4
    - Gotovo sigurno: 5

2) Posljedica:
    - Neznatna: 1
    - Mala: 2
    - Umjerena: 3
    - Značajna: 4
    - Katastrofalna: 5

Nakon što su rizici identificirani i procijenjeni, smješteni su u matricu rizika koja omogućuje vizualnu prezentaciju kombinacije vjerojatnosti i posljedica. Matrica je dalje korištena za rangiranje rizika te za definiranje prioriteta u tretiranju rizika. Na primjer, rizici s visokom vjerojatnošću i visokim posljedicama identificirani su kao prioriteti za tretiranje, dok su rizici s niskom vjerojatnošću i niskim posljedicama smatrani manje kritičnima. Tablica 2 prikazuje matricu rizika poduzeća Global Gaming Services.

Tablica 2. Matrica rizika poduzeća Global Gaming Services

VJEROJATNOST							
	5	Gotovo sigurno				Cyber rizici	
	4	Vrlo vjerojatno			Tržišni rizici	Financijski rizik; Rizici intelektualnog vlasništva	
	3	Vjerojatno			Pravni rizici; Operativni rizici		Tehnički rizici
	2	Malo vjerojatno			Ljudski resursi		
	1	Gotovo nevjerojatno					
			Naznatna	Mala	Umjerena	Značajna	Katastrofalna
			1	2	3	4	5
			POSLJEDICA				

Izvor: Izrada autorice

Tablica 3. Tablica rangiranja i tretiranja rizika poduzeća Global Gaming Services

Razina rizika	Rangiranje	Rizik	Tretiranje
Vrlo nizak rizik	1-2		
Nizak	3-4		
Srednji	4-9	Pravni rizici	Pravni savjetnici, osiguranje, redovito praćenje zakona
		Operativni rizici	Agile metodologije, backup planovi
		Ljudski resursi	Programi obuke, strategije zadržavanja zaposlenika
Visok	10-12	Tržišni rizici	Marketinške analize, prilagodba proizvoda
Vrlo visok rizik	15-16	Financijski rizik	Financijsko planiranje, diversifikacija prihoda
		Tehnički rizici	Cyber sigurnosne mjere, redovito održavanje
		Rizici intelektualnog vlasništva	Pravni tim, registracija IP-a, praćenje kršenja prava
Ekstreman	20-20	Cyber rizici	Firewall, antivirus, redovite sigurnosne provjere

Izvor: Izrada autorice

Rizici povezani s pravnim pitanjima, kao što su povrede autorskih prava ili nepridržavanje lokalnih zakona te oni vezani uz porezne politike su rizici čija je vjerojatnost pojave srednja te pojavnost ovog rizika može imati srednji utjecaj na poslovanje poduzeća. Promjene u zakonodavstvu mogu dovesti do dodatnih troškova, ograničenja poslovanja ili čak zabrane određenih aktivnosti. Angažiranje pravnih savjetnika, osiguranje za pravne sporove, kontinuirano praćenje zakonodavnih promjena neke su od mjera koje poduzeće GGS može poduzeti kako bi poboljšalo upravljanje ovim rizicima.

Rizici vezani uz financiranje, kao što su manjak kapitala ili loše upravljanje financijama imaju visoku vjerojatnost pojavnosti te u slučaju njihove pojavnosti poduzeće bi se susrelo s visokim utjecajem što znači da je ovaj rizik vrlo značajan za poduzeće GGS te da njime treba

učinkovito upravljati. Neke od mjera koje poduzeće može poduzeti su: dobro financijsko planiranje, izrada rezervnih fondova, diversifikacija izvora prihoda, smanjenje troškova i dr.

Rizici vezani uz operativne procese, kao što su problemi u nadogradnji platforme ili problemi sa serverima imaju srednju vjerojatnost pojavnosti u poduzeću GGS te u slučaju njihove realizacije poduzeće bi se suočavalo sa srednjim utjecajem ovog rizika na poslovanje poduzeća. Poduzeće može poboljšati upravljanje ovim rizikom uvođenjem agilnih metodologija, redovitim pregledom i backup planovima. Dodatno, poduzeće može poboljšati upravljanje operativnim rizicima kroz nekoliko ključnih mjera. Prvo, implementacija automatiziranih sustava za nadzor performansi platforme omogućila bi brzo prepoznavanje i rješavanje potencijalnih problema prije nego što postanu ozbiljni. Drugo, redovita testiranja opterećenja (load testing) mogu pomoći u procjeni kapaciteta servera i osiguravanju da platforma može podnijeti povećani promet bez gubitka funkcionalnosti. Konačno, kontinuirana edukacija i obuka tehničkog tima osigurat će da zaposlenici budu sposobni učinkovito reagirati na bilo kakve tehničke izazove i minimizirati rizike povezane s operativnim procesima.

Rizici povezani s tehničkim aspektima, poput cyber napada ili tehničkih kvarova imaju visoku vjerojatnost pojave. U slučaju njihove pojave, oni bi imali visok utjecaj na poslovanje poduzeća što znači da je kod ovih rizika jako važno razviti kvalitetne sustave usmjerene na strateški pristup njihovom upravljanju. Mjere upravljanja uključuju ulaganje u sigurnosne mjere, redovito održavanje tehničke infrastrukture, obuku osoblja za upravljanje kriznim situacijama te izradu planova za reakciju na krizne situacije. Implementacija enkripcije podataka može dodatno zaštititi osjetljive informacije od neovlaštenog pristupa, dok uvođenje višefaktorske autentifikacije smanjuje rizik od neovlaštenog ulaska u sustav. Također, upotreba sigurnosnih zakrpa (patch management) kako bi redovito ažuriralo softver i uklonilo poznate ranjivosti. Provođenje redovite simulacije sigurnosnih incidenata kako bi testirala spremnost vlastitih sustava i osoblja za upravljanje kriznim situacijama, čime bi se dodatno smanjila mogućnost ozbiljnih poremećaja u poslovanju.

Rizici vezani uz tržište, kao što su promjene u preferencijama korisnika ili jaka konkurencija imaju visoku vjerojatnost za pojavu. No, u slučaju njihove pojave utjecaj na poslovanje poduzeća GGS bio bi visok dok bi posljedice na samo poslovanje bile srednje. Mjere upravljanja uključuju kontinuirane marketinške analize, prilagodbu proizvoda i usluge prema tržišnim trendovima te razvoj i implementaciju strategija za brzi odgovor na promjene u

preferencijama korisnika. Poduzeće treba uspostaviti programe za stalno praćenje konkurencije, uključujući analizu njihovih strategija, kako bi anticipiralo njihove poteze i razvilo odgovarajuće odgovore. Također, potrebno je provoditi diversifikaciju proizvoda i usluga kako bi se smanjila ovisnost o određenom tržišnom segmentu i time smanjio utjecaj promjena u preferencijama korisnika. Kontinuirano ulaganje u inovacije i istraživanje tržišta ključno je za proaktivno kreiranje novih trendova, čime se dodatno smanjuje rizik od tržišnih promjena i povećava konkurentska prednost poduzeća na globalnom tržištu.

Rizici vezani uz ljudske resurse, kao što su nedostatak kvalificiranih radnika ili visoka fluktuacija zaposlenika imaju malu vjerojatnost pojave. Utjecaj realizacije ovih rizika na poslovanje poduzeća GGS bio bi srednji te je riječ o rizicima koji se ne uvrštavaju u prioritetne na području gaming industrije. Među mjere upravljanja uvrštavaju se razvoj programa obuke, stvaranje motivirajuće radne okoline, strategije zadržavanja talenata i sl. Također, potrebno je provoditi redovite procjene zadovoljstva zaposlenika kako bi se pravovremeno uočili i riješili eventualni problemi koji bi mogli dovesti do fluktuacije. Poduzeće treba uspostaviti sustave mentorstva i kontinuiranog razvoja karijere kako bi zaposlenici imali jasne putove napredovanja unutar organizacije. To može pomoći u zadržavanju talenata, jer zaposlenici vide dugoročne mogućnosti unutar tvrtke. Također, važna je fleksibilnost u radnim uvjetima, uključujući mogućnosti rada na daljinu ili fleksibilno radno vrijeme, što može povećati zadovoljstvo i smanjiti fluktuaciju. Dodatno, uspostava programa nagrađivanja za postignute rezultate i doprinos može dodatno motivirati zaposlenike i smanjiti rizik od gubitka ključnih radnika. Ulaganje u dobrobiti zaposlenika, kao što su zdravstveno osiguranje, dodatni slobodni dani ili programi za balansiranje rada i privatnog života, također može doprinijeti smanjenju ovih rizika.

Cyber rizici, odnosno rizici povezani s cyber napadima, krađom podataka, ransomware-om i drugim prijetnjama digitalnoj sigurnosti uvrštavaju se među rizike koji imaju visoku vjerojatnost pojave s obzirom na povećanje cyber napada. Utjecaj tih rizika je visok jer pojavnost cyber rizika može dovesti do gubitka podataka, narušavanja reputacije i velikih financijskih gubitaka za poduzeće GGS. Da bi predmetno poduzeće što bolje upravljalo ovim rizicima, treba provoditi sljedeće mjere upravljanja:

- **Implementaciju snažnog firewalla i antivirusnih programa:** Osiguravanje visoke razine zaštite mrežnih sustava kroz upotrebu naprednih firewall i antivirusnih rješenja koja mogu prepoznati i neutralizirati prijetnje,
- **Redovite sigurnosne provjere i ažuriranja softvera:** Provoditi redovite sigurnosne provjere svih sustava te pravovremeno ažurirati softver kako bi se eliminirale ranjivosti koje bi mogle biti iskorištene za napade,
- **Edukaciju zaposlenika o sigurnosnim protokolima:** Stalna edukacija zaposlenika o najnovijim sigurnosnim prijetnjama i protokolima koji se moraju poštivati kako bi se smanjila mogućnost ljudske pogreške koja može dovesti do sigurnosnih incidenata,
- **Backup podataka na sigurne lokacije:** Redovito stvaranje sigurnosnih kopija podataka i pohranjivanje istih na sigurne lokacije kako bi se osigurao kontinuitet poslovanja u slučaju gubitka podataka uslijed napada,
- **Primjena višefaktorske autentifikacije (MFA):** Korištenje višefaktorske autentifikacije za pristup ključnim sustavima i podacima kako bi se dodatno smanjio rizik od neovlaštenog pristupa,
- **Segmentacija mreže:** Razdvajanje mreže na manje segmente kako bi se ograničila šteta u slučaju kompromitacije jednog dijela sustava. Na taj način, eventualni napad neće imati mogućnost širenja kroz cijelu mrežu,
- **Razvoj plana odgovora na incidente:** Izrada i redovita revizija plana za odgovor na cyber incidente koji uključuje korake za brz i učinkovit povratak u normalno poslovanje nakon napada,
- **Redoviti testovi ranjivosti i penetracijski testovi:** Povremeno provoditi testove ranjivosti i penetracijske testove kako bi se otkrile i uklonile potencijalne slabosti u sustavu prije nego što ih napadači mogu iskoristiti.

Rizici intelektualnog vlasništva su rizici povezani s povredom autorskih prava, krađom intelektualnog vlasništva, patentnim sporovima i drugiim kršenjima prava intelektualnog vlasništva. Vjerojatnost realizacije ovog rizika je visoka budući da je gaming industrija obilježena kao industrija s visokom stopom inovacija. Utjecaj pojave ovog rizika na poduzeće GGS bio bi visok jer realizacija ovog rizika može dovesti do pravnih sporova, financijskih gubitaka te gubitaka u kontekstu konkurentske prednosti. Kako bi poduzeće GGS što učinkovitije upravljalo ovim rizikom, treba provoditi sljedeće mjere na području upravljanja:

- **Angažiranje pravnog tima specijaliziranog za intelektualno vlasništvo:** Osiguranje stručne pravne podrške koja će nadzirati sve aspekte intelektualnog vlasništva, od registracije do zaštite autorskih prava, patenata i zaštitnih znakova,
- **Registraciju patenata, autorskih prava i zaštitnih znakova:** Pravovremena registracija svih oblika intelektualnog vlasništva kako bi se osiguralo pravno pokriće i zaštita od potencijalnih povreda prava,
- **Praćenje tržišta za kršenja prava intelektualnog vlasništva i brzo reagiranje na povrede:** Aktivno praćenje tržišta kako bi se identificirale potencijalne povrede prava intelektualnog vlasništva, uz brzo poduzimanje pravnih mjera kako bi se zaštitili interesi poduzeća,
- **Edukaciju zaposlenika o važnosti zaštite intelektualnog vlasništva:** Stalna edukacija zaposlenika o važnosti zaštite intelektualnog vlasništva, uključujući prepoznavanje potencijalnih povreda i postupke prijave istih unutar poduzeća,
- **Provođenje revizije ugovora s vanjskim suradnicima i partnerima**: Osiguranje da svi ugovori s vanjskim suradnicima i partnerima jasno definiraju vlasništvo nad intelektualnim pravima i obvezu zaštite povjerljivih informacija,
- **Uvođenje politike povjerljivosti (NDA)**: Uvođenje i primjena ugovora o povjerljivosti (NDA) s zaposlenicima, vanjskim suradnicima i poslovnim partnerima kako bi se dodatno zaštitile poslovne tajne i druge ključne informacije,
- **Redovita procjena i ažuriranje strategije intelektualnog vlasništva**: Periodično preispitivanje i prilagodba strategije intelektualnog vlasništva kako bi se osigurala njezina učinkovitost s obzirom na promjene u poslovnom okruženju i tržištu.

Ova matrica rizika omogućila je poduzeću Global Gaming Services da bolje razumije i upravlja potencijalnim prijetnjama koje mogu utjecati na njihovo poslovanje. Kroz intervjue s ključnim osobama i detaljnu analizu, poduzeće je dobilo jasnu sliku o rizicima te je razvilo učinkovite strategije za njihovo ublažavanje i kontrolu. Također je važno naglasiti da je matrica rizika neophodan alat za kontinuirano praćenje i prilagodbu strategija upravljanja rizicima u skladu s promjenama u poslovnom okruženju i tehnološkim napretkom. Redovito ažuriranje matrice rizika osigurat će da poduzeće uvijek bude spremno odgovoriti na nove izazove. To uključuje ponavljanje intervjua s ključnim osobama u poduzeću, kao i stalnu edukaciju zaposlenika kako bi se osiguralo da su svi svjesni najnovijih prijetnji i najboljih praksi za njihovo ublažavanje.

5. Zaključak

Gaming industrija, kao jedna od najdinamičnijih i najbrže rastućih industrija današnjice, suočava se s brojnim izazovima i rizicima. Od tehnoloških previranja do promjena u regulatornom okruženju, suočavaju gaming poduzeća na sprenost na nepredviđene situacije. Upravljanje rizicima postaje ključni element za dugoročni uspjeh u ovom kompetitivnom okruženju.

U analizi rizika poduzeća Global Gaming Services provedeno je nekoliko ključnih koraka koji su omogućili detaljno razumijevanje potencijalnih prijetnji s kojima se poduzeće može suočiti. Kroz intervjue s ključnim osobama u poduzeću, uključujući voditelje odjela, vanjske suradnike te stručnjake za pravna i financijska pitanja, identificirani su glavni rizici. Ova analiza uključivala je ne samo identifikaciju rizika već i njihovu procjenu u smislu vjerojatnosti pojave i potencijalnih posljedica na poslovanje poduzeća. Nakon identifikacije, rizici su rangirani pomoću matrice rizika koja omogućuje vizualizaciju rizika u kontekstu njihove vjerojatnosti i utjecaja.

Matrica je poslužila kao osnova za daljnje donošenje odluka o prioritetima u tretiranju rizika. Primjerice, rizici s visokom vjerojatnošću i visokim posljedicama, poput cyber rizika i rizika povezanih s intelektualnim vlasništvom, identificirani su kao prioritetni i zahtijevaju hitne mjere upravljanja. S druge strane, rizici s niskom vjerojatnošću i niskim posljedicama smatrani su manje kritičnima, ali su i dalje uključeni u strategije upravljanja. Tijekom analize, također je definirano kako su određeni razredi rizika (nisko, srednje, visoko) temeljeni na specifičnim postotcima i kriterijima. Na primjer, tehnički rizici povezani s održavanjem i sigurnošću sustava rangirani su visoko zbog njihovog potencijalnog utjecaja na poslovanje, dok su rizici vezani uz ljudske resurse, poput fluktuacije zaposlenika, rangirani niže zbog njihove manje vjerojatnosti pojave. Osim toga, preporučene su specifične mjere za ublažavanje i kontrolu svakog od identificiranih rizika. Za upravljanje cyber rizicima, predloženo je uvođenje naprednih sigurnosnih mjera poput višefaktorske autentifikacije, redovitih sigurnosnih provjera i kontinuirane edukacije zaposlenika. Za operativne rizike, naglasak je stavljen na uvođenje agilnih metodologija i automatiziranih sustava za nadzor performansi platforme.

Zaključno, ova analiza rizika i izrada matrice rizika omogućile su poduzeću Global Gaming Services da precizno identificira, procijeni i prioritizira rizike te razvije učinkovite

strategije za njihovo upravljanje. Preporučuje se da poduzeće redovito ažurira matricu rizika i ponavlja procese procjene kako bi osiguralo da su sve promjene u poslovnom okruženju i tehnologiji pravovremeno identificirane i adekvatno tretirane.

Ova proaktivna praksa upravljanja rizicima ključna je za održavanje konkurentnosti i otpornosti poduzeća na dinamičnom tržištu gaming usluga. Prvi korak u upravljanju rizicima je identifikacija svih potencijalnih rizika s kojima se gaming poduzeće može suočiti. Nakon identifikacije, rizici se procjenjuju prema njihovoj vjerojatnosti i potencijalnom utjecaju na poslovanje. Na temelju procjene, rizici se rangiraju po prioritetu, kako bi se moglo usmjeriti na najvažnije. Za svaki rizik razvijaju se konkretne mjere koje će smanjiti njegovu vjerojatnost ili utjecaj. Proces upravljanja rizicima je kontinuiran i zahtijeva redovitu reviziju i ažuriranje. Upravljanje rizicima je ključni element za dugoročni uspjeh u gaming industriji. Kroz sistematičan pristup identifikaciji, procjeni i ublažavanju rizika, gaming poduzeća mogu povećati svoju otpornost na nepredviđene situacije i osigurati dugoročni rast.

Bibliografija

1. Acquah, C. (2021) The impact of risk of businesses, dostupno na: https://www.researchgate.net/publication/350104154_THE_IMPACT_OF_RISK_ON_BUSINESSES (pristupljeno 17. 5. 2024.)
2. Bhatti, K. (2023) The Importance of Security Compliance in the Gaming Industry, dostupno na: https://www.linkedin.com/pulse/importance-security-compliance-gaming-industry-kaushik-bhatti-/ (pristupljeno 3. 7. 2024.)
3. Deželjin, J. (1998) Poduzetništvo, neizvjesnost i rizik, Računovodstvo, revizija i financije, 8(8), str. 1532.-1539.
4. Course, E. R. (2024) Cyber security in the gaming industry, International Journal of Novel Research and Development, 9(3), str. 16-23.
5. Faster Capital, Risks And Challenges In The Gaming Industry, dostupno na: https://fastercapital.com/topics/risks-and-challenges-in-the-gaming-industry.html (pristupljeno 1. 6. 2024.)
6. Financial Crime Academy (2024) Impact Of Risk On Organizations: Why Manage Risk?, dostupno na: https://financialcrimeacademy.org/impact-of-risk-on-organizations/ (pristupljeno 20. 5. 2024.)
7. Gillis, A. S., ISO 31000 Risk Management, dostupno na: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management (pristupljeno 12. 6. 2024.)
8. GlobalSuite (2023) What is ISO 31000 standard and what is its purpose? Discover the importance of risk management in your organization, dostupno na: https://www.globalsuitesolutions.com/what-is-iso-31000-standard-and-what-is-its-purpose/ (pristupljeno 5. 7. 2024.)
9. Harris, C. i sur., What are the best risk management practices for the gaming industry?, dostupno na: https://www.linkedin.com/advice/0/what-best-risk-management-practices-gaming-industry-grebe (pristupljeno 20. 6. 2024.)
10. InternetReputation (2023) The Intersection of Online Gaming and Reputation Management, dostupno na: https://www.internetreputation.com/online-gaming-reputation-management/ (pristupljeno 22. 6. 2024.)

11. IRM (2018) A Risk Practitioners Guide to ISO 31000: 2018, dostupno na: https://www.demarcheiso17025.com/document/A%20Risk%20Practitioners%20Guide%20to%20ISO%2031000%20%96%202018.pdf (pristupljeno 2. 7. 2024.)
12. Kerzner, H. (2003) Project Management: A Systems Approach to Planning, Scheduling, and Controlling, Eighth Edition, John Wiley & Sons.
13. Klemetti, A. (2006) Risk management in construction project networks. Report 2006/2. Laboratory of Industrial Management, Helsinki University of Technology. Helsinki, Finland.
14. Krakar, Z. (2024) Upravljanje rizicima neusklađenosti, dostupno na: https://www.linkedin.com/pulse/upravljanje-rizicima-neuskla%C4%91enosti-zdravko-krakar/ (pristupljeno 15. 7. 2024.)
15. Olson, D. L., Wu Dash, D., (2008) Enterprises Risk Management, World Scientific Publishing Co. Pte. Ltd. Singapore.
16. Omazić, M. A., Baljkas, S. (2005) Projektni menadžment, Sinergija, Zagreb.
17. Project Management Institute (2004) A Guide to the Body of Knowledge, Third Edition, PMI, Pennsylvania, USA.
18. Orikhon, V., Intellectual Property Protection in the Gaming Industry, dostupno na: https://iprgroup.info/intellectual-property-protection-in-the-gaming-industry-trademark-and-patent-registration-in-one-of-the-fastest-growing-entertainment-industries/ (pristupljeno 2. 7. 2024.)
19. Radović, D. (2001) Rizik kao fenomen privređivanja i projekt menadžmenta, Montenegrin Journal of Economics, 1(9), str. 140-161.
20. Ramanathan, C., Narayanan, S. P., Idrus, A. B. (2012) Construction delays causing risks on time and cost - A critical review. Australasian Journal of Construction Economics and Building, 12(1), str. 37–57.
21. Shahr Development (2018) ISO 31000, dostupno na: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf (pristupljeno 12. 6. 2024.)
22. Sharma, S., How can game developers ensure stability and reliability across platforms?, dostupno na: https://www.linkedin.com/advice/1/how-can-game-developers-ensure-stability-reliability-yk0be (pristupljeno 1. 7. 2024.)
23. Smith, P. G., Merritt, G. M. (2002) Proactive Risk Management, Productivity Press, SAD.

24. Šegudović, H. (2006) Prednosti i nedostaci metoda za kvalitativnu analizu rizika, Infigo, Zagreb.
25. Srinivas, K. (2019) Process of Risk Management, dostupno na: https://www.researchgate.net/publication/331783796_Process_of_Risk_Management (pristupljeno 11. 6. 2024.)
26. The Green Book (2003) Appraisal and Evaluation in Central Government, Treasury Guidance, London, str. 80-90.
27. Van Well-Stam, D. i sur. (2004) Project Risk Management, Kogan Page Publishers, United Kingdom, str. 31-39.

Popis ilustracija

Tablice

Slike