Upravljanje rizicima s aspekta norme sustava upravljanja kontinuitetom poslovanja i povezivanje s normom sustava upravljanja rizicima

Šijak, Ana Marija

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:724743

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

University North Digital Repository

Sveučilište Sjever

ODJEL ZA EKONOMIJU

ODSJEK ZA POSLOVANJE I MENADŽMENT

Završni rad br. 245/PMM/2020

Upravljanje rizicima s aspekta norme sustava upravljanja kontinuitetom poslovanja i povezivanje s normom sustava upravljanja rizicima

Student

Ana Marija Šijak, 2606/336

Mentor

prof. dr. sc. Krešimir Buntak

Koprivnica, rujan 2020.godine

Sveučilište Sjever
Sveučilišni centar Koprivnica
Trg dr. Žarka Dolinara 1, HR-48000 Koprivnica

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL: Odjel za ekonomiju

STUDIJ: preddiplomski stručni studij Poslovanje i menadžment

PRISTUPNIK: Ana Marija Šijak | MATIČNI BROJ: 2606/336

DATUM: 28.09.2020. | KOLEGIJ: Upravljanje kvalitetom

NASLOV RADA: Upravljanje rizicima s aspekta norme sustava upravljanja kontinuitetom poslovanja i povezivanje s normom sustava upravljanja rizicima

NASLOV RADA NA ENGL. JEZIKU: Risk management from the aspect of the norm of the business continuity management and connecting with risk management norm

MENTOR: dr.sc. Krešimir Buntak | ZVANJE: Izvanredni profesor

ČLANOVI POVJERENSTVA:

1. doc.dr.sc. Mirko Smoljić, predsjednik
2. doc.dr.sc. Ana Globočnik Žunac, članica
3. prof.dr.sc. Krešimir Buntak, mentor, član
4. dr.sc. Ivana Martinčević, zamjenska članica
5.

Zadatak završnog rada

BROJ: 245/PMM/2020

OPIS:

Sve veća turbulentnost u organizacijskim okolinama i sve veća potreba vezana uz imperativ osiguranja kontinuiteta poslovanja današnjih organizacija, organizacije prisiljava na promišljanje načina analize rizika povezanih uz narušavanje kontinuiteta poslovanja. Jedan od načina za smanjenje prijetnji povezanih uz narušavanje kontinuiteta poslovanja je implementacija sustava upravljanja rizicima i sustava upravljanja kontinuitetom poslovanja. Budući da je analiza rizika osnova za osiguranje kontinuiteta poslovanja, neophodno je analizirati usklađenost normi sustava upravljanja rizikom i sustava upravljanja kontinuitetom poslovanja. Cilj ovog rada je analizirati povezanost između upravljanja rizicima i upravljanja kontinuitetom poslovanja. U ovom završnom radu potrebno je:

1. Opisati rizik
2. Opisati upravljanje rizicima
3. Opisati metode upravljanja rizicima
4. Opisati normu ISO 22301:2019
5. Opisati normu ISO 31000:2018
6. Analizirati povezanost između upravljanja rizicima i upravljanja kontinuitetom poslovanja

ZADATAK URUČEN: 6.10.2020 | POTPIS MENTORA:

SVEUČILIŠTE SJEVER

ODJEL ZA EKONOMIJU

ODSJEK ZA POSLOVANJE I MENADŽMENT

Završni rad br. 245/PMM/2020

Upravljanje rizicima s aspekta norme sustava upravljanja kontinuitetom poslovanja i povezivanje s normom sustava upravljanja rizicima

Student

Ana Marija Šijak, 2606/336

Mentor

prof. dr. sc. Krešimir Buntak

Koprivnica, rujan 2020.godine

Predgovor

Zahvaljujem svim profesorima i djelatnicima Sveučilišta Sjever na stečenom znanju, pomoći i savjetima. Posebno zahvaljujem svojem mentoru dr. sc. Kršimir Buntak na usmjeravanju, vodstvu, strpljenju te pomoći, kao i na razumijevanju i susretljivosti tijekom procesa nastanka ovog rada. Iznimno se zahvaljujem svojim roditeljima koji su me oduvijek poticali na obrazovanje i bili potpora tijekom cijelog obrazovanja. Isto tako se zahvaljujem svojim prijateljima i kolegama koji su me motivirali i davali mi podršku tijekom trajanja fakulteta.

Sažetak

Ovaj završni rad ima zadatak objasniti čitatelju što znači upravljati rizicima u organizaciji. Rizici su postali svakodnevni dio organizacije , stoga je bitno da organizacija zna kvalitetno upravljati njima. Kako bi pomogla organizacijama da se na pravi način pripreme i nose s rizikom, Međunarodna organizacija za standardizaciju (ISO) objavila je nekoliko normi za lakše upravljanje rizicima. Dalje se u radu definiraju norma ISO 22301:2019 i norma ISO 31000:2018. Nakon tumačenja rizika i normi, slijedi usporedba norme ISO 23001:2019 i norme ISO 31000:2018:2018.

Ključne riječi: upravljanje rizicima, organizacija, ISO 22301:2019, ISO 31000:2018

Summary

This Final Work has the task to explain to the reader, what means to manage the risk in the organisation. Risks have become a daily part of the organisation, so it is essential that the organisation knows how to quality managing them. In order to help organisations to prepare and manage risks, the International Organisation for Standardisation (ISO) has published several standards to easier risk managing. The standards ISO 22301:2019 and ISO 31000:2018 are defined further in the final work. After risk interpretation and standards, comes comparison of ISO 23001: 2019 and ISO 31000: 2018 standards

Key words: Risk managing, organization, ISO 22301:2019, ISO 31000:2018.

Popis korištenih kratica

BCM

Business Continuity Management

BCMS

Business Continuity Management System

BCP

Business Continuity Plan Business

BIA

Business Impact Analysis

IEC

International Electrotechnical Commission

ISO

International Organization for Standardization

IT

Informatička tehnologija

PDCA

Plan, Do, Check, Act

RTO

Recovery Time Objective

Sadržaj

1.Uvod 1

2.Rizik 2

1.1. Izvori rizika 3

2.2. Podjela rizika 4

3.Upravljanje rizicima 6

3.1. Uspostavljanje konteksta 7

3.2. Identifikacija rizika 7

3.3. Analiza rizika 7

3.4. Procjena rizika 9

4.Metode upravljanja rizicima 11

5.Norma ISO 22301:2019 Sigurnost i otpornost - sustavi upravljanja kontinuitetom poslovanja 13

5.1.Struktura norme ISO 22301:2019 Sigurnost i otpornost – sustavi upravljanja kontinuitetom poslovanja 18

6.Norma ISO 31000:2018 sustav upravljanja rizicima 27

6.1 Načela norme ISO 31000:2018 29

6.2.Okvir norme ISO 31000:2018. 29

6.3. Proces upravljanja rizikom u normi ISO:31000:2018 37

7. Povezanost između upravljanja rizicima i upravljanja kontinuitetom poslovanja 44

8. Zaključak 47

1.Uvod

U ovom završnom radu obrađena je tema vezana za upravljanje rizicima, te povezivanje rizika s aspekta norme ISO 23001:2019 i povezivanje s normom ISO 31000:2018 u organizaciji. U današnje vrijeme organizacije su pod stalnim neizvjesnostima i promjena zbog situacije koja vlada na tržištu. Organizacije su pod utjecajem mnogobrojnih negativnih čimbenika, te moraju biti pripremljene za nastanak novih. Negativni čimbenici koji utječu na organizaciju nazivamo rizicima, a njime se mogu zaštiti kreirajući plan upravljanja rizicima.

Rizik, upravljanje rizikom, te upravljanje kontinuitetom poslovanju su povezani sa rješavanjem ili smanjenjem rizika. Organizacije su prisiljene odmah reagirati na pojavu rizika, iako nemaju planove za ovakve situacije. Brza reakcija može rezultirati lošim donošenjem odluke koja može utjecati na kontinuitet poslovanja. Upravljanje kontinuitetom poslovanja je postupak kojim se utvrđuju s kojima se rizikom organizacija susrela. Više nije dovoljno izraditi plan odgovora koji predviđa i umanjuje posljedice prirodnih, slučajnih ili namjernih rizika, već organizacije također moraju poduzeti prilagodljive i proaktivne mjere kako bi smanjile utjecaj rizika.

Upravljanje rizikom i planovi kontinuiteta poslovanja presudni su za kontinuirani rad svih organizacija. Još važnije, ovi planovi poprimaju sve veću važnost kako se organizacije sve više oslanjaju na tehnologiju u poslovanju. ISO 31000:2018 standard pod nazivom „Upravljanje rizicima - Smjernice" mogu koristiti bilo koje organizacije kako bi postigle svoje ciljeve, poboljšale prepoznavanje prilika i prijetnji i učinkovitije koristile resurse za rješavanje rizika. ISO 22301:2019, prvi svjetski međunarodni standard za upravljanje kontinuitetom poslovanja, razvijen je kako bi pomogao organizacijama da minimaliziraju rizik. Upravljanje oporavkom od katastrofa obično se odvija u procesu upravljanja kontinuitetom poslovanja..

2.Rizik

Postoje mnoge definicije koji opisuju rizik, a neka opća definicija glasi, rizik nastaje od vjerojatnosti nekog događaja koji može imati negativne posljedice bilo to za pojedinca ili organizaciju, te se on smatra kao nemogućnost predviđanja krajnjeg rezultata sa sigurnošću. Organizacije svakodnevno nailaze na rizike. Stoga, neke Organizacije će doživjeti neuspjeh u budućnosti jer nemaju dovoljno znanja o vrstama rizika i upravljanju njima, te ne mogu poboljšati svoju strategiju. Rizik se najčešće veže uz poslovanje te ga s tog aspekta definira kao vjerojatnost pojave nekog događaja koji će imati negativan utjecaj na poslovanje organizacije, kao što su na npr. porast troškova, smanjenja zarada i sl. Na rizik se ne mora uvijek gledati kao na nešto negativno, ponekad on predstavlja šansu. Rizik se minimalizira pomoću analize vjerojatnosti budućih događaja na temelju prošlosti i tek se tada njime može upravljati, u suprotnom rizik donosi neizvjesnost pa ga nije moguće minimalizirati. Frank Knight je u svojoj knjizi dao odličan primjer rizika i neizvjesnost, za primjer je uzeo dvojicu kockara koji izvlače crnu i crvenu kuglicu iz posude. Kockar broj 1 ne zna koliko se crvenih i crnih kuglica nalazi u posudici, pa pretpostavlja da ih je jednak broj i da je vjerojatnost izvlačenja 50%/50%. Kockar broj 2 zna da na svake tri crvene dolazi jedna crna kuglica, uz tu informaciju točno izračunava vjerojatnost izvlačenja crvene kuglice. (Rak M. 2015.).

Dolazi se do zaključka da je kockar broj 1 zbog svojeg neznanja izložen neizvjesnosti, dok je sa druge strane kockar broj 2 izložen riziku s kojim se kroz analizu može upravljati. Prilikom upravljanja rizicima potrebno je proučiti njegov širi aspekt koji obuhvaća negativne ali i pozitivne rezultate. Teorija odlučivanja govori da se vjerojatnost nekog događaja kreće između jedan i nula. Jedan označava sigurnost događaja, a nula označava da je događaj nemoguć i baš se između te dvije točke nalazi rizik i neizvjesnost. Postoje rizici čija je vjerojatnost pojave jako mala, ali zato mogu jako naštetiti poslovanju organizacije, pa stoga oni spadaju pod visokorizične rizike.

1.1. Izvori rizika

Kako se svijet razvija tako je rizik sve više prisutniji. Riziku su izloženi pojedinci, organizacije i šira društvena zajednica. Postoje raznovrsni izvori rizika koji ugrožavaju živote, zdravlje, imovinu i prihode. William, Smith i Young (1998.) izvore rizika dijeli na:

- Fizičko okruženje
- Društveno okruženje
- Političko okruženje
- Pravno okruženje
- Operativno okruženje
- Ekonomsko okruženje

Okruženje na koje organizacija ne može utjecati je glavni izvor rizika. Povoljni klimatski uvjeti mogu pružiti priliku za razvoj poljoprivrede ili turizma. S druge strane prirodne katastrofe mogu uzrokovati ogromne gubitke. Društveno okruženje povezano je s djelovanjem društvenih čimbenika poput običaja, kulture, ponašanja, jezika i slično. Ti su čimbenici posebno važni u slučaju ulaska na nova tržišta. Kulturne razlike, različita shvaćanja, mogu predstavljati ogromne probleme, čak i velikim organizacijama. Događaji u regiji najbolji su pokazatelj kako političko okruženje može biti ključni izvor rizika. Dolazak novih političkih struktura može rezultirati novim poreznim propisima kao i promjenama u sustavu socijalne zaštite što može uzrokovati pojavu novih rizika. Donošenjem zakona stvara se okruženje za razvoj koji potiče cjelokupni razvoj zemlje. Druga strana je neprimjerenost zakona ili ljudi koji ga donose. Bez obzira da li se organizacija bavi proizvodnjom robe ili pruža usluge, operativno upravljanje u organizaciji značajno je utjecalo na rizike u poduzeću. Vrlo je važno kako je organizirana transformacija inputa, odnosno kako se donose odluke o kvaliteti učinkovitosti. U zemljama koje nemaju izraženu ekonomsku moć, ekonomsko okruženje se sve više povezuje sa političkim. Osim gubitka, postoje i drugi negativni aspekti rizika. „Naime, sama činjenica da postoji mogućnost da se dogodi nesreća zahtijeva racionalnu osobu da se na to pripremi.“ (Vujović,2009.). Jedan način za to je osigurati kod osiguravajućih društava, a drugi je stvoriti vlastiti rezervni fond iz kojeg će se pokrivati rizik. Ta sredstva donose veliki oportunitetni trošak jer su potrebni u trenutku nesreće. Rezervna sredstva čuvaju se u tekućem obliku, a prinos po njima u pravilu je jednak nuli.

2.2. Podjela rizika

Kao što i definicije, tako postoje i brojne podjele i vrste rizika. Prema Beškeru (2009.), rizici se dijele na unutarnje (direktni) i vanjske (indirektini) rizike.

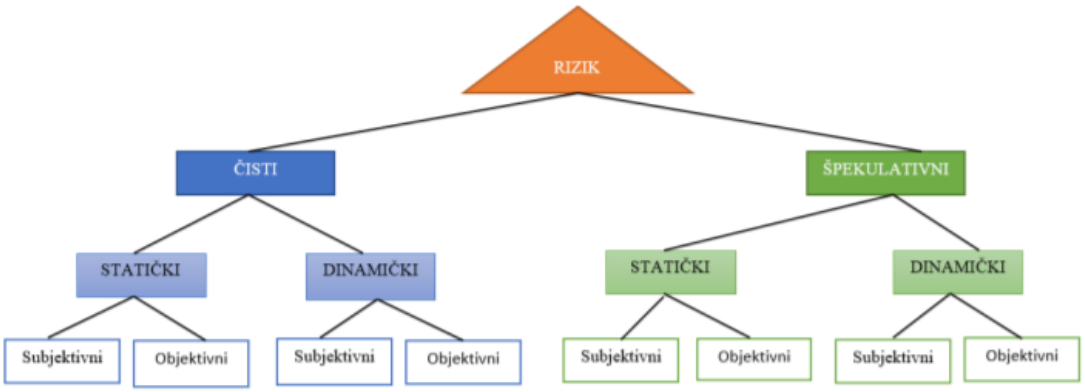
Direktni rizici dijele se na:

- Strategijske – politika, organizacije, upravljanje troškovima i dr.
- Upravljačke – sustav kontrole, radna atmosfera, organizacijska strukura i sl
- operativne - projektni rizici, sigurnost na rad,
- financijske rizike – kreditni, kamatni, fin.izvješaji.

S druge strane, vanjski rizici se dijele na:

- tržišne - tržišne novca, IT sektor
- političke – politička nestabilnost, štrajkovi, novi zakoni
- društvene – nastali iz međuljudske komunikacija na razini društvene skupine ili pojedinca.
- pravne – javlja se prilikom sklapanja ugovora, promjene pravnih i poreznih propisa
- rizike nastale elementarnom nepogodom.

Direktni rizici nastaju unutar organizacije, pa je uzrok njihova nastajanja unutar organizacije. Oni se mogu kontrolirati, mjeriti i nadzirati. Za razliku od direktni, indirektne rizike je teže kontrolirati, mjeriti i nadzirati. Indirektni rizici se moraju prihvatiti i smanjiti njihov učinak na organizaciju. Prema Young i Tippins (2001.) rizici se dijele na špekulativne i hazardne. Kod hazardnog rizika imamo samo jedan ishod, u najčešćem slučaju negativan ishod.



Slika.2.2. „Podjela rizika“, Izvor: Vujović R. (2009.) „Upravljanje rizicima i osiguranje“.

Kad je riječ o špekulativnim rizicima moguće je ostvariti dobit ili ostvariti gubitak. Klasičan primjer tome je kockanje, kartanje i sl. Sa svakim rizikom se može ostvariti dobiti ili gubitak, dok je kod hazardnog rizik moguć samo gubitak.

3.Upravljanje rizicima

Cilj procesa upravljanja rizicima je kontroliranje i mudro upravlja unutar svake organizacije u okviru svih aktivnosti. U idealnom upravljanju rizicima slijedi postupak određivanja prioriteta gdje se prvo rješavaju rizici s najvećim gubitkom i najvećom vjerojatnošću pojave, a kasnije se rješavaju rizici s nižom vjerojatnošću pojave i nižim gubitkom. U praksi proces upravljanja rizicima može biti vrlo rizičan, stoga je bitno da organizacija uspostavi ravnotežu između rizika s velikom vjerojatnošću nastanka, ali nižim gubitkom u odnosu na rizik s visokim gubitkom, ali nižom vjerojatnošću pojavljivanja često se može pogrešno rješavati. To je proces identifikacije, procjene i odgovaranja na rizike te pravovremenog informiranja o rezultatu tih procesa odgovarajućim strankama. Učinkovit sustav upravljanja rizicima:

- poboljšava postupke planiranja
- pruža uslugu smanjenja vjerojatnosti potencijalno skupih posljedica rizika i pomaže u pripremi neželjenih događaja i ishoda
- doprinosi boljoj raspodjeli resursa usmjeravajući ih tamo gdje su potrebni
- poboljšava učinkovitost i doprinosi razvoju pozitivne organizacijske kulture
- dodaje vrijednost kao ključnu sastavnicu donošenja odluka, planiranja, politike, uspješnosti i dodjele sredstava, kada se trajno poboljšavaju. (Veleučilište Velika Gorica, 2011.).

Prema normi ISO 31000:2018 kako bi poboljšale upravljanje rizikom organizacije moraju slijediti sljedeće korake:

1.uspostavljanje konteksta;
2. identificirati rizik;
3. analizirati rizik;
4. procjena rizika i
5. obrada rizika

3.1. Uspostavljanje konteksta

Prema normi ISO 31000:2018, organizacija mora uspostaviti kontekst strategije rizika u smislu unutarnjih i vanjskih čimbenika, vrste rizika, planova mjerenja i odgovarajućih procesa. Također se mora uzeti u obzir da strategija upravljanja rizikom nije samostalna u odnosu na druge aktivnosti organizacije te ona mora biti sastavni dio svakog područja poslovanja za učinkovito upravljanje rizikom. Važno je da se kontekst organizacije razvije kako bi bio pouzdan u utvrđivanju konteksta strategije rizika u njoj.

3.2. Identifikacija rizika

Rizici se odnose na događaje koji će, kada se pokrenu, izazvati probleme. Stoga utvrđivanje rizika može započeti s uzrokom problema ili sa samim problemom. Analiza izvora rizika može biti unutarnja ili vanjska, a ovisi o cilju upravljanja rizikom. Metode identifikacije sastoje se od utvrđivanje izvora, problema ili događaja. Rizik može utvrditi sljedećim metodama:

- Analiza postojećih podataka
- FMEA
- Mapiranje rizika
- Ankete
- Delfi metoda
- SWOT analiza
- Monte Carlo tehnika

3.3. Analiza rizika

„Analiza rizika je skup metoda i postupaka koji omogućuju potpunije razumijevanje problema u situacijama strateškog odlučivanja i pomažu da se pronađe zadovoljavajuća strategija prema unaprijed postavljenom kriteriju izbora. Strukturiranjem i modeliranjem problema odlučivanja rizik se identificira, odnosno dijagnosticira, zatim se izmjeri njegova veličina, te se konačno na temelju razmatranja razdioba (distribucija) vjerojatnosti ključnih varijabli, njihovih međusobnih utjecaja i očekivanih konačnih rezultata, može izvršiti izbor dostatno dobre strategije.“ (Kadlec Ž, Udovčić A., 2013.). Analizira se prema kvalitativnim i kvantitativnim metodama.

KVALITATIVNA ANALIZA	
PREDNOSTI	**NEDOSTATCI**
• „Relativno je brza i jednostavna. • Pruža bogat dijapazon informacija uz financijske utjecaje i vjerojatnosti, kao što su • ranjivost, vrijeme nastupanja, ali i nefinancijske učinke, kao što su zdravlje, sigurnost i • reputacija. • Lako je razumljiva velikom broju zaposlenih koji ne moraju poznavati sofisticirane kvantifikacijske tehnike.	• Ograničena je u razlikovanju razine rizika (vrlo visok, visok, srednji i nizak). • Neprecizna je. Rizični događaji unutar iste razine rizika mogu predstavljati značajno različite prijetnje rizika. • Ne može brojčano izraziti međuodnose i korelacije između identificiranih rizika. • Daje ograničenu mogućnost izvođenja studije isplativosti.
KVANTITATIVNA ANALIZA	
PREDNSOTI	**NEDOSTATCI**
• Omogućava numerička združivanja uzimajući u obzir međuodnose između identificiranih rizika pri uporabi mjera kao što je 'rizik novčanog tijeka'. • Omogućava provođenje studije isplativosti. • Omogućuje raspodjelu kapitala na temelju rizika na poslovne aktivnosti s optimalnim povraćajem rizika. • Pomaže izračunati kapitalne potrebe za održavanje likvidnosti u ekstremnim uvjetima	• Postupak analize može biti dugotrajan i skup, osobito u početnom tijeku razvoja modela. • Uz odabiranje neke novčane jedinice mjere, kao npr. dolar, može na godišnjem nivou dovesti do previđanja određenih kvalitativnih učinaka. • Pretpostavke nisu uvijek jasne.“

Tablica 3.3. „Kvalitativna i kvantitativna analiza“, Izvor: Izrada autora prema Baričević (2019.) Metode upravljanja rizicima - Visoka škola za inspekcijski i kadrovski Menadžment, Split.

Glavni izlazni dokument je prioritetna lista. Ona se formira na temelju izračuna statističke vjerojatnosti događaja i intenziteta utjecaja,a služi kako bi se kreirao dobar plan akcije, troškova i sl. Postoje razni računalni programski paketi koji mogu pomoći riješiti gore navedeno, ali sa takvim paketima organizacija treba biti vrlo oprezna, pogotovo prilikom interpretacije rezultata. Bitno je napomenuti da ti paketi ne daju cjelokupno rješenje, već vam ukazuje probleme i navodi vas do rješenja. Kada organizacija završi sa analizom bitno je da se sve prikupljene informacije dokumentiraju. Prema (Bulat, 2007) rizične investicije podrazumijevaju investicijske projekte, te kako bi se projekti realizirali potreban je dugotrajna i opsežna priprema metode analize rizika. Rizici se često vežu za kontrolu čiji je zadatak smanjiti rizike. Prema Crvarić (2019.) kontrola rizika obuhvaća:

- „procjenu rizika - kod procjene rizika bitno je prepoznati rizik, njegov izvor, procijeniti vjerojatnost nastanka i moguće posljedice prilikom nastanka rizika.
- upravljanje rizikom – je funkcionalna značajka dobrog menadžmenta, jer se zapravo provodi u svim hijerarskihim razinama organizacije
- komunikaciju rizika. - zadnji je korak plana upravljanja, a odnosi se na komunikaciju i razmjenu informacija tijekom analize rizika.

Proces analize rizika koristan je za djelotvoran i učinkovit rad i pružanje pomoći pri utvrđivanju rizika koji zahtijeva pozornost uprave. Čimbenici povezani sa zakonima i propisima nisu jednostavna opcija za bilo koju organizaciju. Prihvaćanje primjenjivih zakona i provedba sustava kontrole radi postizanja usklađenosti obvezni su čimbenici. Organizacija ima mogućnost financijske zaštite od učinka rizika koji uključuje osiguranje.

3.4. Procjena rizika

Norma ISO 31000:2018 zahtijeva da organizacija koristi postupak procjene rizika, kako bi se identificirali rizici kojima bi se organizacija mogla suočiti i s kojima se trenutno suočava. Norma ISO 31000:2018 opisuje procjenu rizika u širem smislu i korisna je za one koji nisu upoznati s ključnim načelima. Identifikacija potencijalnih rizika najbolje se postiže pristupom koji je nastao na temelju scenarija. Više o procjeni rizika bit će prikazano u ostatku rada.

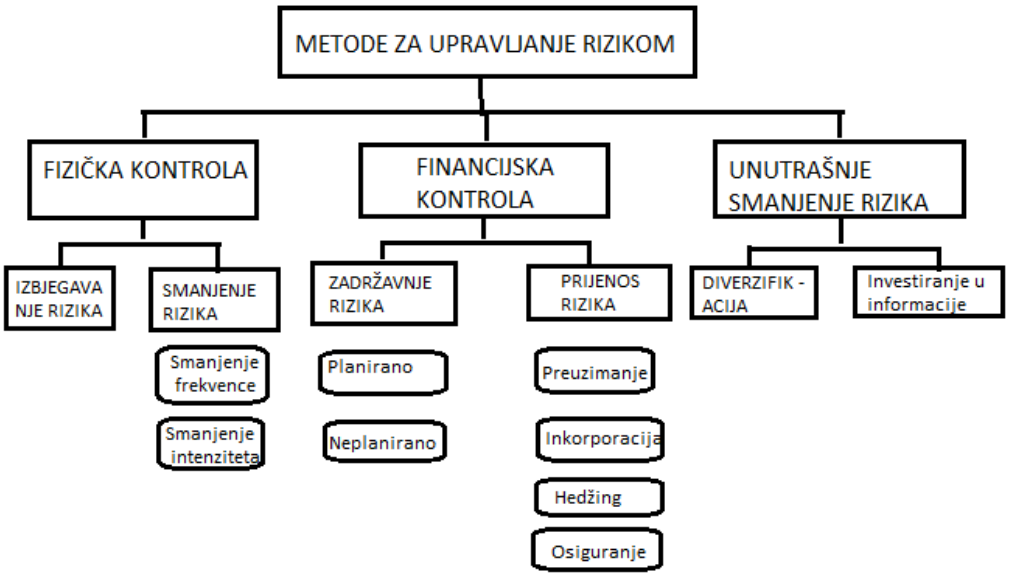
3.5. Obrada rizika

„Obrada rizika predstavlja izradu i primjenu specifičnih troškovno učinkovitih strategija i akcijskih planova za povećanje potencijalnih koristi i smanjenje potencijalnih troškova. Kada smo identificirali i procijenili rizike, sljedeći korak je razmatranje pristupa koji se mogu koristiti u upravljanju rizicima i odabir tehnike koja bi se trebala koristiti za svaki od njih. Taj se postupak zove obrada/tretman rizika.“ (Džolan, 2017.)

4.Metode upravljanja rizicima

Nakon identifikacije rizika kojima je organizacija izložena te određivanja njihovog utjecaja na novčane tokove organizacije i njegovu vrijednost, bitno je odlučiti što učiniti da bi ih izbjegli. Sljedeća slika prikazuje metode upravljanja rizikom.

Slika 4, Metode upravljanja rizicima,



Izvor: Izrada autora prema Vujović R, (2009.) „Upravljanje rizicima i osiguranje“

Kod metode fizičke kontrole postoje dva načina podjele a to su : izbjegavanje rizika i smanjenje rizika. Kod izbjegavanja rizika organizacija neće ostvariti svoju namjeru iz koje proizlazi rizik, te će na taj način potpuno izbjeći rizik, neće dopustiti da se bilo što dogodi. Što se tiče smanjenja rizika, organizacija pokušava smanjiti posljedice rizika koje se ne mogu izbjeći. Koriste ju velike organizacije. Kako bi eliminirale utjecaj rizika organizacije koriste aktivnosti smanjenja intenziteta.

Zadržavanje rizika i prijenos rizika su metode financijske kontrole organizacije. Kod zadržavanja rizika organizacija odluči zadržati i prihvatiti rizik koji dolazi uz određene aktivnosti npr. Određene proizvode. Razlog zadržavanja je taj da očekivani profit proizvoda je značajno veći od troška rizika. Kod planiranog zadržavanje rizika, menadžer je svjestan odabira, a sa druge strane kod neplaniranog zadržavanja, menadžer nije svjestan da postoji rizik. Prijenos rizika označava aktivnosti kod koje se rizik prenosi na drugu osobu ili organizaciju putem ugovora ili osiguranja.

Zadnja metoda upravljanja rizikom je unutrašnje smanjenje rizika, a ona se dijeli na diversifikaciju koja se koristi kako bi se zaštitila financijska situacija organizacije i na investiranje u informacije. Investiranjem se dobivaju najtočnije informacije o očekivanim rizicima, te se može smanjiti njihov utjecaj na novčani tok organizacije.

5.Norma ISO 22301:2019 Sigurnost i otpornost - sustavi upravljanja kontinuitetom poslovanja

„Norma ISO 22301:2019 je objavila sustav upravljanja koji je objavila Međunarodna organizacija za standardizaciju, a specificira zahtjeve za planiranje, uspostavljanje, implementaciju, upravljanje, praćenje, pregled, održavanje i kontinuirano poboljšanje dokumentiranog sustava upravljanja kako bi se zaštitili, smanjili vjerojatnost pojave, pripremili, odgovarali i oporavili od ometajućih incidenata kada oni nastaju. Namijenjen je primjeni na sve organizacije ili njihove dijelove, bez obzira na vrstu, veličinu i prirodu organizacije.“ (Adriacert, 2019.)

Organizacije koje implementiraju sustav upravljanja kontinuitetom poslovanja (BCMS) temeljene na zahtjevima i certificiraju ga normom ISO 22301:2019 mogu proći formalni postupak ocjenjivanja putem kojeg mogu dobiti akreditiranu potvrdu prema ovom standardu. Ovjereni BCMS internim i vanjskim dionicima pokazuje da se organizacija pridržava dobre prakse u upravljanju kontinuitetom poslovanja. „Slično ostalim ISO standardima za sustave upravljanja, zahtjevi navedeni u ISO 22301:2019 generički su i namijenjeni su primjeni na sve organizacije ili njihove dijelove, bez obzira na vrstu, veličinu i prirodu organizacije.“ (ibid). Međutim, opseg primjenjivosti zahtjeva ovisi o okolišu i složenosti organizacije.

Još u prošlosti, na mnoge organizacije ozbiljno su utjecale neočekivani rizici i katastrofe. Prekid poslovanja može dovesti do oštećenja i ne uspjeha Organizacije. Stoga je potrebno da sve organizacije uspostave i primijene sustav upravljanja kontinuitetom poslovanja (BCM) temeljen na ISO 22301:2019 koji odgovara njegovim potrebama. ISO 22301:2019 je međunarodna norma koja pomaže organizacijama da izrade kvalitetan plan kontinuiranog poslovanja. ISO 22301:2019 služi kako bi se organizacije zaštitile i brže oporavile ako dođe do problema. Također pomaže identificirati potencijalne prijetnje u poslovanju i izgraditi kapacitete za rješavanje nepredviđenih događaja. Može se smatrati jednim od najuspješnijih sveobuhvatnim pristupima koji pomažu organizacijskoj otpornosti. „ISO 22301:2019 temelji se na strukturi visokerazine koja je zajednički okvir za sve nove standarde sustava upravljanja. Organizacijama olakšava uključivanje sustava za upravljanje kontinuitetom poslovanja (BCMS) u osnovne poslovne procese, učinkovitost i veću uključenost višeg rukovodstva.“ (The British Standards Institution, 2019.).

Kontinuitet poslovanja je proces upravljanja, koji identificira potencijalne čimbenike koji prijete organizaciji i pruža okvir za izgradnju otpornosti i sposobnosti za učinkovit odgovor. Ovaj odgovor mora zaštititi interese svojih ključnih dionika, kao i reputaciju organizacije. Upravljanje kontinuitetom poslovanja predmet je kontinuiranog razvoja i istraživanja.

„Četiri su ključne poslovne prednosti koje tvrtka može postići primjenom norme osiguranja kontinuiteta poslovanja“ (Advisera,2019)

1) Pridržavanje zakonskih zahtjeva - sve je više zemalja koje definiraju zakone i propise koji zahtijevaju držanje propisa kontinuiteta poslovanja. Osim državnih interesa, privatne Organizacije također zahtijevaju od svojih dobavljača i partnera da implementiraju rješenja za kontinuitet poslovanja. Norma ISO 22301:2019 pruža savršen okvir i metodologiju za potporu poštivanju ovih zahtjeva.
2) Ostvarivanje marketinške prednosti – ako je tvrtka certificirana prema ISO 22301:2019, a konkurenti nisu, tvrtka će imati prednost nad njima kada su u pitanju kupci koji su osjetljivi na održavanje kontinuiteta svog poslovanja i isporuku svojih proizvoda i usluga. Uz to, takvo certificiranje može pomoći tvrtki da privuče nove kupce, što će dovesti do povećanog tržišnog udjela i veće dobiti.
3) Smanjenje ovisnosti o pojedincima - kritične aktivnosti Organizacije oslanjaju se na samo nekoliko ljudi koje je teško zamijeniti kada ti ljudi napuste organizaciju. Rukovoditelji koji su toga svjesni mogu iskoristiti prakse kontinuiteta poslovanja kako bi postali daleko manje ovisni o tim pojedincima.
4) Sprječavanje velikih šteta - u svijetu usluga i transakcija u stvarnom vremenu, svaka minuta usluge košta. Čak i ako poslovanje nije tako osjetljivo na mala razdoblja nedostupnosti, poremećaji koji ga ometaju mogu koštati organizaciju.

NOVO	KOMENTAR
Koristi od BCM-A	Prednosti BCM-A sada su uključene kao podtočka 1.2. tako da je korisnicima jednostavno da ih unaprijed identificiraju.
Klauzula 8.	Sadržaj operacija je redizajniran, dupliciranje uklonjeno, a terminologija pojednostavljena i dosljednija
Strategija kontinuiteta poslovanja	Klauzula 8.3. sada eksplicitnije ističe razmatranje strategije kontinuiteta poslovanja i rješenja
Manje propisiva dokumentacija i postupci	Uklanjaju se neki od dokumentiranih zahtjeva u pogledu informacija i imenovanih postupaka. To organizacijama daje veću slobodu i fleksibilnost pri uspostavljanju BCM-OVA tj. organizacije moraju provesti i održavati proces analize poslovnog učinka i procjene rizika, ali to više nije potrebno posebno dokumentirati
Promjene terminologije	Uključeni su novi uvjeti kao što su poremećaj i utjecaj. Uklanja se velika količina termina, te su neke definicije prilagođene
Planiranje	U stavku 6.1. dodaje se važna napomena mjerama za rješavanje rizika i prilika. Rizici i prilike se u ovoj pododredbi odnose na učinkovitost sustava upravljanja. Rizici povezani s poremećajem poslovanja razmatrani su u 8.2. Točka 6.2. sada se usredotočuje na planiranje postizanja ciljeva kako bi se osigurala

	kontinuirana aktivnost. Planiranje promjena BCM-OVA sada je uključeno kao nova odredba 6.3 kako bi se osiguralo obračunavanje promjena. Planovi i postupci sada su uključeni u odredbu 8.4. Konkretno, planovi se sada jasno povezuju s potporom timovima i ljudima koji će odgovoriti na prekid (točka 8.4.4.).
Uklonjena zaštita i ublažavanje	Podtočka 8.3.3. uklonjena je jer su vrlo slični zahtjevi u pogledu „tretmana rizika" sada uključeni u 8.3.2. Identifikacija strategija i rješenja.
Revizija upravljanja	Sada su uključeni eksplicitniji zahtjevi za ulaznim i izlaznim podacima revizije upravljanja.
Unutarnja revizija 9.2	unutarnja revizija sada ima više podstavki u kojima su navedeni zahtjevi što organizacije moraju.

Tablica 5. „Usporedba Norme ISO 22301 pije i sada", Izvor: Izrada autora prema The British Standards Institution, (2019.), 'ISO 22301 Business continuity management '[Internet], <raspoloživo na: https://www.bsigroup.com/globalassets/localfiles/en-au/ISO%2022301/22301%20Resources/iso-22301-business-continuity-mapping-guide-bsi0362-1911-au.pdf > [pristupljeno 1.9.2020.]

Certificiranjem sustav upravljanja kontinuitetom poslovanja SO 22301:2019 može se poboljšati poslovanje organizacije osiguravajući planirajući, učinkoviti BCM-a na svim razinama, uključujući:

- identifikaciju na razini organizacije i razumijevanje ključnih poslovnih procesa i mogućih rizika
- povećane razine otpornosti i sposobnosti otkrivanja te kontinuirani opstanak organizacije
- smanjen financijski učinak prilikom nastanka rizika
- bolji imidž.

„Fokus norme ISO 22301:2019 je osigurati kontinuitet isporuke proizvoda i usluga nakon pojave problema. To se postiže utvrđivanjem prioriteta kontinuiteta poslovanja, čiji potencijalni ometajući događaji mogu utjecati na poslovanje, definiranjem onoga što treba učiniti kako bi se spriječili takvi događaji, a zatim definiranjem načina oporavka minimalnog i normalne operacije u najkraćem mogućem roku. Stoga se glavna filozofija ISO 22301:2019 temelji na analizi utjecaja i upravljanja rizicima. Bitno je da otkrijte koje su aktivnosti važnije i koji rizici mogu utjecati na njih. Strategije i rješenja koja treba provesti obično su u obliku politika, postupaka i tehničke provedbe. U većini slučajeva organizacije nemaju na raspolaganju svu tehniku, stoga provedba ISO 22301:2019 uključuje ne samo postavljanje organizacijskih pravila, nego i planira tehničke i druge resurse kako bi se omogućio kontinuitet i oporavak poslovnih aktivnosti.“ (Adriacert, 2019.)

Ovaj dokument specificira strukturu i zahtjeve za uvođenje i održavanje Sustava upravljanja kontinuitetom poslovanja (BCMS) koji razvija kontinuitet poslovanja u skladu s količinom i vrstom utjecaja koji organizacija može ili ne mora prihvatiti nakon problema. BCMS naglašava važnost:

- razumijevanja potreba organizacije i nužnosti uspostavljanja politike i ciljeva kontinuiteta poslovanja;
- upravljanje i održavanje procesa
- praćenje i pregled izvedbe i učinkovitosti BCMS-a;
- neprekidno poboljšanje kvalitativnih i kvantitativnih mjera.

„BCMS kao sustav upravljanja, uključuje:

a) politiku

b) kompetentni ljudi s definiranim odgovornostima;

c) procese upravljanja koji se odnose na:

1) politiku;

2) planiranje;

3) provedbu i rad;

4) procjenu učinka;

5) pregled menadžmenta;

6) kontinuirano poboljšanje;

d) dokumentirane informacije koje podržavaju operativnu kontrolu i omogućuju procjenu izvedbe.“ (Međunarodna Organizacija za Standardizaciju ,2019.)

U normi se navode zahtjevi za provedbu, održavanje i poboljšanje sustava upravljanja radi zaštite od: smanjenja vjerojatnosti pojave, pripreme, odgovaranja i oporavka od rizika kada se pojave. Zahtjevi su namijenjeni za sve organizacije, bez obzira na vrstu, veličinu i prirodu organizacije. Opseg primjene tih zahtjeva ovisi o operativnom okruženju i složenosti organizacije. Norma se primjenjuje na sve vrste i veličine organizacija koje:

1. provode, održavaju i unapređuju BCM;
2. nastoje osigurati usklađenost s navedenom politikom kontinuiteta poslovanja;
3. su u mogućnosti nastaviti isporučivati proizvode i usluge tijekom krize;
4. nastoje povećati njihovu otpornost učinkovitom primjenom BCM-a. (Mravoić O.T., 2019.)

Ovaj dokument može se koristiti za procjenu sposobnosti organizacije da zadovolji vlastite potrebe i obveze kontinuiteta poslovanja

5.1.Struktura norme ISO 22301:2019 Sigurnost i otpornost – sustavi upravljanja kontinuitetom poslovanja

Norma ISO 22301:2019 se sastoji od sljedećih točaka:

„0) Uvod : objašnjava svrhu ISO 22301 i njegovu kompatibilnost s drugim standardima upravljanja.

- Općenito
- Prednosti sustava upravljanja kontinuitetom poslovanja
- Ciklus planiranja-provjere-provjere (PDCA)
- Sadržaj dokumenta

1) Opseg : objašnjava da je ovaj standard primjenjiv na bilo koju vrstu organizacije
2) Normativne reference : odnosi se na ISO 22300 kao standard gdje su dane definicije za neke izraze koji se koriste u ISO 22301
3) Pojmovi i definicije : ponovno se odnosi na ISO 22300.

4) Kontekst organizacije : ovaj je dio faze Plana u PDCA ciklusu i definira zahtjeve za razumijevanje vanjskih i unutarnjih problema, zainteresirane strane i njihove zahtjeve te definiranje opsega BCMS-a.

- 4.1 Razumijevanje organizacije i njezinog konteksta
- 4.2 Razumijevanje potreba i očekivanja zainteresiranih strana
- 4.3 Utvrđivanje opsega sustava upravljanja kontinuitetom poslovanja
- 4.4 Sustav upravljanja kontinuitetom poslovanja“ (Advisera, 2019.)

5) Vodstvo– ovaj dio odnosi se na:

- 1.„VODSTVO I PREDANOST- najviše rukovodstvo treba dokazati svoje vodstvo i predanost u pogledu BCM-a putem:

  - uspostave politike kontinuiteta poslovanja i ciljeva kontinuiteta poslovanja te usklađenost sa strateškim smjerom organizacije;
  - osiguranja integracije zahtjeva BCM-A u poslovne procese organizacije;
  - osiguravanja dostupnosti sredstava potrebnih za BCM;
  - priopćavanja važnosti učinkovitog kontinuiteta poslovanja i usklađenosti sa zahtjevima BCM-A;
  - osiguravanja da odabrana tržišta ugovora ostvare željene rezultate;
  - usmjeravanja i podupiranja osoba za doprinos učinkovitosti BCM-OVA;
  - promicanja kontinuiranog poboljšanja;
  - podupiranja drugih relevantnih upravljačkih uloga kako bi se pokazalo njihovo vodstvo i predanost kako se to odnosi na njihova područja odgovornosti.“ (ISO 22301:2019, 2019)

- 2. USPOSTAVU POLITIKE KONTINUITETA POSLOVANJA – prilikom uspostavljanja kontinuiteta poslovanja najviše rukovodstvo mora obratiti pažnju da politika upravljanja odgovara ciljevima organizacije.

- 3. ULOGE, ODGOVORNOSTI I OVLASTI – dodjeljuje ih najviše rukovodstvo

Od ključne su važnosti vodstvo i predanost BCM-u. BCM je nastao kao upravljačka disciplina, pomoću koje se može sveobuhvatno upravljati rizicima. Vrlo je bitno da organizacija ozbiljno shvati problem koji je nastao jer inače BCM neće biti učinkovit. Stoga je potrebno da organizacija osnuje odbor za kontinuitet poslovanja ili odbor za upravljanje rizicima, jer se na taj način lakše upravlja BCMS. Velike organizacije većinom imaju posebnog voditelja kontinuiteta poslovanja, dok se sa druge strane manje spajaju s postojećim upravljačkim položajem. Odgovorna osoba za BCM mora razumjeti sustave upravljanja i potrebu za kontinuitetom poslovanja.

6)Planiranje - razmatra se sljedeće:

1. Mjere za rješavanje rizika i prilika – utvrđuje se rizik i mogućnosti nastanka rizika i prilika
2. Ciljevi kontinuiteta poslovanja i njihovo planiranje
    - Uspostavljanje ciljeva kontinuiteta poslovanja -
    - utvrđivanje ciljeva kontinuiteta poslovanja
3. Planiranje promjena sustava upravljanja kontinuitetom poslovanja

BCM mora isplanirati sve moguće promjene, kako ne bi došlo do štetnog učinka. Najizraženiji dio je zahtjev za definiranje ciljeva za BCM i planiranje pristupa koji će organizacija zauzeti kako bi ih postigla. Ciljevi čine osnovu za kontinuirano unapređenje BCM-a. Norma sadrži posebne zahtjeve kako bi ciljevi trebali izgledati.

7)Potpora

Kao što je već spomenuto, za provedbu i održavanje BCM-a potrebni su resursi. Organizacije moraju uzeti u obzir osoblje, opremu i infrastrukturu i dr., a to ovisi čime se organizacija bavi. Normirani zahtjevi u pogledu stručnosti prilično su jednostavni, jer je samo potrebno provjeriti stručnost za projekt BCM, a zatim treba zaposliti novo stručno osoblje ili usavršiti postojeće. Kao što se uprava mora obvezati, svi ostali u organizaciji također moraju razumjeti zašto je kontinuitet poslovanja važan i koju ulogu imaju u osiguravanju učinkovitosti BCM-a. Za većinu zaposlenika trebalo bi biti dovoljno temeljno osposobljavanje, no za one zaposlenike s posebnim odgovornostima u pogledu plana vjerojatno će biti potrebna detaljnija izobrazba. Može biti korisno definirati te odgovornosti u opisima radnih mjesta i pregledati ih tijekom pregleda izvedbe. Ovaj dio standarda obuhvaća unutarnje ili vanjske komunikacije povezane s BCM-om. Interne komunikacije mogu uključivati obavješćivanje relevantnih

zaposlenika o promjenama u BCM-u. Upravljanje dokumentima ključna je komponenta svih sustava upravljanja. Ključne dokumente kao što su analize poslovnog učinka i, naravno, sam plan treba kontrolirati kako bi se osigurala primjena najnovije verzije. Isto vrijedi i za postupke, radne upute, procjene rizika i druge postupke koji čine jezgru BCM-a.

8) Opernacionalizacija

Ovaj dio standarda je jezgra norme ISO 22301:2019 – odjeljka koji definira procese i planove koji omogućuju kontinuitet poslovanja. Kao rezultat toga, to je najdulja pojedinačna sekcija u standardu. „Sadrži:

1. planiranje i kontrola;
2. analiza poslovnog učinka i procjena rizika;
3. strategije i rješenja za kontinuitet poslovanja;
4. planove i postupke kontinuiteta poslovanja;
5. programi vježbanja; i
6. ocjena dokumentacije i sposobnosti kontinuiteta poslovanja i sposobnosti.“ (Advisera,2019)

a) Proces planiranja i kontrole

Proces planiranja je proces odlučivanja načina na koji će se pristupiti za rješavanje rizika i na koji način će se provoditi aktivnosti bitne za organizaciju. Planiranje je bitno kako bi se osiguralo da organizacija na najbolji način upravlja rizicima Plan planiranja upravljanja rizicima je potrebno napraviti na početku faze planiranja.

b) Analizu poslovnog učinka

Kako bi organizacija razvila plan upravljanja kontinuitetom poslovanja, najprije mora razmotriti i razumjeti učinak koji bi se dogodio ako poslovne aktivnosti proizvodnje budu prekinute. Postizanje toga na sustavan, ponovljiv način je smisao analize poslovnog utjecaja (BIA - Business impact analysis). Norma opisuje proces analize poslovnog utjecaja (BIA) u nizu koraka. Potrebno je utvrditi koliko je organizacija sprema tolerirati prekide proizvodnje. To je poznato kao cilj vremena oporavka (RTO – Recovery time objective). RTO je osnova na kojoj su prioritet aktivnosti oporavka – što je RTO kraći, to je prioritet veći. Kao i ostatak BCM-a, BIA je ponavljajuća aktivnost.

Učestalost provedbe pregleda BIA ovisi o organizaciji, no ona bi se uvijek trebala provoditi nakon svake velike promjene u načinu rada organizacije.

c) Procjena rizika

Procjena rizika cjelokupni je postupak utvrđivanja rizika, analize rizika i evaluacije rizika. Procjena rizika trebala bi se provoditi sustavno, ponavljajući na temelju znanja i stajališta organizacije. Treba se koristiti najboljim dostupnim informacijama i, prema potrebi, dodatnim upitima. Procjena rizika se koristi kako bi se na temelju dobivenih rezultata procjene utvrdilo gdje organizacija treba dodatno djelovati. To može dovesti do odluke da organizacija:

- ne učini više ništa;
- razmotri opcije za obradu rizika;
- provede dodatnu analizu;
- održavati postojeće kontrole;

Pri donošenju odluka sagledava se širi kontekst te stvarne i uočene posljedice za vanjske i unutarnje dionike. Ishod procjene rizika treba evidentirati, priopćiti i potom potvrditi na odgovarajućim razinama organizacije.

d) Strategije rješenja kontinuiteta poslovanja

Potrebno je razlikovati strategije i rješenja. Strategije provođenja kontinuiteta poslovanja su dugoročni planovi koji se koriste za postizanje ciljeva kontinuiteta poslovanja, a rješenja su način na koji se implementiraju te strategije i ostvaruju ciljevi. Organizacija treba biti sigurna da su rješenja koja se primjenjuju prije, tijekom i nakon nastanka problema doista učinkovita. Također treba identificirati, odabrati i provesti strategije i rješenja kontinuiteta poslovanja, te osigurati resurse na koje se ta rješenja oslanjaju.

e) Planovi i postupci kontinuiteta poslovanja

Kao osnovna komponenta BCM-A, planiranje kontinuiteta poslovanja (BCP - Business Continuity Planning) koristi sve informacije određene u ranijim odjeljcima standarda. Međutim, plan nije samo jedan dokument, nego se sastoji od nekoliko dijelova, od kojih svi rade zajedno kako bi osigurali učinkovitu obnovu organizacije.

Plan kontinuiteta poslovanja uključuje:

- Postupke upravljanja kontinuitetom poslovanja – plan upravljanja kontinuitetom poslovanja mora biti potkrijepljen postupcima koji detaljno opisuju radnje potrebne za oporavak. Norma ISO 22301:2019. opisuje zahtjeve za te postupke, uključujući one koji se često zanemaruju: fleksibilnost. Kada se dogode štetni incidenti, oni su rijetko onakvi kakve organizacija želi prilikom planiranja za njih, a prerestriktivni postupci mogu izazvati probleme u trenutku. Zbog toga organizacija treba omogućiti određeni stupanj fleksibilnosti u postupcima odgovora. Štetni događaji mogu utjecati i na komunikaciju, a osobito u početnim fazama, obično ih prati mala količina stresa i zabuna. Jasna i sažeta procedura dugoročno osigurava nesmetan oporavak.
- Struktura odgovora – odnosi se na tim ili timove koji usmjerava, vodi i provodi aktivnosti odgovora i oporavka. Tim treba obuhvaćati kompetentne ljude za donošenje odluka o mjerama odgovora. Treba uključiti osoblje iz svih glavnih područja organizacije kako bi se osigurao najširi mogući raspon iskustva i znanja u slučaju incidenta. Svaki član bi trebao razumjeti i procijeniti utjecaj rizika na njegovo područja stručnosti i odabrati odgovarajuće mjere.
- Upozorenje i komunikacija – organizacija treba razviti procedure za komunikaciju sa zainteresiranim stranama i odgovaranje na njih o štetnim incidentima i radnjama koje poduzima kako bi se oporavila od njih. Standard također zahtijeva da se razvije proceduru koja će osigurati da sredstva komunikacije ostanu na raspolaganju tijekom štetnih događaja. Čak će i najbolje postavljeni komunikacijski planovi propasti ako uopće ne postoji komunikacija.

Pri izradi planova kontinuiteta bitno je izraditi plan za više mogućih scenarija. Planovi trebaju biti jasni i specifični te se izravno odnositi na unaprijed definirane pragove za aktiviranje plana. Također bi trebalo utvrditi kada se planovi mogu deaktivirati, kako se provodi izvješćivanje, uloge i odgovornosti osoba uključenih u provedbu plana, procese koji se moraju koristiti i sve popratne informacije.

f) Program vježbe

Nije dovoljno razvijati planove i jednostavno pretpostaviti da će oni raditi kada budu raspoređeni, mnoge se teškoće otkrivaju samo u tome. Standard zahtijevaj da organizacija periodično testira svoje planove. Vježbe jednom ili dvaput godišnje tipične su, čiji bi ishod trebalo zabilježiti i ocijeniti kako bi se utvrdila sva pitanja ili nedostaci i provela poboljšanja.

g) Procjena dokumentacije i sposobnosti kontinuiteta poslovanja

Ovaj dio standarda zahtijeva da organizacija evaluira i poboljša svoju dokumentaciju i mogućnost oporavka, te da se ne miješa sa sljedećim odjeljkom, koji se fokusira na ocjenjivanje i unapređenje samog BCM-a. Same planove i dokumentaciju na koju se oslanjaju, uključujući BIA, procjene rizika, postupke, mjere za osiguravanje pravne usklađenosti itd., trebalo bi periodički evidentirati, neovisno o tome koriste li se planovi ili ne. Također bi ih trebalo preispitati nakon svake aktivacije plana i nakon svih značajnih promjena organizacije i načina na koji on djeluje. Također treba izmjeriti aspekte plana i pripadajuću dokumentaciju, itd. koja se smatra korisnom za poboljšanje.

9) Procjena učinka

Svi sustavi upravljanja uključuju procjenu učinkovitosti kako bi se potaknulo poboljšanje. To se postiže kombinacijom sljedećeg:

1. praćenje, mjerenje, analiza i procjena.
2. unutarnja revizija.
3. pregled upravljanja.

ISO 22301:2019 postavlja zahtjeve organizaciji kako bi odredila što treba pratiti i kako se provode mjerenja i analiza. Organizacija ne mora mjeriti svaki aspekt BCM-a., nego se treba usredotočiti na korisne informacije. U praksi to obično znači definiranje ključnih pokazatelja uspješnosti za BCM, kao što su učestalost pregleda i ažuriranja procjene rizika . Nije dovoljno samo prikupiti dokumentaciju već organizacija mora procijeniti i analizirati prikupljene podatke.

Rezultat analize pokreće akciju poboljšanja, pa ako trend u ukupnom vremenu oporavka pokaže da vrijeme oporavka raste, tada se istražuje uzrok i poduzimaju se radnje za ublažavanje rizika. Revizije su još jedno zajedničko obilježje sustava upravljanja i BCM-a.

Završna komponenta procjene učinkovitosti još je jedan čimbenik zajednički svim sustavima upravljanja. Mora uključivati stavke navedene u standardu, kao što su trendovi u praćenju i rezultati mjerenja, učinkovitost u odnosu na BCM ciljevi, promjene organizacije koje bi mogle utjecati na BCM, rizike i prilike itd. Revizijom se također moraju prikazati stavke koje zahtijeva standard. Pregled i njegove ulazne podatke i izlazne rezultate treba zabilježiti tako da se može pratiti i poboljšati razvoj BCM. Revizija upravljanja obvezan je dio nadzora koji provode certifikacijska tijela, stoga je važno osigurati da se svaki zahtjev obračunava.

10) Poboljšanje

„Rezultati metoda ocjenjivanja učinkovitosti izravno ulaze u poboljšanje BCM-a na dva načina:

1. nesukladnost i korektivne mjere.
2. kontinuirano poboljšavanje.“ (ISO 22301:2019, 2019.)

Neusklađenost i korektivne mjere ukazat će na nesukladnosti u BCM-u. Nalazi revizorskog izvješća povezani su s korektivnom radnjom koja navodi nesukladnost, uzrok i predloženo rješenje. Rješenje se primjenjuje i preispituje naknadno kako bi se osiguralo njegovo djelovanje. Važno je napomenuti da rijetki sustavi upravljanja ostaju savršeni tijekom vremena jer kako se organizacija i sustav upravljanja razvijaju, očekuju se nesukladnosti. Nesukladnosti bi općenito trebalo promatrati kao priliku za poboljšanje BCM-a umjesto kao nešto negativno. Uobičajeno je da se nesukladnosti dodjeljuju jednoj od tri kategorije koje opisuju ozbiljnost pitanja:

1. Veća – ove nesukladnosti općenito se odnose na potpuni izostanak zahtjeva ili produljenog ili namjernog neispunjavanja zahtjeva.
2. Manje – te se nesukladnosti općenito odnose na zahtjeve koji su djelomično ¸ zadovoljeni, ali imaju nedostatke
3. Prilika za poboljšanje – općenito ukazuje na sada prihvatljivu situaciju, ali to bi moglo rezultirati problemom u budućnosti.

Kontinuirano poboljšanje - znači da se uvijek mora tražiti načine za poboljšanje BCMa. To se može postići pod uvjetom da je revizija i korektivne mjere, mjerenje i analiza, pregled menadžmenta itd. učinkoviti i da postoji dobra komunikacija između tima za upravljanje

krizama, vrhunskog menadžmenta i ostatka organizacije koja omogućuje postavljanje i ispravljanje problema.

Prednosti certificiranja ISO 22301:2019.:

- Održava poslovanje u slučaju prekida
- Zaštićuje imovinu,promet i dobit
- Povećati konkurentsku prednost i poboljšati korporativni ugled
- Smanjuje troškove osiguranja od prekida poslovanja

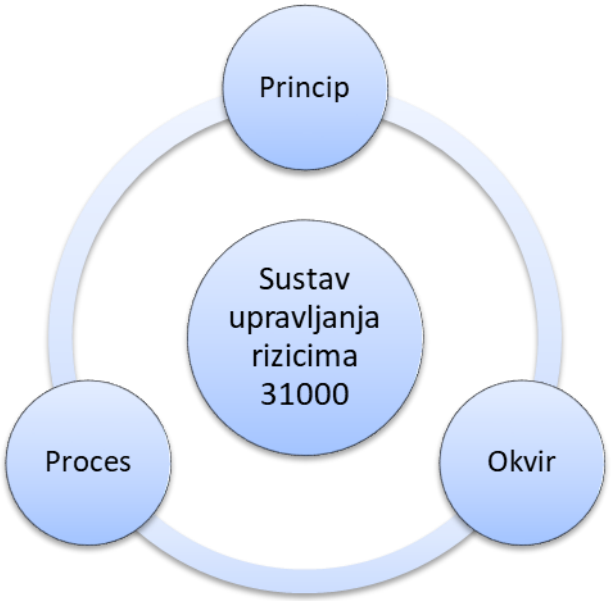
6.Norma ISO 31000:2018 sustav upravljanja rizicima

„Postoji mnogo mišljenja koja se odnose na to što upravljanje rizikom treba obuhvatiti, kako da se implementira i što može postići. Međunarodna organizacija za normizaciju ISO preko norme ISO 31000:2018 Upravljanje rizicima - načela i smjernice o primjeni nastoji odgovoriti na postavljena pitanja. Treba odmah napomenuti da ova norma nije predviđena za certifikaciju. To znači da se prema njoj ne može vršiti certificiranje organizacija koje je primjenjuju. Ovo proizlazi iz činjenice da se u njoj ne nalaze nikakvi zahtjevi koji se moraju primijeniti za uspostavu sustava upravljanja rizicima u organizaciji.“ (Sekulić ,2016.). Norma ISO 31000: Upravljanje rizikom, izvorno je objavljena 2009. godine, a ažurirana verzija objavljena je u veljači 2018. godine. Međutim, ukupna namjena norme ISO 31000:2018 ostaje ista – uključivanje upravljanja rizicima u strateški sustav upravljanja. Verzija 2018. je vrlo slična originalnoj verziji, ali glavne promjene su:

- Ispitana su načela upravljanja rizicima;
- istaknuta je važnost rukovođenja najvišim rukovodstvom, kao i integracija upravljanja rizicima, počevši od upravljanja organizacijom;
- veći naglasak stavlja se na upravljanja rizicima, jer je novo znanje i analiza vođeno revizijom procesa, postupaka i kontrola;
- sadržaj je pojednostavljen s više otvorenih sustava.

Norma nije namijenjena za certifikaciju, što bi značilo da se norma ne sastoji od pravila i zahtjeva koje organizacija mora primjenjivati, nego se pomoću nje mogu smanjiti rizici u poslovanju i time poboljšati samo poslovanje. „Generički pristup upravljanju rizicima koji promovira norma ISO 31000:2018 ne zavisi od područja primjene, a koncepcijski pruža kvalitetnu osnovu za analizu, procjenu te obradu rizika. U okviru te norme procjena rizika ne tretira se u metodološkom smislu, pa generički pristup omogućava da se proces upravljanja rizicima bez poteškoća primjeni u bilo kojem području, bilo da se radi o procesima sigurnosti nekom drugom poslovnom procesu ili društvenim procesima.“ (Buntak, K., Kovačić, M. 2020.). Norma zapravo govori kako upravljene rizikom treba prestati gledati kao na zasebnu djelatnosti i početi primjenjivati u svim segmentima.

Norma ISO 31000:2018 se sastoji se od tri sastavne cjeline koju su međusobno povezane, te kako bi sustav funkcionirao moraju biti u međusobnoj interakciji.



Slika 6. „Sustav upravljanja rizicima“, Izvor: izrada autora prema ISO 31000:2018.

„Norma ISO 31000:2018 preporučuje da organizacije razvijaju, provode i neprekidno poboljšavaju okvir kojemu je svrha integracija procesa za upravljanje rizikom u sveukupno upravljanje organizacijom, u strategiju i planiranje, u upravljanje, u procese izvješćivanja, politike, vrijednosti i kulturu.

Prihvaćanje usklađenih procesa upravljanja rizikom može pomoći da se u organizaciji rizikom upravlja djelotvorno i usklađeno. Generički pristup opisan u normi ISO 31000:2018 daje načela i upute za upravljanje svakim oblikom rizika na sustavan, razvidan i vjerodostojan način, u svakome području primjene i u svakome kontekstu.“ (Crvarić,2019.) . Stoga je norma ISO 31000:2018 ključna za utvrđivanje konteksta, koji je bitan za početak upravljanja rizikom. Utvrđivanje konteksta obuhvaća ciljeve organizacije, vanjsko okruženje, njezine dioničare te posebne kriterije rizika.

Struktura upravljanja rizikom razlikuju se ovisno o svrsi, ciljevima i složenosti organizacije. Rizikom se upravlja u svakom dijelu strukture organizacije. Svatko u organizaciji ima odgovornost za upravljanje rizikom. Upravljanje usmjerava tijek organizacije, njezine vanjske i unutarnje odnose te pravila, procese i prakse potrebne za postizanje njezine svrhe.

Upravljačke strukture prevode smjer upravljanja u strategiju i povezane ciljeve potrebne za postizanje željenih razina održivog učinka i dugoročne održivosti.
Utvrđivanje odgovornosti za upravljanje rizikom i nadzorne uloge unutar organizacije sastavni su dijelovi upravljanja organizacijom. Integriranje upravljanja rizicima u organizaciju dinamičan je i ponavljajući proces te ga treba prilagoditi potrebama i kulturi organizacije.

6.1 Načela norme ISO 31000:2018

ISO 31000:2018 navodi da je svrha upravljanja rizicima stvaranje i zaštita vrijednosti. U načelima navedenima u normi ISO 31000:2018 daju se smjernice o obilježjima učinkovitog i efektivnog upravljanja rizikom, naglašava se njegova vrijednost i objašnjava njegova namjena i svrha. U normi je prikazano ukupno „osam načela:

1. cjelovitost,
2. strukturiranost i sveobuhvatnost,
3. prilagodljivost,
4, uključivost,
4. dinamičnost,
6, najbolju informiranost,
7. ljudske i kulturne čimbenike i
8. neprekidno poboljšavanje.“ (Svijet kvalitete, 2018.)

Prvih pet načela daju smjernice o tome kako bi se trebala osmisliti inicijativa za upravljanje rizicima, a načela sedam i osam odnose se na djelovanje inicijative za upravljanje rizicima. Prema zadnjim principima može se zaključiti da je vrlo bitno primjenjivati informacije koje su dostupne organizaciji, a mehanizmi upravljanja rizicima trebali bi osigurati kontinuirano poboljšanje.

6.2.Okvir norme ISO 31000:2018.

Načela upravljanja rizicima i okvir usko su povezani. Na primjer, jedno od načela je da upravljanje rizicima treba biti integrirano, a jedna od komponenti okvira je integrirana. Princip navodi što se mora postići i okvir pruža kako postići. Smjernice ISO 31000:2018 usredotočene su na vodstvo i predanost. Preostale komponente okvira su projektiranje, implementacija, evaluacija i unapređenje.

Ovaj pristup često se prikazuje u literaturi upravljanja kao plan-do-check-act. On jamči da će se prikupljene informacije o riziku implementirati na primjeren način za organizaciju. ISO 31000:2018 stavlja veliki naglasak na razumijevanje organizacije i njezina konteksta. Daju se informacije o tome kako ispitati vanjski i unutarnji kontekst organizacije. Također postoje savjeti i smjernice o artikuliranju predanosti upravljanju rizicima, dodjeljivanju odgovornosti i dodjeljivanju sredstava. U rubrici ISO 31000:2018 nalaze se smjernice za uspostavu komunikacije i konzultanata s detaljnijim informacijama u procesnoj sekciji smjernica. Stoga smjernice o komunikaciji i savjetovanju u okvirnom odjeljku treba pročitati u skladu sa smjernicama o istoj temi u poglavlju procesa ISO 31000:2018. Razumijevanje organizacije i njezina konteksta uključeno je kao dio okvirnih smjernica u normi ISO 31000:2018. Komponente osnivanja konteksta opisane su kao definicije prema kojima se uređuje svrha i opseg aktivnosti upravljanja rizicima; uspostavlja vanjski, unutarnji i kontekst upravljanja rizicima. Šest je sastavnih cjeline koju su međusobno povezane, te kako bi sustav funkcionirao moraju biti u međusobnoj interakciji. Prema normi ISO 31000:2018, okvir upravljanja rizicima se sastoji od:

1. VODSTVA I PREDANOSTI - Najviša upravljačka tijela i nadzorna tijela trebala bi, prema potrebi, osigurati da upravljanje rizicima bude integriran u sve organizacijske aktivnosti i trebao bi demonstrirati vodstvo i predanost:

    - prilagođavanje i provedba svih komponenti okvira;
    - izdavanje izjave ili politike kojom se uspostavlja pristup, plan ili tijek djelovanja upravljanja rizicima;
    - osiguravanje da se potrebna sredstva dodijele upravljačkom riziku;
    - dodjeljivanje ovlasti, odgovornosti i odgovornosti na odgovarajućim razinama unutar organizacije.

To će pomoći organizaciji da uskladi upravljanje rizicima sa svojim ciljevima, strategijom i kulturom, prepozna i riješi sve obveze, utvrdi iznos i vrstu rizika koji se mogu ili ne moraju poduzeti kako bi se vodio razvoj rizika. Uprava je zadužena za upravljanje rizicima, dok su nadzorna tijela odgovorna za nadzor.

Od nadzornih tijela često se očekuje ili se od njih zahtijeva da:

- osiguraju da se rizici primjereno razmotre pri utvrđivanju ciljeva organizacije;
- prepoznaju rizike organizacije;
- osiguraju da se sustavi za upravljanje takvim rizicima provode i učinkovito djeluju;
- osiguraju da su takvi rizici primjereni u kontekstu ciljeva organizacije.

Najviše rukovodstvo odgovorno je za upravljanje rizikom, dok su nadzorna tijela odgovorna za nadzor upravljanja rizikom. Često se od nadzornih tijela očekuje ili traži da:

- osiguraju da se rizici uzmu u obzir prilikom postavljanja ciljeva organizacije;
- razumiju rizike;
- osiguraju da se sustavi za upravljanje takvim rizicima provode i djeluju učinkovito;
- osiguraju da su takvi rizici primjereni u kontekstu ciljeva organizacije;
- osiguraju da se informacije o takvim rizicima i njihovom upravljanju pravilno komuniciraju.

2. INTEGRACIJE

Integracija se oslanja na razumijevanje organizacijskih struktura i konteksta. Struktura se može razlikovati ovisno o svrsi organizacije, ciljevima i složenosti organizacije. Rizikom se upravlja svakim dijelom organizacije te svatko ima odgovornost za upravljanje rizikom. Integraciju upravljanja rizicima potrebno je prilagoditi potrebama i kulturi organizacije.

Upravljanje usmjerava tijek organizacije, njezine vanjske i unutarnje odnose te pravila, procese i prakse potrebne za postizanje njezine svrhe. Upravljačke strukture prevode smjer upravljanja u strategiju i povezane ciljeve potrebne za postizanje željenih razina održivog učinka i dugoročne održivosti. Utvrđivanje odgovornosti za upravljanje rizikom i nadzorne uloge unutar organizacije sastavni su dijelovi upravljanja organizacijom. Upravljanje rizikom trebao bi biti dio organizacijske svrhe.

3. DIZAJNA

Dizajn sustava upravljanja rizicima sastoji se od:

- Razumijevanja organizacije i njezina konteksta - ispitivanje vanjskog konteksta organizacije (unutarnje i vanjske čimbenike, ključnih pokretača i trendove koji utječu na ciljeve organizacije, ugovorne odnose i obveze, složenost mreža i ovisnosti isl.) i ispitivanje unutarnjeg konteksta organizacije (vizija i misija, strategija,ciljevi i politike, kultura organizacije i sl.)
- Naglašavanje obveze upravljanja rizicima - najviša upravljačka tijela i nadzorna tijela trebala bi pokazati njihovu predanost kroz izjavu u kojoj objašnjavaju ciljeve organizacije i prikazuju predanost upravljanju rizicima.
- Dodjeljivanje organizacijskih uloga, ovlasti i odgovornosti – Najviši menadžment trebao bi se pobrinuti da se nadležnim tijelima dodijele uloge pri upravljanju rizicima.
- Dodjela resursa - Najviša upravljačka i nadzorna tijela trebala bi, prema potrebi, osigurati dodjelu odgovarajućih sredstva za upravljanje rizicima, koja mogu uključivati.
- Uspostava komunikacije i savjetovanje - organizacija bi trebala uspostaviti komunikaciju kako bi olakšala prilagodbu na rizike i njihovo upravljanje. upravljanja rizicima. (ISO, 2019.)

Prilikom dizajniranja okvira, organizacija ima zadatak proučiti svoj vanjski i unutarnji kontekst. Kod ispitivanja vanjskog konteksta, organizacija mora pripaziti na:

- socijalne kulturne, političke i dr. čimbenike;
- nove trendove koji mogu imati utjecaj na organizaciju;
- odnose, percepcije, vrijednosti, potrebe i očekivanja vanjskih dionika;
- ugovorne odnose i obveze;
- složenost mreža i ovisnosti.

Ispitivanje unutarnjeg konteksta organizacije sastoji se od:

- vizije, misije i vrijednosti;
- upravljanja, organizacijske strukture;
- strategije, ciljeva i politike;
- kulture organizacije;
- iskoristivosti resursa i znanja
- podataka, informacijskih sustava i informacijskih tokova;
- odnosa s unutarnjim dionicima, uzimajući u obzir njihove percepcije i vrijednosti;
- ugovornih odnosa i obveza;
- međuovisnosti i međusobne veze.

Tijela najvišeg menadžmenta i nadzora, tamo gdje je to primjenjivo, trebaju pokazati i definirati svoju trajnu predanost upravljanju rizicima politikom, izjavom ili drugim oblicima koji jasno prenose ciljeve i predanost organizacije upravljanju rizicima. Obveza treba sadržavati, ali nije ograničena na:

- svrhu organizacije za upravljanje rizikom i veze s njezinim ciljevima i drugim politikama;
- jačanje potrebe za integriranjem upravljanja rizicima u ukupnu kulturu organizacije;
- vođenje integracije upravljanja rizicima u osnovne poslovne aktivnosti i donošenje odluka;
- ovlasti, odgovornosti i odgovornosti;
- stavljanje na raspolaganje potrebnih resursa;
- način na koji se rješavaju sukobljeni ciljevi;
- mjerenje i izvještavanje u okviru pokazatelja uspješnosti organizacije;
- pregled i poboljšanje. (ISO,2019.)

Predanost upravljanju rizicima treba priopćiti unutar organizacije i dionicima, prema potrebi. Vrhovna uprava i nadzorna tijela, tamo gdje je to primjenjivo, trebala bi osigurati da se

ovlasti, odgovornosti i odgovornosti za relevantne uloge u pogledu upravljanja rizicima dodijele i komuniciraju na svim razinama organizacije, te bi trebale:

- „naglasiti važnost upravljanja rizikom;
- pronaći pojedince koji imaju sposobnosti da upravljaju rizikom“ (ISO,2019)

Vrhovna uprava i nadzorna tijela, tamo gdje je to primjenjivo, trebala bi osigurati raspodjelu odgovarajućih resursa za upravljanje rizikom. Organizacija bi trebala razmotriti mogućnosti i ograničenja postojećih resursa. Također, organizacija bi trebala uspostaviti odobreni pristup komunikaciji i savjetovanju kako bi podržala okvir i olakšala učinkovitu primjenu upravljanja rizicima. Komunikacija uključuje razmjenu informacija s ciljanom publikom. Savjetovanje također uključuje sudionike koji daju povratne informacije s očekivanjem da će pridonijeti i oblikovati odluke ili druge aktivnosti. Metode i sadržaj komunikacije i savjetovanja trebaju odražavati očekivanja dionika, tamo gdje je to potrebno. Komunikacija i savjetovanje trebaju biti pravovremeni i osigurati da se relevantne informacije prikupljaju, uspoređuju, sintetiziraju i dijele, prema potrebi, te da se daju povratne informacije i vrše poboljšanja.

4. IMPLEMENTACIJA

Organizacija mora implementirati okvir upravljanja rizicima kroz razvoj odgovarajućeg plana, utvrđivajući gdje, kako i kada se donose odluke i dr. Kako bi implementacija bila uspješna potrebno je angažirati i dionike.

Organizacija mora implementirati okvir upravljanja rizikom na način da:

- razvija odgovarajući plan;
- utvrđuje gdje, kada i kako u organizaciji donose različite vrste odluka i tko ih donosi;
- modificira primjenjivanje postupaka donošenja odluka po potrebi;
- osigura da se aranžmani organizacije za upravljanje rizicima jasno razumiju i prakticiraju

Uspješna provedba okvira zahtijeva angažman i svijest dionika. To omogućuje organizacijama da se izričito bave nesigurnošću u donošenju odluka, istovremeno osiguravajući da se svaka nova ili kasnija nesigurnost mogu uzeti u obzir čim se pojave. Ispravno osmišljen i implementiran, okvir upravljanja rizicima osigurat će da postupak upravljanja rizikom bude dio svih aktivnosti u cijeloj organizaciji, uključujući donošenje odluka, te da će promjene u vanjskom i unutarnjem kontekstu biti na odgovarajući način zabilježene.

5. PROCJENA

Kako bi mogla procijeniti učinkovitost okvira organizacija treba mjeriti učinak okvira upravljanja rizicima u odnosu na njegovu svrhu, planove provedbe, pokazatelje i očekivano ponašanje. „Prilikom osmišljavanja okvira za upravljanje rizicima, organizacija bi trebala proučiti i razumjeti vanjski (vanjske zainteresirane strane, socijalne, zakonske, tehnološke i druge faktore...) i unutarnji kontekst (vizija, misija, vrijednosti, strategija, ciljevi, organizacijska kultura...) organizacije. Ne postoji jedinstveni način implementacije sustava upravljanja rizicima.“ (Puškadija, 2029.)

6. POBOLJŠANJE

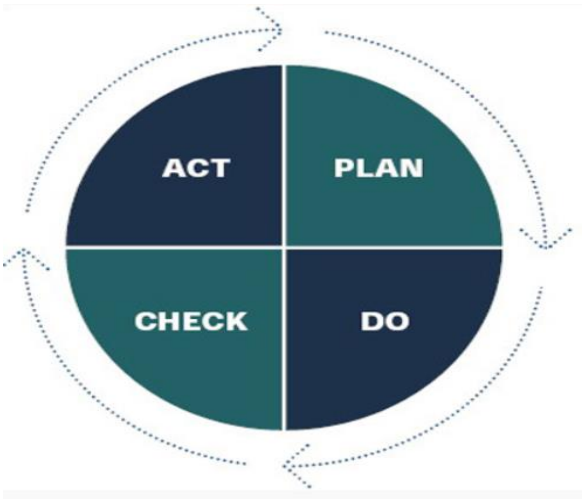
Organizacija bi trebala stalno pratiti i prilagođavati okvir upravljanja rizicima jer samim time poboljšava svoju vrijednost. Također, organizacija bi trebala kontinuirano poboljšavati prikladnost i učinkovitost okvira upravljanja rizicima. Organizacija bi trebala kontinuirano nadzirati i prilagođavati okvir upravljanja rizicima kako bi se pozabavila vanjskim i unutarnjim promjenama. Pritom organizacija može poboljšati svoju vrijednost.

Organizacija bi trebala kontinuirano poboljšavati prikladnost, primjerenost i efikasnost okvira upravljanja rizicima, i to na primjeren način na koji je integriran postupak upravljanja rizicima.

Kada organizacija identificira nedostatke i pronađe mogućnost poboljšanja, tada je potrebno razviti plan i dodijeliti zadatke. Jednom provedena, ova poboljšanja trebala bi pridonijeti poboljšanju upravljanja rizicima.

Rad okvira vizualno prikazuje Demingovim PDCA (Plan-Do-ControlAct) krug. PDCA model razvio je 1950-ih William Deming kao proces učenja ili usavršavanja temeljen na znanstvenoj metodi rješavanja problema. Sam Deming nazvao ga je drugim pojmom - ciklusom Shewhart-a, jer je stvorio model na osnovu ideje svog mentora. PDCA ciklus

predstavlja petlju, a ne krajnji proces. Cilj je poboljšati svako poboljšanje u tekućem procesu učenja i rasta.



Slika 6.2.1. „PDCA model“, Izvor: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug

PDCA krug se sastoji od četiri cjeline:

- P (eng. Plan) – prepoznati problem, prikupiti relevantne podatke i razumjeti osnovni uzrok problema, razviti hipoteze o tim problemima i odlučiti koju treba testirati.
- D (eng. Do) – primjena tih procesa, te razvoj i implementacija riješnja
- C (eng. Check) - nadziranje i mjerenje procesa i proizvoda s obzirom na postavljenu politiku, ciljeve i zahtjeve. Proučiti rezultat, izmjerite učinkovitost i odlučite podržava li hipotezu ili ne.
- A (eng. Act) – dokumentiranje rezultata, ako je rješenje bilo uspješno, implementirajte ga. Ako ne treba ponoviti PDCA ciklus.

Potrebno je ponoviti kako okvir baš kao i sama norma, nije pravilo koje se organizacija treba pridržavati. PDCA-a krug služi kao pomoć organizaciji kako bi lakše upravljala rizicima , i vrlo je bitno da svaka organizacija okvir prilagodi sebi i situaciji u kojoj se nalazi. PDCA okvir ima niz prednosti i nedostataka, stoga poduzeće treba dobro razmisliti prije nego što ga odluči primijeniti.

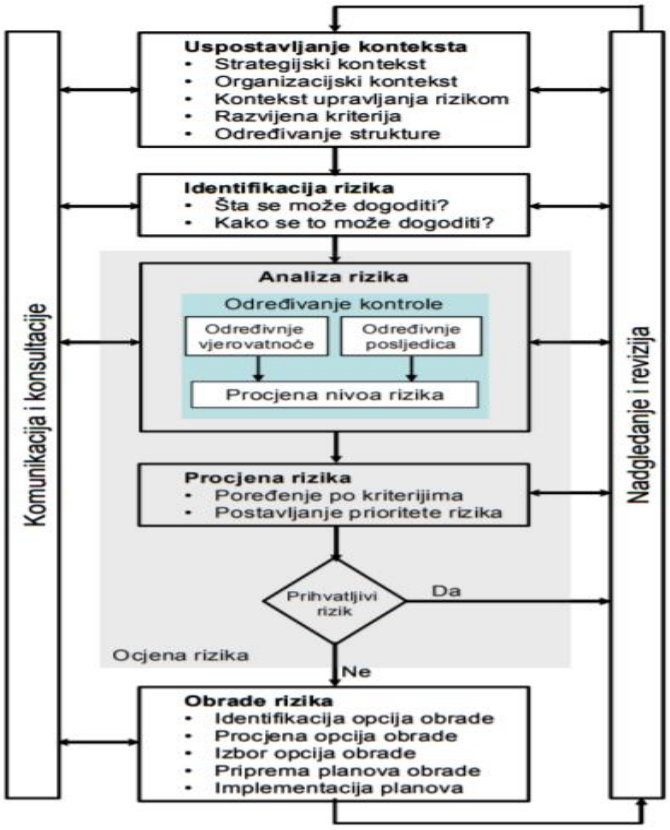
6.3. Proces upravljanja rizikom u normi ISO:31000:2018

„Proces upravljanja rizicima uključuje sustavnu primjenu politika, postupaka i praksi s aktivnostima komuniciranja i konzultiranja, uspostavljanje konteksta i ocjenjivanja, postupanja, praćenja, preispitivanja, bilježenja i izvještavanja o rizicima. Ocjenjivanje rizika obuhvaća prepoznavanje rizika, analizu rizika i vrednovanje rizika. Svrha vrednovanja rizika je biti potpora donošenju odluka. Vrednovanje rizika uključuje usporedbu rezultata analize rizika s uspostavljenim kriterijima kako bi se utvrdila potreba za djelovanjem. Vrednovanjem rizika može se utvrditi da nije potrebno djelovati (rizik je u prihvatljivim granicama) ili da je potrebno: razmotriti postupanje s rizikom, poduzeti daljnje aktivnosti za bolje razumijevanje rizika, održavati postojeće kontrole rizika, ponovno razmotriti ciljeve.“ (Svijet kvalitete, 2018.)

U mnogim su organizacijama komunikacija, savjetovanje, nadzor i preispitivanje povezane aktivnosti usko usklađene s okvirom. Te četiri djelatnosti su dio konteksta upravljanja rizicima i zato trebaju biti i dio okvira upravljanja rizicima. Okvir upravljanja rizicima često se opisuje kao arhitektura rizika, strategija i protokoli organizacije.

Na prirodu i opseg aktivnosti upravljanja rizicima u organizaciji uvelike utječu stav i sklonost organizacije prema riziku. Odnos organizacije prema riziku pruža temelj za provođenje procjena rizika i bilježenje rezultata. Priroda i razmjer komunikacije informacija sadržanih u registru rizika kroz cjelokupnu arhitekturu organizacije također pomaže definirati kontekst upravljanja rizicima. Kontekst upravljanja rizicima dio je unutarnjeg konteksta organizacije.
Unutarnji kontekst odnosi se na samu organizaciju, aktivnosti koje ona poduzima, raspon vještina i sposobnosti dostupnih unutar organizacije, te na način na koji je strukturirana. Interni dionici i njihova očekivanja dio su unutarnjeg konteksta. Interni se kontekst odnosi na kulturu organizacije, raspoložive resurse, primanje rezultata iz postupka upravljanja rizicima i osiguravanje da oni ponašanjima podržavaju i osiguravaju upravljanje rizicima.

Unutarnji kontekst odnosi se na ciljeve organizacije, njezine kapacitete, te na temeljne poslovne procese koji su uspostavljeni. Organizacija mora na pravi način donijeti odluku.



Slika 6.3. „Način donošenja odluke“, Izvor: Delić E. i Šišić R. (2019.) ' Upravljanje rizicima kao standardizirana procedura', Tuzla, Uiverzitet u Tuzli, <raspoloživo na: http://www.atex.ba/extern/documents/ex-tribine/2012/tema4/401%20-%20Delic,%20Sisic%20-%20Upravljanje%20rizicima%20kao%20standardiziran.pdf >

a)Komunikacija i konzultacija – trebaju se razviti na samom početku realizacije plana, jer uz dobru komunikaciju između članova sama realizacija će biti efikasnija. “Efektivna vanjska i unutarnja komunikacija osigurava da odgovorni za vođenje i provođenje upravljanja rizicima održavanju konstantnu komunikaciju s vodstvom organizacije, te da se u tijeku komunikacije prenesu sve bitne informacije kako bi se mogle donijeti ispravne odluke o daljnjem poslovanju. Važno je da osobe koje donose odluke budu upoznate sa rizicima koje one sa sobom povlače.

Pristup u kojem se odražava komunikacija donosi mnoge prednosti:

1. Osigurava razumijevanje želja i interesa organizacije
2. Pomaže u pravovremenom prepoznavanju rizika i njegovoj identifikaciji
3. Više stručnjaka iz različitih područja može pridonijeti rješavanju problema
4. Osigurava se pogled na više aspekata rizika.“ (Džolan, 2017.)

b)Utvrđivanje konteksta – kako bi organizacija utvrdila razinu rizika ona mora odrediti unutarnje i vanjske indikatore.

- „Utvrđivanje vanjskog konteksta – u vanjskom okruženju organizacija pronalazi i ostvaruje svoje ciljeve. Prilikom analize rizika bitno je da organizacija poznaje svoj vanjski kontekst. „Vanjski kontekst predstavlja veoma široko polje faktora, ali prilikom analize bitno je analizirati one faktore koji su od najveće važnosti za samu organizaciju. Vanjski faktori mogu biti:
  - Socijalno i kulturno okruženje
  - Politički ustroj
  - Ekonomsko stanje“ (Džolan,2017.)

- Utvrđivanje unutarnjeg konteksta – „proces mora biti u skladu sa unutarnjom organizacijom. Unutarnji kontekst podrazumijeva:
  - Vodstvo i organizacijsku strukturu;
  - Politiku i ciljeve organizacije;
  - Strategiju poslovanja organizacije;
  - Kapacitet organizacije;
  - Odnosi unutar organizacije;
  - Sustav transporta informacija;
  - Postojeće standarde po kojima organizacija posluje.“ (Sekulić,2016.)

- Utvrđivanje konteksta upravljanja rizikom – Prilikom utvrđivanja konteksta organizacija treba utvrditi svoje ciljeve, strategiju i elemente organizacije u kojima će se upravljati rizikom. Potrebno je definirati sve troškove i resurse koji će se koristiti u procesu upravljanja. Kontekst se može mijenjati prema potrebama organizacije, a može uključivati sljedeće:

• „Definiranje ciljeva procesa upravljanja rizikom
• Definiranje odgovornosti unutar procesa upravljanja rizikom
• Odgovornosti procesa upravljanja rizikom
• Definiranje raspona aktivnosti upravljanja rizikom
• Definiranje procesa, funkcija, projekata, proizvoda i usluga
• Definiranje metoda procjene rizika i sl.“(Džolan,2017.)

Kako bi došla do svoga cilja, organizacija se mora fokusirati da sve buduće i postojane rizike riješi određenim pristupom i alatima. Prilikom rješavanja rizika, bitno je da organizacija putem komunikacije i savjetovanja pomogne relativnim dioničarima da razumiju rizik i zašto se provode određene aktivnosti. Međusobna suradnja između komunikacije i savjetovanja trebala bi olakšati razumijevanje rizika i olakšati prikupljanje informacija. Komunikacija i savjetovanje s odgovarajućim vanjskim i unutarnjim dionicima trebali bi se odvijati unutar i kroz sve korake postupka upravljanja rizicima.

e) Procjena rizika - čini ju procesa utvrđivanja analize i procjene rizika. Procjenu rizika treba provoditi sustavno i u suradnji, oslanjajući se na znanje i stavove dionika. Treba koristiti najbolje dostupne informacije, po potrebi nadopunjene daljnjim ispitivanjem.

d) Identifikacija rizika- služi kako bi se mogli pronaći, prepoznati i opisati rizici, koji bi mogli spriječiti postizanje ciljeva organizacije. Relevantne, prikladne i ažurne informacije važne su za prepoznavanje rizika. Organizacija može koristiti niz tehnika za utvrđivanje nesigurnosti koje mogu utjecati na jedan ili više ciljeva.
Treba uzeti u obzir sljedeće čimbenike i odnos između tih čimbenika:

- materijalni i nematerijalni izvori rizika;
- uzroci i događaji;
- prijetnje i mogućnosti;
- ranjivosti i mogućnosti;
- promjene u kontekstu;
- pokazatelji novih rizika;
- prirodu i vrijednost imovine i resursa;
- posljedice i utjecaj na ciljeve;

- ograničenja znanja i pouzdanost informacija;
- čimbenici povezani s vremenom;
- pristranosti, pretpostavke i uvjerenja uključenih.

Organizacija bi trebala prepoznati rizike, bez obzira jesu li njihovi izvori pod njezinom kontrolom ili ne. Može postojati više ishoda, što može dovesti do raznih opipljivih ili nematerijalnih posljedica.

f) Analiza rizika - Svrha analize rizika je shvatiti prirodu rizika i njegove karakteristike, uključujući, prema potrebi, razinu rizika. Analiza rizika uključuje detaljno razmatranje neizvjesnosti, izvora rizika, posljedica, vjerojatnosti, događaja, scenarija, kontrola i njihove učinkovitosti. Događaj može imati više uzroka i posljedica i može utjecati na više ciljeva. Analiza rizika može se izvoditi s različitim stupnjevima detalja i složenosti, ovisno o svrsi analize, dostupnosti i pouzdanosti informacija i raspoloživim resursima.“ (Puškadija, 2019.) Tehnike analize mogu biti kvalitativne, kvantitativne ili kombinacija istih, ovisno o okolnostima i namjeni. Kada se radi analiza rizika, potrebno je sagledati:

- vjerojatnost događaja i posljedica;
- prirodu i veličinu posljedica;
- složenost i povezanost;
- vremenski povezani čimbenici
- učinkovitost postojećih kontrola;
- razina osjetljivosti i pouzdanosti.

Na analizu rizika može utjecati svako razilaženje mišljenja i prosudbi. Dodatni utjecaji su kvaliteta korištenih informacija, pretpostavki, sva ograničenja tehnika i način na koji se izvršavaju. Te utjecaje treba razmotriti, dokumentirati i priopćiti donositeljima odluka. Jako neizvjesne događaje može biti teško kvantificirati. To može biti problem pri analizi događaja s teškim posljedicama. U takvim slučajevima, korištenje kombinacije tehnika općenito daje bolji uvid. Analiza rizika daje ulaz u procjenu rizika, odluku kako rizik tretirati, te o najprikladnijoj strategiji i metodama smanjeja rizika.

A) Tretiranje rizika – svrha istoga je odabrati i primijeniti mogućnosti za rješavanje rizika. Tretiranje rizika uključuje:

- formuliranje i odabir mogućnosti smanjenja rizika;
- planiranje i provođenje smanjenja rizika;
- procjena učinkovitosti smanjenja;
- odluka da li je preostali rizik prihvatljiv;
- ako nije prihvatljivo, poduzimanje daljnjih aktivnosti za smanjenje.

Odabir najprikladnijih opcija tretiranja rizika uključuje uravnoteženje potencijalnih koristi ostvarenih u vezi s postizanjem ciljeva u odnosu na troškove, napor ili nedostatke provedbe. Opcije za smanjenje rizika mogu uključivati:

- izbjegavanje rizika (kako ne bi došlo do započinjanja ili nastavljanja s aktivnošću zbog koje nastaje rizik);
- preuzimanje ili povećanje rizika, radi iskorištavanja prilike;
- uklanjanje izvora rizika;
- promjena vjerojatnosti i posljedica;
- dijeljenje rizika (npr. putem ugovora, kupnje osiguranja);
- zadržavanje rizika informiranom odlukom.

Opravdanje za tretiranje rizika šire je od isključivo ekonomskih razloga i zato u obzir treba uzeti obveze organizacije, dobrovoljne obveze i stavove dionika. Odabir mogućnosti tretiranja rizika trebao se izvršiti u skladu s ciljevima organizacije, kriterijima rizika i raspoloživim resursima. Pri odabiru mogućnosti tretiranja rizika, organizacija bi trebala razmotriti vrijednosti, percepcije i potencijalno sudjelovanje dionika te najprikladnije načine komuniciranja i savjetovanja s njima. Iako su podjednako učinkoviti, neki tretmani rizika mogu biti prihvatljiviji za neke dionike nego za druge. Čak i ako se organizacija pažljivo ophodi prema riziku, ipak na kraju može doći do neželjenih posljedica. Kada se rizik „liječi“ bitno je kvalitetno praćenje i preispitivanje, kako bi organizacija bila sigurna da izabrani oblici smanjenja rizika postaju i ostaju učinkoviti. Ispravljanje rizika također može uvesti nove rizike kojima treba upravljati. Ako nisu dostupne mogućnosti tretiranja rizika ili ako mogućnosti ispravljanja ne mijenjaju dovoljno rizik, rizik treba evidentirati i održavati u

tijeku pregleda. Donositelji odluka i drugi dionici trebali bi biti svjesni razmjera preostalog rizika nakon tretmana rizika. Preostali rizik treba dokumentirati i podvrgnuti praćenju, pregledu i, prema potrebi, daljnjem tretiranju.

B) Praćenje i preispitivanje rizika - svrha praćenja i preispitivanja je osigurati i poboljšati kvalitetu i djelotvornost dizajna procesa, provedbe i ishoda. Organizacija bi trebala uzastopno pratiti i pregledavati proces i njegove ishode. Nadzor i pregled trebali bi se odvijati u svim fazama procesa. Praćenje i pregled uključuje planiranje, prikupljanje i analizu podataka, bilježenje rezultata i pružanje povratnih informacija. Rezultati praćenja i pregleda trebali bi biti uključeni u aktivnosti upravljanja učinkom, mjerenja i izvještavanja organizacije.

C) Dokumentiranje rizika - proces upravljanja rizikom i njegovi ishodi trebali bi se dokumentirati i izvještavati putem odgovarajućih mehanizama. Snimanje i izvještavanje ima za cilj:

- iskomunicirati aktivnosti i ishode upravljanja rizikom kroz cijelu organizaciju;
- pružiti informacije za lakše donošenje odluka;
- poboljšati aktivnosti upravljanja rizikom;
- pomoći u interakciji s dionicima, uključujući one koji su odgovorni i odgovorni za aktivnosti upravljanja rizikom.

Odluke o stvaranju, zadržavanju i rukovanju dokumentiranim informacijama trebale bi uzeti u obzir, ali ne ograničavajući se na: njihovu upotrebu, osjetljivost informacija te vanjski i unutarnji kontekst. Izvješćivanje je sastavni dio upravljanja organizacijom i trebalo bi poboljšati kvalitetu dijaloga sa dionicima i podržati najviše rukovodstvo i nadzorna tijela u ispunjavanju njihovih odgovornosti.

7. Povezanost između upravljanja rizicima i upravljanja kontinuitetom poslovanja

U većini slučajeva kontinuitet poslovanja je poddomena upravljanja rizicima. Kada je riječ o kontinuitetu poslovanja i upravljanju rizicima, rizik je na vodećem mjestu. Kontinuitet poslovanja kao dio sveukupnog programa otpornosti ublažava rizik Velike organizacije ne mogu tolerirati prekide poslovanja, stoga od svoji timova traže upravljanja rizicima i kontinuitetom poslovanja, da budu spremni za sve moguće vrste rizika. To im omogućuje proaktivno razvijanje strategija za ublažavanje rizika. Upravljanje kontinuitetom poslovanja je sustav koji reagira kada dođe do prekida poslovanja, dok se upravljanje rizikom poduzeća koristi za postizanje poslovnih ciljeva organizacije. Rizik upravljanja kontinuitetom poslovanja podpodručje je upravljanja rizikom poduzeća, poput upravljanja rizikom informacijske sigurnosti ili upravljanja rizicima zdravlja i sigurnosti. To je zbirka dobrih praksi upravljanja povezane zajedno. Analiza poslovnog utjecaja povlači se iz procesa upravljanja rizikom u poduzeću, a plan kontinuiteta poslovanja niz je nepredviđenih akcija. Okvir sustava upravljanja kontinuitetom poslovanja sustav je koji povezuje aktivnosti. Međutim, ako se za upravljanje kontinuitetom poslovanja organizacije oslanjamo na stručnjake za kontinuitet poslovanja, tada stvaramo paradoks nemogućnosti odgovora. Na temelju stručnjakove procjene rizika, organizacija na temelju tih informacija izrađuje plan. Rezultat procjene rizika omogućuje vodstvu da odredi prihvatljivi apetit organizacije za rizikom. Nakon što se definira apetit za rizikom, to će odrediti hoće li se ići dalje s ostatkom okvira za upravljanje kontinuitetom poslovanja.

Izvođenje određene procjene rizika povezane s upravljanjem kontinuitetom poslovanja pomaže organizaciji razmotriti različite resurse i rizike za njih. Također pomaže provjeriti valjanost postojećih kontrola i procijeniti sve dodatne kontrole koje bi mogle biti postavljene. Upravljanje rizikom u poduzeću važnije je od upravljanja kontinuitetom poslovanja, jer upravljanje rizikom promatra svaku nesigurnost koja može utjecati na ciljeve organizacije. Iako se u procjeni rizika kod kontinuiteta poslovanja razmatraju specifičniji rizici koji obuhvaćaju resurse koji utječu na procese i isporuku proizvoda i usluga. Upravljanje kontinuitetom poslovanja je više usredotočeno na utjecaj rizičnih događaja, a ne na vjerojatnost da će oni biti nepredvidljivi i neizbježni. Stoga je potrebno razumjeti koji bi rizici mogli zaustaviti poslovne aktivnosti. Jednom kada se rizik prepozna, tada se mogu razvijati odgovarajući planovi kontrole ili ublažavanje utjecaja rizika. Ako organizacija ima mogućnost

oporavka od određene opasnosti, istu strategiju bi mogla primijeniti za širok spektar prijetnji. Organizacija treba izgraditi mogućnosti oporavka na temelju utjecaja događaja (gubitak resursa, lokacija, osoblja, itd.), a ne samog rizika. Organizacije bi trebale upravljati rizicima, ali moraju priznati da resursi ne postoje da bi se svi rizici sveli na nulu. „U mnogim organizacijama, upravljanjem rizikom u poduzeću i upravljanjem kontinuitetom poslovanja vjerojatno upravlja isti tim, jer su tako usko isprepleteni - uostalom, nije moguće izraditi plan kontinuiteta poslovanja za rizični događaj ako nemate dobar osjećaj za moguće rizične događaje. Na isti način, nije moguće na odgovarajući način zaštititi tvrtku od prekida bez plana da se to riješi kad se dogodi. Drugim riječima: ako vaša tvrtka ima menadžera rizika i menadžera kontinuiteta poslovanja, bolje se pobrinite da su oni najbolji prijatelji.“ (Riskmethods) Zbog toga se jednak napor treba posvetiti pripremljenosti, jer upravo tu dolazi do kontinuiteta poslovanja. Jednako vrijeme treba posvetiti kontinuitetu poslovanja i upravljanju rizicima, umjesto da se dvije discipline izvode dvostruko.

Upravljanje rizicima uspostavljena je u poduzećima relativno dugo u usporedbi s kontinuitetom poslovanja i dobro je ukorijenjeno i razumljivo u mnogim organizacijama. Teško je zamijeniti ovu funkciju modernim upravljanjem kontinuitetom poslovanja. To nije nužno zbog bilo kakvih zaključaka, već više zbog percepcije, razumijevanja i općeg otpora promjenama. ISO 31000:2018 daje smjernice za razvoj sustava upravljanja rizicima za bilo koju vrstu rizika na korporativnoj razini. ISO 22301:2019 definira zahtjeve za razvoj kontinuiteta poslovanja, uključujući politiku kontinuiteta poslovanja, analizu učinka poslovanja, strategiju kontinuiteta poslovanja, planiranje i još mnogo toga. Kontinuitet poslovanja i upravljanje rizikom ponekad se smatraju različitim funkcijama ili međusobnim podskupovima ili jednostavno istim. Na primjer, pristup prevenciji, pripravnosti, odgovoru i oporavku u upravljanju rizicima predstavljen je kao upravljanje rizikom. Međutim, kada su svi koraci ispune i skupe rezultati, na kraju se dobije plan kontinuiteta poslovanja. U poslovanju se prvo pojavljuje pojama „upravljanje rizikom“, a tek kasnije se razvija kontinuitet poslovanja. Upravljanje rizikom može se sažeti kao izbjegavanje, ublažavanje, prenošenje ili prihvaćanje rizika, dok kontinuitet poslovanja odgovara izbjegavanju ili prenošenju rizika, više nego njegovom ublažavanju ili prihvaćanju.

	Upravljanje rizicima	Upravljanje kontinuitetom poslovanja
Ključna metoda	Analiza rizika	Analiza poslovnog utjecaja
Ključni parametri	Utjecaj i vjerojatnost	Dostupnost i utjecaj
Vrsta incidenta	Sve vrste događaja	Događaji koji uzrokuju značajne poslovne poremećaje
Veličina događaja	Svi događaji koji utječu na organizaciju	Oni koji prijete dostupnošću temeljnih procesa organizacije
djelokrug	Fokusira se prvenstveno na upravljanje rizicima za ključne poslovne ciljeve, kako biste spriječili ili smanjili incidente	Fokusira se uglavnom na upravljanje incidentima i oporavak kritičnih poslovnih procesa nakon incidenta
Intenzitet	Sve, od postupnog do naglog	Iznenadni ili brzi događaji (premda i odgovor može biti prikladan ako puzajući incident iznenada postane ozbiljan)

Tablica 7. „Usporedba upravljanja rizicima i upravljanja kontinuitetom poslovanja“ Izvor: European Union Agency for Cybersecurity, „BC/RM Interfaces“, [Internet], <raspoloživo na: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces >, [pristupljeno 1.9.2020.]

Organizacija dolazi u situaciju da se kontinuitet poslovanja i upravljanje rizikom preklapaju. I ako nisu isti, postoje zajedničke komponente, a jedna nije nužno podskup druge. Poanta je u tome da je važno međusobno razumijevanje onoga što netko podrazumijeva pod „upravljanjem rizicima“ ako stvarno žele biti sigurni da razumiju odnos s kontinuitetom poslovanja. Ispravnim razumijevanjem rizika postoji veća šansa da se svaka funkcija pravilno izvršava u organizaciji do potrebne razine

8. Zaključak

Organizacije svakodnevno nailaze na rizike, ali se boje suočiti s njima. Stoga, neke Organizacije će doživjeti neuspjeh u budućnosti jer nemaju dovoljno znanja o vrstama rizika i upravljanju njima, te ne mogu poboljšati strategiju. Rizik se najčešće veže uz poslovanje te ga s tog aspekta definira kao vjerojatnost pojave nekog događaja koji će imati negativan utjecaj na poslovanje organizacije, kao što su na primjer porast troškova, smanjenja zarada i sl. Upravljanje rizicima je proces upravljanja bilo koje organizacije. Cilj tog procesa je da se rizici kontroliraju i da se s njima mudro upravlja unutar svake aktivnosti u okviru portfelja svih aktivnosti. To znači smanjiti troškove rizika u poslovanju. U idealnom načinu upravljanja rizicima slijedi postupak određivanja prioriteta gdje se prvo rješavaju rizici s najvećim gubitkom i najvećom vjerojatnošću pojave, a kasnije se rješavaju rizici s nižom vjerojatnošću pojave i nižim gubitkom. Norma ISO 22301:2019 je norma sustava upravljanja kontinuitetom poslovanja koja definira kriterije za planiranje, uspostavljanje, provedbu, upravljanje, nadzor i dr.

Namijenjena je primjeni na sve organizacije ili njihove dijelove, bez obzira na vrstu, veličinu i prirodu organizacije. Organizacije koje implementiraju sustav upravljanja kontinuitetom poslovanja (BCMS) temeljene na zahtjevima ISO 22301:2019 mogu proći formalni postupak ocjenjivanja putem kojeg mogu dobiti akreditiranu potvrdu prema ovom standardu. Certificirani BCMS internim i vanjskim dionicima pokazuje da se organizacija pridržava dobre prakse u upravljanju kontinuitetom poslovanja. Slično ostalim ISO standardima sustava upravljanja zahtjevi navedeni u ISO 22301:2019 prilagođeni su za sve. Kako bi olakšala upravljanje rizicima Međunarodna organizacija za normizaciju (ISO) izdala je normu ISO 31000:2018 u kojoj su navedene smjernice i načela namijenjena organizaciji. Struktura ISO 31000:2018 izvorno je objavljena 2009. godine, a ažurirana verzija objavljena je u veljači 2018. godine. Međutim, ukupna namjena norme ISO 31000:2018 ostaje ista – uključivanje upravljanja rizicima u strateški sustav upravljanja. Verzija 2018. je vrlo slična originalnoj verziji, ali glavne promjene se odnose na načela upravljanja rizicima, isticanje važnosti rukovođenja najvišim rukovodstvom, veći naglasak stavlja se na upravljanja rizicima, jer je novo znanje i analiza vođeno revizijom procesa, postupaka i kontrola te je sadržaj pojednostavljen s više otvorenih sustava.

Odnos između kontinuiteta poslovanja i upravljanja rizicima ovisi o organizaciji.
U većini slučajeva kontinuitet poslovanja je poddomena upravljanja rizicima. Kada je riječ o kontinuitetu poslovanja i upravljanju rizicima, rizik je na vodećem mjestu. Kontinuitet poslovanja kao dio sveukupnog programa otpornosti ublažava rizik.

U Koprivnici, _____ _____

(datum) (vlastoručni potpis)

Sveučilište
Sjever

SVEUČILIŠTE SJEVER

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, ANA MARIJA ŠIJAK *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog *(obrisati nepotrebno)* rada pod naslovom UPRAVLJANJE RIZICIMA S ASPEKTA UTJECAJA SUSTAVA UPRAVLJANJA KONTINUITETOM POSLOVANJA I POVEZIVANJE S DOBROM SUSTAVA UPRAVLJANJA RIZICIMA *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)
Ana Marija Šijak
(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, ANA MARIJA ŠIJAK *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog *(obrisati nepotrebno)* rada pod naslovom UPRAVLJANJE RIZICIMA S ASPEKTA UTJECAJA SUSTAVA UPRAVLJANJA KONTINUITETOM POSLOVANJA I POVEZIVANJE S DOBROM SUSTAVA UPRAVLJANJA RIZICIMA *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)
Ana Marija Šijak
(vlastoručni potpis)

Literatura

(1) Adriacert, (2019.), *'Sustavi upravljanja'*, [Internet] <raspoloživo na: https://adriacert.hr/ > [pristupljeno 12.9.2020.]

(2) Advisera, (2019.), *'The basics of ISO 22301'* [Internet] < raspoloživo na: https://advisera.com/27001academy/what-is-iso-22301/ > [pristupljeno 12.9.2020.]

(3) Baričević M. (2019.), *'Metode upravljanja rizicima*', Završni rad, Split, Visoka škola za inspekcijski i kadrovski Menadžment <raspoloživo na: https://repozitorij.vsikmp.hr/islandora/object/vsikmp%3A12/datastream/PDF/view > [pristupljeno 3.9.2020.]

(4) Bešker, M.,(2009). '*Sustav upravljanja organizacijom'*, Oskar, Zagreb.

(5) Buntak, K., Drožđek, I., i Košćak, M. (2014). *'Metodologija implementacije upravljanja rizicima FMEA metodom*', Tehnički glasnik, 8(1), [Internet] <raspoloživo na : https://hrcak.srce.hr/120069 > [pristupljeno 4.9.2020.]

(6) Chapman C.; Ward S.(2003.), *'Project Risk Management: Processes, Techniques, and Insights, Management'*, American Management Association, New York, 2001.

(7) Džolan, I. (2016.), *'Upravljanje rizicima'* Završni rad , Zagreb, Sveučilište u Zagrebu [Internet] <raspoloživo na: http://repozitorij.fsb.hr/8008/1/Dzolan_2017_zavrsni_rad.pdf> [pristupljeno 3.9.2020.]

(8) European Union Agency for Cybersecurity, *'BC/RM Interfaces'*, [Internet], <raspoloživo na: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces >, [pristupljeno 1.9.2020.]

(9) Kadlec Ž, Udovčić A. (2013.), *'Analiza Rizika upravljanja poduzećem'*, Pregledni rad, [Internet] <raspoloživo na: https://www.scribd.com/document/319981914/PM-br6-cl6>, [pristupljeno 3.9.2020.]

(10) Manec K., (2018.), *'Upravljanje rizicima u sustavu poslovanja na primjeru „VNUK" „d.o.o.*",, Završni rad, Varaždin, Sveučilište Sjever, [Internet] <raspoloživo na: https://repozitorij.unin.hr/islandora/object/unin:1973/datastream/PDF/view > [pristupljeno 5.9.2020.]

(11) Međunarodna Organizacija za Standardizaciju (ISO), (2018). *'Norma ISO 31000:2018 – sustav upravljanja rizicima'* [Internet], < https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en > [pristupljeno 5.9.2020.]

(12) Međunarodna Organizacija za Standardizaciju (ISO), (2019). *'Norma ISO 23001:2019, Sigurnost i otpornost - Sustavi upravljanja kontinuitetom poslovanja – Zahtjevi'* [Internet], < https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en > [pristupljeno 5.9.2020.]

(13) Ministarstvo vanjskih i Europskih poslova Republike Hrvatske – Glavno tajništvo, (2012.), *'Strategija upravljanja rizicima'* [Internet], <raspoloživo na: http://www.mvep.hr/files/file/dokumenti/STRATEGIJA-UPRAVLJANJA-RIZICIMA-MVEP-11-2012.pdf >, [pristupljeno 1.9.2020.]

(14) Mravoić O.T., (2019.), ' *Preporuke ISO standarda za pametne gradove za područje Emergency Managementa i procjena stanja na primjeru Grada Splita'*, Diplomski rad, Split, Ekonomski fakultet, [Internet] <raspoloživo na: https://core.ac.uk/download/pdf/270133171.pdf >, [pristupljeno 24.9.2020.]

(15) Puškadija N.(2019.), *'Analiza nesukladnosti na primjeru proizvodnog poduzeća za obradu metala'*, Diplomski rad, Zagreb, Sveučilište u Zagrebu [Internet] <raspoloživo na: https://repozitorij.fsb.unizg.hr/islandora/object/fsb:5380/datastream/PDF/view>, [pristupljeno 5.9.2020.]

(16) Rak M. (2015.), *'Rizici terorizma'*, Završni rad, Šibenik , Veleučilište u Šibeniku [Internet] <raspoloživo na: https://repozitorij.vus.hr/islandora/object/vus:64/datastream/PDF/view >, [pristupljeno 3.9.2020.]

(17) Riskmethods, *'Enterprise Risk Management vs. Business Continuity Management: What's the Difference?'* [Internet] <raspoloživo na: https://www.riskmethods.net/resilient-enterprise/erm-vs-bcm > [pristupljeno 8.9.2020.]

(18) Sekulić I., (2016,), *'Upravljanje rizicima na primjeru proizvodnog poduzeća'*, Završni rad, Varaždin, Sveučilište Sjever, [Internet] <raspoloživo na: https://zir.nsk.hr/islandora/object/unin:1148/preview > [pristupljeno 3.9.2020.]

(19) Svijet kvalitete (2018.), *'Upravljanje rizicima prema HRN ISO 31000:2018'* [Internet] <raspoloživo na: https://www.svijet-

kvalitete.com/index.php/normizacija/4106-upravljanje-rizicima-prema-hrn-iso-31000-2018 > [12.9.2020.]

(20) The British Standards Institution, (2019.), *'ISO 22301 Business continuity management* '[Internet], <raspoloživo na: https://www.bsigroup.com/globalassets/localfiles/en-au/ISO%2022301/22301%20Resources/iso-22301-business-continuity-mapping-guide-bsi0362-1911-au.pdf > [pristupljeno 1.9.2020.]

(21) Veleučilište Velika Gorica, (2011.), *'IV. Međunarodna konferencija „Dani kriznog upravljanja*‟ [Internet], <raspoloživo na: https://dku.hr/wp-content/uploads/2016/09/zbornik2011.pdf > [pristupljeno 7.9.2020.]

(22) Vujović, R. (2009.): *'Upravljanje rizicima i osiguranje'*, Univerzitet Singidunum, Beograd

(23) Williams C. A.; Smith M.L. ; Young P.C., (1998.), Boston, Massachusetts: Irwin / McGraw-Hill,

(24) Young C. P. and S. C. Tippins,(2003.) '*Managing Business Risk: An Organization Wide Approach to Risk'*, Wiley, New York, 2003.

Popis slika

(1) Slika.2.2. „*Podjela rizika*“, Izvor: Vujović R. (2009.) „Upravljanje rizicima i osiguranje“……..……5

(2) Tablica. „*Kvalitativna i kvantitativna analiza*“, Izvor: Izrada autora prema Baričević (2019.) Metode upravljanja rizicima - Visoka škola za inspekcijski i kadrovski Menadžment, Split……..……...9

(3) Slika 4, „*Metode upravljanja rizicima*“, Izvor: Vujović R, (2009.) „Upravljanje rizicima i osiguranje“ ……..……....12

(4) Tablica 5. „*Usporedba Norme ISO 22301 pije i sada*“, Izvor: Izrada autora prema The British Standards Institution, (2019.), 'ISO 22301 Business continuity management '[Internet], <raspoloživo na: https://www.bsigroup.com/globalassets/localfiles/en-au/ISO%2022301/22301%20Resources/iso-22301-business-continuity-mapping-guide-bsi0362-1911-au.pdf > [pristupljeno 1.9.2020.]…….....….....….....16

(5) Slika 6. „*Sustav upravljanja rizicima*“, Izvor: izrada autora ……..……....28

(6) Slika 6.2.1. „*PDCA model*“, Izvor: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdcakrug.....…….....37

(7) Slika 6.3. „*Način donošenja odluke*“, Izvor: http://www.atex.ba/extern/documents/ex-tribine/2012/tema4/401%20-%20Delic,%20Sisic%20-%20Upravljanje%20rizicima%20kao%20standardiziran.pdf...…….....39

(8) Tablica 7. „*Usporedba upravljanja rizicima i upravljanja kontinuitetom poslovanja*“ Izvor European Union Agency for Cybersecurity, „BC/RM Interfaces“, [Internet], <raspoloživo na: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces >, [pristupljeno 1.9.2020.].....48