Korištenje Balanced Scorecard metode za upravljanje IT rizicima

Dora, Trogrlić

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:956501

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Dora Trogrlić

KORIŠTENJE BALANCED SCORECARD METODE ZA UPRAVLJANJE IT RIZICIMA

DIPLOMSKI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Dora Trogrlić

Matični broj: 0016116640

Studij: Organizacija poslovnih sustava

Korištenje Balanced Scorecard metode za upravljanje IT rizicima

DIPLOMSKI RAD

Mentorica:

Prof. dr. sc. Melita Kozina

Varaždin, veljača 2021.

Dora Trogrlić

Izjava o izvornosti

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

Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Korištenje Balanced Scorecard metode za upravljanje IT rizicima nije tema koja se bavi isključivo teorijskim pregledom Balanced Scorecard metode, IT rizika, te načina upravljanja istima, već kroz istraživanje na konkretnom primjeru prikazuje korištenje same metode. Upravljanje rizicima iznimno je širok pojam, ali i relativno nov u poslovnom svijetu, a odnosi se na prevenciju štete koja bi potencijalno mogla ugroziti poslovanje neke organizacije, što bi zapravo značilo da je upravljanje rizicima poduzimanje određenih akcija. Upravljanje rizicima obuhvaća i pojam korporativnog upravljanja rizicima, što se odnosi na samu upravljačku strukturu i poslovne procese. Pojam rizika odnosi se na određene prijetnje ili opasnosti, te vjerojatnost da će to u određenim okolnostima zapravo predstavljati ranjivost sustava, kojom je moguće nanijeti štetu organizaciji, dok IT rizici proizlaze iz sve veće i intenziviranije upotrebe IT-a kao važne podrške i segmenta unapređenja poslovanja. Uspješnost poslovanja neke organizacije uglavnom se ogleda kroz financijske pokazatelje, no Balanced Scorecard jedna je od metoda koja za uspješnost poslovanja uzima više čimbenika osim financija, te se iz tog razloga uglavnom stavlja u kontekst pokazatelja uspješnosti organizacije. Osim određivanja stupnja uspješnosti, ova metoda može se koristiti i za upravljanje IT rizicima što je u radu prikazano na stvarnom primjeru. Istraživanje se odnosi na neprofitnu organizaciju, VI. osnovnu školu u Varaždinu. Za organizaciju su definirani strateški ciljevi, strateška mapa, IT ciljevi koji su zatim mapirani sa strateškim ciljevima, stavljeni su u kontekst CobiT 5 procesa, definirane su prijetnje i opasnosti, razine rizika te je dan prijedlog poboljšanja.

Ključne riječi: Balanced Scorecard; upravljanje rizicima; korporativno upravljanje rizicima; IT rizici; ISO 31000:2009; CobiT 5;

Sadržaj

1. Uvod

Kako ne samo poslovanje, već i sam život, često može biti nepredvidiv, nestabilan, te pun promjena i rizika, vrlo je važno određene rizike unaprijed prepoznati. Rizici poslovanja često se očituju kroz iskušenja i određene opasnosti koje prijete uspjehu i ostvarenju poslovnih ciljeva. Sa sve većom primjenom informacijske tehnologije i digitalne transformacije poslovanja, u poslovanju se javlja i sve više informatičkih rizika. Informatički rizici ne pojavljuju se isključivo kroz tehničke poteškoće koje dolaze sa korištenjem tehnologije, već postoje i rizici od prevelikih i neisplativih ulaganja u informatiku, problemi neuspješnosti informatičkih projekata, prekidi u radu informacijskog sustava ili pak otežani rad sustava, te problemi vezani uz privatnost i sigurnost podataka. Veoma je bitno da se svi rizici, ne samo oni informatički, tretiraju i da se njima upravlja, kako se poslovanju ne bi nanijela prevelika šteta. Upravljanje rizicima relativno je nov pojam i pristup u poslovanju, a ključna stavka ovog pristupa jest poduzimanje određenih mjera za tretiranje rizika, kako bi se oni ili smanjili ili pak u potpunosti izbjegli.

Balanced Scorecard metoda je koja se uglavnom koristi za određivanje uspješnosti poslovanja neke organizacije ili poduzeća, a ono najbitnije po čemu se razlikuje od ostalih metoda za određivanje uspješnosti, jest to što u glavni fokus ne stavlja financijske pokazatelje. Balanced Scorecard metoda u obzir uzima četiri perspektive poslovanja. Jedna od te četiri perspektive proučava financijske pokazatelje, zato što su između ostalog i ti pokazatelji važni za prikaz uspješnosti. Druga perspektiva ogleda se u poslovnim procesima organizacije ili poduzeća, te prikazuje koji su poslovni procesi iznimno bitni za daljnje funkcioniranje organizacije. Ukoliko postoje određeni zastoji u poslovnim procesima, kroz ovu metodu moguće je vidjeti koje je procese bolje kreirati iznova, a koje je poslovne procese lakše prilagoditi trenutnom stanju poduzeća. Treća perspektiva odnosi se na zaposlenike i kolektiv same organizacije, te na njihovo napredovanje, učenje, rast i razvoj. Ova perspektiva veoma je bitna, jer je svojevrsni pokretač cijele organizacije. Za svako poslovanje bitno je da se zaposlenici osjećaju sigurno i zadovoljno, te da imaju mogućnost učenja i napretka kako bi se i cijelo poslovanje moglo kretati ka boljem. Četvrta perspektiva predstavlja odnos sa klijentima i krajnjim korisnicima, te procjenjuje koliko su zapravo ključni korisnici zadovoljni sa samim poduzećem.

Ova metoda ne koristi se samo za mjerenje uspješnosti poslovanja, već se može koristiti i pri upravljanju rizicima u organizaciji, što je na primjeru prikazano u poglavlju Istraživanje, u nastavku rada.

2. Metode i tehnike rada

Metode i tehnike rada koje su korištene pri razradi teme Korištenje Balanced Scorecard metode za upravljanje IT rizicima odnose se na proučavanje dostupne literature, kako bi se stvorila teorijska podloga, ali i baza za istraživanje. Istraživanje je napravljeno u suradnji sa zaposlenicima VI. osnovne škole u Varaždinu. Osim korištenja dostupne literature, kroz razgovor sa zaposlenicima škole, ne samo sa stručnom službom, već i kroz razgovor s učiteljima, informatičarima, te kroz proučavanje dostupne dokumentacije, prikupljeni su svi potrebni podaci. Svi prikupljeni podaci korišteni su u identifikaciji strateških ciljeva, kreiranju strateške mape, identifikaciji IT ciljeva, mapiranju IT ciljeva sa strateškima, te identifikaciji prijetnji i rizika.

3. Upravljanje rizicima

Upravljanje rizicima relativno je novi pristup i pojam koji se javlja u poslovnom svijetu, a prethodi mu pristup izbjegavanja rizika. Pojam izbjegavanja rizika naglasak je stavljao na prevenciju, odnosno poduzimanje akcija kojima bi se poslovanje zaštitilo od mogućih rizika, štete kojom određeni rizik rezultira, bez obzira na izloženost i vjerojatnost svakog pojedinog rizika. Upravljanje rizicima, s druge strane, pristup je koji se temelji na nekoliko različitih točaka. Kako bi se kvalitetno upravljalo rizicima potrebno je pronaći slabije strane sustava, odnosno organizacije – tehnički problemi poput problema u infrastrukturi, opskrbi električne energije… Druga perspektiva upravljanja rizicima odnosi se na financijski aspekt, određivanje količine ulaganja, ali i kreiranje protumjera koje pomažu u očuvanju imovine organizacije. Poslovanje se i inače veže s pojmom nestabilnosti i dinamičnosti, no u današnje vrijeme ta je veza još jača. Iako to često nije moguće, te teško predvidivo, kroz upravljanje rizicima potrebna su iznimno velika ulaganja kako bi se poslovanje stabiliziralo, a sigurnost povećala. Posljednja perspektiva u kojoj se upravljanje rizicima ogleda jest ona najkompleksnija, odnosno, koja je granica uspješnog poslovanja tvrtke, ili barem održivog. Svaka mogućnost postojanja neželjenog ishoda, ali i posljedice, nekog događaja ili odluke predstavlja rizik, te događaj ili odluku čini rizičnom. Primjeri takvih neželjenih ishoda su novčani gubitak, gubitak ugleda tvrtke u bilo kojem pogledu, gubitak povjerljivih informacija koji može rezultirati i neovlaštenim pristupom informacijama, kroz sigurnosni propust. Upravljanje rizicima, prema svojoj definiciji, je proces kroz koji organizacija i njeni menadžeri pronalaze, identificiraju, smanjuju i kontroliraju rizike koji bi se mogli javiti i rezultirati određenim gubitcima, te bi trebao obuhvaćati nekoliko aktivnosti – utvrđivanje imovine, prijetnji, ranjivosti, rizika te protumjera. Sam pristup upravljanja rizicima pruža uvid u razmjer određenih gubitaka, vjerojatnosti da će do istih doći te određivanje mjera kojima bi se opseg ili vjerojatnost gubitaka mogli smanjiti. Nakon svega navedenog i prikaza uzročno-posljedične veze između rizika i gubitaka, što je veća vjerojatnost da će nastupiti neki neželjeni događaj ili ishod, te što su posljedice teže, to je i sam rizik veći. Kako bi se upravljanje rizicima moglo provoditi, potrebno je sagledati nekoliko prethodno navedenih pojmova – prijetnje, ranjivost, imovina i mjere, odnosno protumjere. Prijetnje se odnose na aspekt rizika na koji organizacija kao takva nema utjecaja, već je isključivo namjera određene osobe. Osoba koja ugrožava interese organizacije naziva se ugroziteljem. Ranjivost je aspekt rizika koji je pod utjecajem organizacije te se odnosi na bilo kakvu slabost organizacije. S obzirom na to da se ranjivost nalazi pod utjecajem organizacije, razinu ranjivosti moguće je smanjiti kroz primjenu određenih mjera. Mjere se zapravo odnose na sve aktivnosti i alate, poput softverskih rješenja, ili određenih uređaja, kojima se rizik nastoji umanjiti, prije no što počne djelovati. Sva materijalna imovina (novčana sredstva, strojevi, zemljišta, zgrade, …),

ali i nematerijalna imovina (poslovne informacije, znanja, ideje, patenti i softveri), podložni su rizicima i kao takve ih treba zaštititi.

Upravljanje rizicima veoma je širok pojam, ali s obzirom na sve veću zastupljenost digitalizacije, jako je bitno obratiti pažnju na informatičke rizike koji se javljaju u poslovanju. Iako digitalizacija uglavnom ima pozitivan utjecaj na sveopće poslovanje, te se iz istog razloga ulaganja u informatiku intenziviraju, ona ima i svoje loše strane, te sa sobom nosi rizike koji su novi i na koje menadžeri nisu navikli. Samim time dovodi se do velike štete i gubitaka. Područje informacijske sigurnosti jedno je od najpopularnijih rizičnih područja prilikom pojačanog uvođenja informatike, a upravo je najpoznatiji rizik krađa osobnih podataka. Američka multinacionalna kompanija TJX Companies imala je propust u vidu nezaštićene bežične mreže, što je uzrokovalo krađu podataka čak 94 milijuna kreditnih i debitnih kartica. Još jedan sličan primjer jest primjer Vladine agencije – Carinska i porezna uprava Velike Britanije, gdje je došlo do gubitka dva diska sa osobnim podacima 25 milijuna obitelji u Velikoj Britaniji. Osobni podaci čak 12,5 milijuna klijenata ukradeni su kroz krađu traka s pričuvnom pohranom podataka iz sistemske sobe Banke New York Mellon. Ne dolazi samo do krađa i gubitaka osobnih podataka, u primjeru Heartland Payment Systems došlo je do gubitka podataka o velikom broju transakcija zbog infekcije informacijskog sustava uz pomoć zloćudnog softvera. Sonyev multimedijalni servis PlayStation Network zbog krađe 24 milijuna osobnih podataka, transakcija i zaporki korisnika pretrpio je gubitak od 171 milijuna dolara. Riječka banka je zbog propusta unutarnjih kontrola izgubila 75 milijuna eura kroz transakcije za koje je godinama bio zadužen trgovac devizama banke. HSBC Bank, odnosno britanska organizacija za multinacionalne bankarske i financijske usluge, platila je kaznu od 3,2 milijuna funti zbog gubitka nekriptiranog diska na kojem su se nalazili podaci životnog osiguranja od 180.000 klijenata. Međutim, ovo su samo neki od poznatijih primjera posljedica nekompetentnog upravljanja IT rizicima. Nažalost, ovakve se stvari događaju svakodnevno. Informatički rizici po svojoj prirodi sve više postaju sigurnosni rizici. Sigurnosni rizici bez obzira na svoju različitost, kompleksnost i brzi razvoj imaju određena obilježja. Sve češće dolazi do hakerskih pljački automobila, bankomata, *cyber* kriminal u Sjedinjenim Američkim Državama proizvodi trošak od 1.000 milijardi USD, na godišnjoj razini, dok trošak zaštitnih mjera iznosi 67 milijardi USD. Na dnevnoj razini šalje se čak 100 milijardi *spam* poruka, na razini pojedinaca sve češće se javljaju krađe osobnih podataka, cyber prostor proglašen je, uz kopno, more, zrak i svemir, petom vojnom domenom, a najveća prijetnja sigurnosti i dalje ostaju ljudi, kao krajnji korisnici, koji bi svoje lozinke otkrili u zamjenu za čokoladu. Iz svih navedenih primjera jasno je vidljivo kako se prema IT rizicima i upravljanju njima više ne smije odnositi kao isključivo prema tehnološkom pitanju, već bi se istima trebalo pristupati i s najviših pozicija menadžmenta. Iz

toga proizlazi da je upravljanje IT rizicima postala veoma bitna karika korporativnog upravljanja informatikom. [7] [9]

3.1. Korporativno upravljanje rizicima

Korporativno upravljanje pojam je koji se odnosi na upravljačke strukture i procese unutar poslovnih sustava, što bi zapravo značilo da je korporativno upravljanje određeni skup mehanizama kojima se osigurava da se sva ulaganja vrate ponovno u poduzeće, no na način na koji se ne ugrožava opstanak poduzeća ili organizacije. Korporativno upravljane sastoji se od mnogo područja – menadžment, dioničari, drugi *stakeholderi* (radnici), javnost, vlasnici, društvena odgovornost poduzeća… Korporativno upravljanje rizicima daje uvid u procjenu štete, odnosno učinka neželjenih događaja, te određivanje mjera kojima se šteta izbjegava ili smanjuje. Izazova koji se javljaju u okruženju *cyber* sigurnosti ima sve više. Poduzeća sve više koriste nove digitalne tehnologije, te uvelike napuštaju tradicionalne i klasične informacijske sustave. Takva promjena i primjena otvorenog informatičkog okruženja prisiljava poduzeća na korištenje mobilnih, pametnih i digitalnih uređaja, čime se nameće i novi način upravljanja *cyber* sigurnošću. Sve više *cyber* napada je ciljano i organizirano, čak i do nacionalne razine, dok su još donedavno napadi bili uglavnom izdvojeni i na razini pojedinaca. Velik problem javlja se u nedostatku kompetencija, naglasak se sve više stavlja isključivo na tehnološke kompetencije, a ne i na samo razumijevanje poslovanja u kontekstu informatičke sigurnosti. Nedostatak kompetencija velik do populacije čini vrlo lakim metama, ljudi su najčešće mete *cyber* napada različitih oblika, od krađa identiteta, lažnih predstavljanja, zlonamjernih računalnih kodova, pa sve do hakiranja i društvenog inženjeringa. Međutim, ljudi nisu najčešće mete isključivo zbog nedostatka kompetencija, koje bi služile kao svojevrsne vještine u obrani od *cyber* napada, već velik problem i najveću prijetnju sigurnosti čini upravo nedostatak svijesti o *cyber* napadima i informatičkoj sigurnosti. Pogrešno je mišljenje da su pojedinci izuzeti od *cyber* napada, naime, više ne postoje izuzeci, *cyber* napadi pogađaju cjelokupno stanovništvo koje se služi suvremenom tehnologijom, što znači da su pojedinci i mali poduzetnici mete jednako kao i velike korporacije.

Korporativno upravljanje informatičkim rizicima zapravo omogućuje određeni stupanj informatičke sigurnosti. Informatička sigurnost temelji se na tri parametra: povjerljivost, integritet i raspoloživost. Povjerljivost se odnosi na siguran pristup cijelom informacijskom sustavu samo i isključivo ovlaštenim osobama unutar poduzeća. Integritet se odnosi na same informacije i na informacijski sustav, odnosno osiguravanje ispravnih i cjelovitih informacija. Kako se povjerljivost odnosi na mogućnost pristupa informacijama samo ovlaštenim osobama, raspoloživost se pak odnosi na stalnu i pravodobnu mogućnost pristupa istima. Svako

narušavanje sigurnosti informacija i prethodno navedenih parametara za poduzeće predstavlja rizik u poslovanju. Povjerljivost, integritet i raspoloživost, osim kao parametri informacijske sigurnosti, navode se i kao svojstva informacija koje se koriste u poslovanju. Narušavanje povjerljivosti sa sobom nosi određene posljedice, kao što su gubitak konkurentske prednosti, gubitak povjerenja kupaca i krajnjih korisnika, kršenje regulatornih okvira, veliki financijski gubitci i slično. Ukoliko dođe do narušavanja integriteta informacija, neke od posljedica mogu biti pogrešno i nepravovremeno donošenje krucijalnih poslovnih odluka, gubitak povjerenja kupaca i klijenata te kršenje regulatornih okvira, kao i prilikom narušavanja povjerljivosti. Raspoloživost kao posljednje svojstvo informacija, prilikom narušavanja također nosi posljedice, poput nemogućnosti isporuke proizvoda i usluga, što je uzrokovano zbog nemogućnosti pristupa informacija o ugovorenom poslu, nemogućnost ispunjenja ugovorenih obaveza, te kršenje regulatornih okvira. Iako su ovo samo neke od mogućih posljedica, realno je za očekivat da jedna za sobom povlači ostale. Teško je moguće da će nakon kršenja regulatornih okvira i nemogućnosti ispoštivanja ugovorenih obaveza, poduzeće zadržati povjerenje klijenata, što zapravo donosi i teške financijske gubitke. Sve je ovo moguće izbjeći, ili barem uvelike smanjiti mogućnost da dođe do toga, kroz definiranje i poduzimanje zaštitnih kontrolnih mjera. Potrebno je uvesti mjeru identifikacije i autorizacije korisnika, zaštititi podatke u prijenosu i mirovanju, te primjenom kontrolnih mjera koje su vezanje uz upravljanje kontinuitetom poslovanja, dostupnosti informacija, dostupnosti informacijskog sustava i resursa, te primjenom metoda brzog i učinkovitog oporavka poslovanja ukoliko ipak dođe do nekog neželjenog događaja. [7] [9]

3.2. Zaštitne kontrolne mjere informacijske sigurnosti

Kao što je već navedeno u prethodnim poglavljima, prilikom izbjegavanja ili umanjivanja rizika, potrebno je definirati i provodit određene zaštitne kontrolne mjere. Informacijskom sustavu prijete opasnosti i rizici iz više izvora – prirodni i ljudski. Prirodne opasnosti i rizici koji mogu nanijeti štetu informacijskom sustavu su požari, poplave, jaka svjetlost, no i prljavština i prašina na koju se vrlo često ne obraća prevelika pozornost. Opasnosti i rizici čiji su izvor ljudi mogu biti namjerni i slučajni, u namjerne opasnosti i rizike ubrajaju se *cyber* napadi, odnosno računalni kriminalci i hakeri, ali i nezadovoljni zaposlenici, dok se u slučajne opasnosti i rizike ubrajaju nenamjerno brisanje podataka, nestručnost, neznanje, nedostatak kompetencija, nemar i nepravilno rukovanje opremom. Prethodno su navedeni parametri informacijske sigurnosti i ključna svojstva informacija koje predstavljaju rizik za poslovanje ukoliko dolazi do narušavanja istih, no i informacijska sigurnost ima svoje zahtjeve – zahtjev sigurnosti, zahtjev dostupnosti i zahtjev tajnosti.

Zahtjev sigurnosti osigurava nesmetano i neprekidno izvođenje svih funkcija određenog informacijskog sustava, što bi zapravo značilo osiguravanje stalnog i pouzdanog procesa prikupljanja, pohrane i obrade podataka u informacije, ali i pohranu te tumačenje i prezentaciju rezultata obrade podataka. Zahtjev dostupnosti uvjetuje da pristup svim ključnim informacijama mora biti dostupan svim ključnim korisnicima, koji su za to prethodno ovlašteni. Utvrđivanje ovlaštenja veoma je bitno kako bi se odredilo tko ima pristup i uvid u podatke, tko smije obavljati transakcije nad podacima, ali i tko je odgovoran za njihovo održavanje, odnosno promjenu, kopiranje i brisanje. Zahtjev tajnosti posljednji je zahtjev sigurnosti informacijskog sustava, a odnosi se na sve pojedinačne i privatne podatke i informacije koji moraju i smiju biti dostupni samo korisnicima koji su za to ovlašteni. Prilikom ispunjavanja zahtjeva tajnosti veoma je bitno razlikovati tajne i povjerljive podatke od privatnih. Povjerljivi i tajni podaci i informacije trebale bi biti dostupne isključivo uskom krugu ovlaštenih korisnika i biti pod posebnim sustavom zaštite. Primjer povjerljivih i tajnih podataka su opisi poslovnih procesa poduzeća, proces izrade proizvoda ili receptura, cijene proizvoda i marža i slično. Kako bi se zahtjev o tajnosti mogao održati, ovlašteni korisnici za pristupanje tajnim i povjerljivim podacima i informacijama dužni su potpisati posebne ugovore o čuvanju poslovne tajne. Privatni podaci su isto tako tajni, no oni ne predstavljaju poslovnu tajnu, već se radi o podacima o imovini, plaćama, zdravstvenom stanju pojedinih zaposlenika i slično. Privatnost i tajnost podataka uređena je i zakonom, odnosno Općom uredbom o zaštiti podataka ili GDPR-om (eng. General Data Protection Regulation).

Pojmovi *cyber* sigurnost i sigurnost informacijskih sustava često se izjednačavaju. Oba pojma podrazumijevaju razvijanje i implementaciju određenih kontrolnih mjera kako bi se ne samo poduzeća i organizacije, već i pojedinci štitili od informatičkih napada, krađa podataka i incidenata. Pojam *cyber* sigurnosti ipak se odnosi na veoma specifične metode kojima se želi spriječiti ili umanjiti posljedice stalnih opasnosti i rizika, obuhvaćajući pri tome organizacijske, tehnološke, ali i društvene segmente i napada i zaštite.

Kada se govori o upravljanju *cyber* sigurnošću, tada postoji nekoliko različitih pristupa upravljanja – inženjerski pristup, nacionalni pristup i ekonomsko-tržišni pristup. Korištenjem inženjerskog pristupa smatra se da je maksimalnu sigurnost moguće ostvariti korištenjem kriptiranja, robusnijih softvera, ali i tehničkih standarda. Nacionalni pristup smatra kako je ključ sigurnosti u otkrivanju, kako domaćih, tako i inozemnih, ilegalnih radnji koje utječu na nacionalne interese. Posljednji pristup je ekonomsko-tržišni, a on se ogleda u kreiranju ekonomskih i tržišnih sustava, odnosno regulativa, poreznih politika, obveza analize sigurnosnih incidenata, *cyber* osiguranja, kojih će se morati pridržavati svi dionici. Temeljni segmenti ovog pristupa su troškovi, materijalna i nematerijalna dobit, opstojnost i prilagodljivost. [9]

3.3. Pojam informatičkih i *cyber* rizika

„Rizik je opasnost ili vjerojatnost da će odgovarajući izvor prijetnje u određenim okolnostima predstavljati ranjivost sustava, čime se, posljedično, može počiniti neka šteta organizaciji.“ (Spremić, Korporativno upravljanje – Tipurić i suradnici)

„Informatički rizici (eng. IT risks) jesu rizici koji proizlaze iz intenzivne upotrebe informatike i informacijskih sustava i tehnologije kao važne podrške događanju i unaprjeđenju poslovnih sustava i poslovanja uopće.“ (Spremić, Korporativno upravljanje – Tipurić i suradnici)

Informatički rizici referiraju se na sve opasnosti i prijetnje koje uzrokuje sve veća primjena informatike u poslovanju, što u krajnjoj liniji dovodi do nekih neželjenih posljedica i šteta koje se očituju uglavnom u materijalnim i financijskim gubitcima. Utjecaj pojedinog rizika mjeri se stupnjem nastale štete, stoga je veoma bitno odrediti težinu i incidenciju pojavljivanja pojedinog rizika. Sve dalje sve je teže odrediti čvrste granice između poduzeća i organizacija, pa tako pojedini rizici utječu na sve sudionika pojedinih poslovnih procesa. Informatika u poslovanju često se pogrešno smatra zasebnom cjelinom u poduzeću, no upravljanje informatičkim rizicima nije problem samo informatičke organizacijske jedinice, već cijele organizacije. Informatički rizici imaju dva važna obilježja – stalna prisutnost i „dvostruku osobnost“. Bez obzira na to prihvaća li organizacija informatičke rizike ili ne, oni su sve dalje sve prisutniji zbog sve većeg korištenja tehnologije i digitalne transformacije. Dvostruka osobnost informatičkih rizika očituje se u vođenju informatike i informatičkih inicijativa. Informatika koja je u organizaciji dobro vođena, organizaciji stvara dodanu vrijednost, prilike i konkurentsku prednost, dok loše vođenje informatike može biti fatalno za poslovanje zbog akumuliranja troškova, frustracije zaposlenika, trošenja resursa, a ne stvaranja dodane vrijednosti. Kako bi se što bolje upravljalo informatičkim rizicima, potrebno je promatrati parametar frekventnosti pojave određenog rizika te težinu nekog rizika, odnosno njegov utjecaj na samo poslovanje. Svaki informatički rizik proizlazi iz postojanja i djelovanja određene prijetnje, koje se mogu očitovati kroz neovlašteni pristup tajnim i povjerljivim informacijama, ili pak njihovo nesvjesno odavanje, krađa resursa informacijskog sustava, hakerski napadi, društveni inženjering i slično. Svaku pojedinu prijetnju koja se identificira, potrebno je promotriti iz konteksta ranjivosti informacijskog sustava, odnosno u kojem dijelu bi određena prijetnja mogla izazvati ozbiljnu štetu za poslovanje. Prema Spremić, 2017. s obzirom na specifična područja poslovanja na koje se informatički rizici odnose, oni se mogu podijeliti na strateške, odnosno korporativne rizike, rizike provedbe informatičkih programa i projekata, rizike provedbe poslovnih procesa te infrastrukturne informatičke rizike. Strateški, odnosno korporativni rizici odnose se na sve rizike koji na bilo koji način ugrožavaju strateški poslovni interes, zbog nedonošenja ili pogrešnog donošenja odluka koje su vezane uz upotrebu

informacijske tehnologije i digitalne transformacije, što u konačnici nosi pozitivne učinke, inovaciju poslovnih procesa, te realizaciju definiranih poslovnih ciljeva. Strateški rizici poslovanju nanose iznimno veliku štetu i velike financijske gubitke, a nalaze se na najvišoj razini upravljanja informatičkim rizicima. Ova vrsta rizika zapravo se odnosi na nespremnost menadžmenta na prihvaćanje trendova digitalne transformacije poslovanja, zbog kojih poduzeće neće postati, ali ni ostati, konkurentno na tržištu. Sljedeća vrsta rizika odnosi se na rizike provedbe informatičkih programa i projekata. Ova vrsta rizika fokus stavlja na ulaganja u informatiku. Problem koji se ovdje javlja je pogrešno ulaganje, te neučinkovitost istih, što dovodi do da informatički projekti i programi poduzeću ne stvaraju nikakvu novu i dodanu vrijednost. Operativni rizici, tj. rizici koji se odnose na provedbu poslovnih procesa, su rizici digitalizacije postojećih poslovnih procesa, primjer ove vrste rizika su rizik integriteta podataka, rizik neovlaštenog ubacivanja podataka u informacijski sustav, rizik nedostupnosti informacijskog sustava, promjene softvera, nedostupnosti podataka, neovlaštenog pristupa programima i podacima, te njihova neovlaštena promjena… Infrastrukturni informatički rizici zapravo su vrsta rizika tehnološke prirode, odnosno rizici rada informatičke opreme. [10] [11]

3.4. Koncept i plan upravljanja informatičkim rizicima

Na temelju prethodnih poglavlja, jasno je kako informatički rizici nisu problem tehnološke prirode, već problem koji treba uvidjeti na korporativnoj razini, te je veoma bitno sastaviti i uvesti model korporativnog upravljanja informatičkim rizicima. Koncept upravljanja informatičkim rizicima sastoji se od pet aktivnosti koje valja provoditi: analiza stanja i identifikacija svih rizika, procjena težine i učestalost pojave te određivanje prioriteta, određivanje protumjera, kontrola i dodjela odgovornosti, testiranje učinkovitosti i djelotvornosti kontrola, te *portfolio* pristup rizicima i usklađenje sa strategijom poslovanja.

Korak analize stanja i identifikacije rizika ponekad zna predstavljati najizazovniji dio plana upravljanjem informatičkim rizicima upravo iz razloga što ne predstavlja samo popis svih mogućih informatičkih razloga, već sadržava i sve ostale dijelove upravljanja rizicima – pregled mogućih prijetnji, slabosti postojećeg sustava, kategorizaciju otkrivenih rizika, vjerojatnost pojedinog rizika, ali i događaje koji potiču razvoj rizika. Glavni cilj prvog koraka jest procjena utjecaja pojedinog rizika na poslovanje, kategorizacija prema kritičnosti, ali i vjerojatnost nastanka ili mogućeg uzastopnog pojavljivanja. Prilikom analize stanja potrebno je prikupiti što više informacija o postojećem informacijskom sustavu i infrastrukturi (hardver, softver, mreža, podaci, ovlašteni zaposlenici). Iako se glavnina fokusa stavlja na informacijski sustav i infrastrukturu, potrebno je prikupiti i informacije o misiji, viziji, strategiji poduzeća i stratešku važnost samog sustava za poduzeće. Revizori informacijskog sustava u ovom se koraku

uglavnom služe tehnikama anketiranja, kroz razne upitnike ili razgovore sa ključnim korisnicima informacijskog sustava i menadžmentom poduzeća. Osim direktnog anketiranja, pregledava se postojeća dokumentacija, promatra se rad sustava i na temelju svih prikupljenih informacija donose se zaključci.

Nakon analize stanja i klasifikacije informatičkih rizika potrebno je procijeniti njihovu težinu i odrediti prioritete. U drugom koraku plana potrebno je definirati ključne varijable funkcija rizika, odnosno imovinu poduzeća, moguće prijetnje i ranjivost. Imovina poduzeća nije samo sve ono što poduzeće posjeduje, već i sve ono što donosi nekakvu vrstu poslovne vrijednosti. Imovina može biti materijalna ili nematerijalna. Za neke dijelove imovine moguće je odrediti poslovnu vrijednost i moguću štetu koja može biti nanijeta, no za nematerijalnu imovinu, poput softvera, vrlo je teško odrediti potencijalni gubitak ili moguću nastalu štetu. Prijetnja se može definirati kao loša namjera neke osobe, odnosno postupanje koje nije u skladu sa politikom i ciljevima poduzeća ili organizacije, no osim toga, moguće su i prirodne prijetnje (poplave, potresi, prirodne katastrofe i slično). Ljudski faktor uvijek predstavlja najveću prijetnju, iz razloga što ne mora uvijek biti nužno namjerno, već prijetnja može proizaći iz slučajne pogreške. Osim slučajnih, ili namjernih, pogrešaka, postoji vjerojatnost i slučajnog događaja ili neke nenamjerne aktivnosti, koja može uzrokovati određenu slabost sustava. Iako se radi o slučajnim događajima i nenamjernim aktivnostima, one uvelike mogu ugroziti rad samog sustava. Neki od tih događaja su požari ili poplave, na koje ne postoji preveliki utjecaj, ali ipak je moguće unaprijed poduzeti određene mjere koje će ili spriječiti štetu ili ju ublažiti. Iduća prijetnja su sve namjerne aktivnosti koje ugrožavaju sustav i nanose štetu sustavu, a posljedično i cijelom poslovanju. Namjerne aktivnosti zapravo spadaju u čimbenike unutar poduzeća ili organizacije, te su uglavnom počinjene od strane zaposlenika. Čimbenici van okruženja poduzeća također se mogu odnositi na napade i korištenja zlonamjernih kodova, ali ovaj puta od strane računalnih hakera, kriminalaca ili pak poslovnih konkurenata. Ranjivost je pojam koji se odnosi na svaku slabost bilo kakve imovine poduzeća, a kada se radi o informacijskim sustavima, odnosi se na politiku sigurnosti, dizajn, algoritme i slično. Svaki rizik ima određeni utjecaj na poslovanje i mjeri se određenom visinom štete. Usporedno s visinom štete koja se mjeri, vrlo je važno odrediti težinu i vjerojatnost pojavljivanja pojedinog informatičkog rizika. Kako bi se to moglo odrediti, bitno je pratiti i analizirati sve prijetnje koje su moguće, povezati ih s potencijalnim slabostima sustava, odnosno ranjivosti, odrediti u kolikoj se mjeri pojedini rizik može tolerirati, te odrediti mjere uz pomoć kojih se pojedina slabost može izbjeći ili umanjiti do nekog prihvatljivog nivoa. Kako bi se procijenili intenziteti informatičkih rizika, koriste se kvalitativne i kvantitativne metrike. Kvantitativne metrike najčešće se bave određenim brojčanim iznosima, uglavnom financijskim gubitcima, a temelje se i na izravnoj i neizravnoj šteti. Kvalitativne metrike procjenjuju rizike kao kritične, visoke,

srednje i nisko rizične. Ukoliko se radi o kritičnom riziku, tada znači da je vjerojatnost da dođe do neželjenog događaja veoma visoka, odnosno da je sustav prilično ranjiv, te da je utjecaj rizika na poduzeće izrazito negativan. Određivanje prioriteta i sam način na koji će se rizicima upravljati, određuje se na temelju vjerojatnosti i učestalosti nastanka pojedinog neželjenog događaja te na temelju utjecaja rizika na poslovanje (engl. *BIA – Business impact analysis*).

Kako bi se rizici izbjegli, ili bi se načinjena šteta umanjila, važan je korak određivanja protumjera. Strategije koje se pojavljuju u uobičajenim scenarijima upravljanja informatičkim rizicima su prihvaćanje rizika, smanjivanje intenziteta, izbjegavanje rizika i podjela rizika. Strategija prihvaćanja rizika znači da je menadžment upoznat s određenim rizikom, te da je rizik pod konstantnom kontrolom, kako bi rizik bio unutar unaprijed dogovorenih korporativnih pravila. U trenutku kada rizik pređe razinu koja je prema korporativnim pravilima prihvatljiva, tada se poduzimaju određene mjere smanjenja. Smanjivanje intenziteta rizika strategija je kod koje poduzeće poduzima aktivnosti kojima se smanjuje ili ranjivost sustava ili ozbiljnost određenog rizika. Treća strategija je kada poduzeće u skladu sa korporativnim pravilima izbjegava sve rizike u najvećoj mogućoj mjeri. Posljednja strategija je strategija podjele rizika, odnosno, prebacivanje rizika na drugu stranu, primjerice kroz kupovinu police osiguranja. Nakon svih prethodnih koraka, slijedi dodjela odgovornosti i provođenje plana upravljanja. [10] [11]

3.4.1. Principi, okvir i proces upravljanja IT rizicima prema normi ISO 31000:2009

Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization – ISO*) 2009. godine izdala je međunarodnu normu ISO 31000. Norma se odnosi na dizajn, provedbu i održavanje upravljanja rizicima. Kao što je već prethodno navedeno u radu, rizik je sastavni dio suvremenog poslovanja, stoga upravo ova norma opisuje način na koji bi se organizacije trebale postaviti prema upravljanju istima, odnosno, prema identifikaciji, analizi te procjeni rizika i njihovih učinaka. Norma ISO 31000:2009 ne odnosi se ni na koju specifičnu industriju, već je primjenjiva na bilo koju vrstu organizacije, pa čak i pojedinca. Norma je organizirana u tri ključne odredbe – načela ili principe, okvir i proces upravljanja rizicima.

Principi norme ISO 31000:2009 govore o tome kako upravljanje rizicima stvara, ali i štiti vrijednost svake organizacije ili poduzeća, dio je donošenja odluka, te bi trebao biti sastavni dio svih organizacijskih procesa poduzeća, izričito se bavi nesigurnošću, te se temelji na najboljim dostupnim informacijama. Osim toga, veoma je bitno da upravljanje rizicima ne bude samo trenutno, kad rizik već ozbiljno zaprijeti ili nanese nekakvu štetu, već da bude sustavan, strukturiran i pravovremen. Upravljanje rizicima, iako je na neki način veoma generalan pojam,

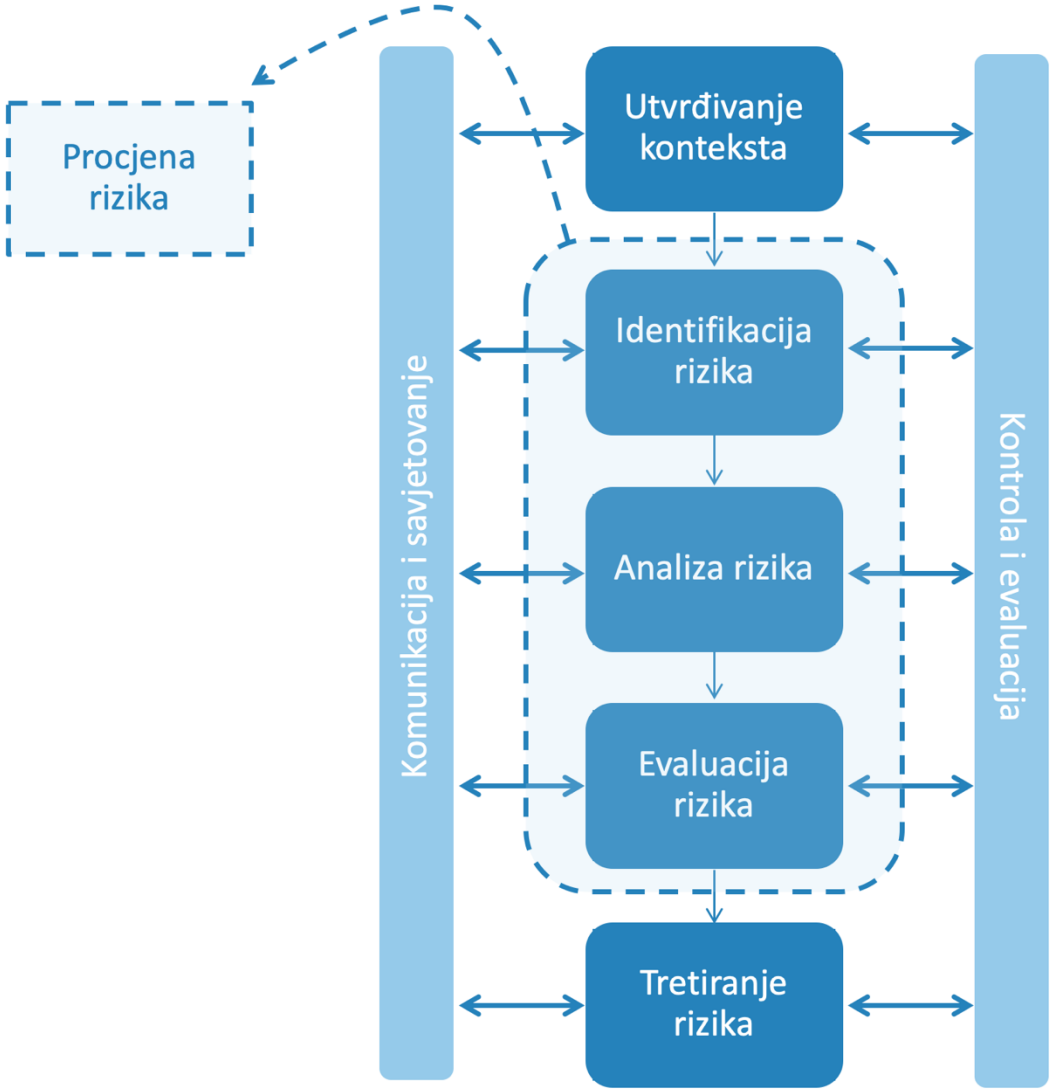
važno je da bude prilagođeno svakoj organizaciji, struci i industriji, te da u obzir uzima sve ljudske i kulturne čimbenike. Uzimanje o obzir svih ljudskih čimbenika, znači da bi upravljanje rizicima itekako trebalo biti transparentno i uključivo, na način da svi članovi nekog kolektiva budu upoznati i mogu prepoznati i identificirati pojedine rizike, analizirati ih i procijeniti. Osim činjenice da bi upravljanje rizicima trebao biti sustavan, strukturiran i pravovremen proces, važno je da bude iterativan, no to ne znači da se svim rizicima pristupa na isti način ili pak da se rizicima godinama upravlja na isti način, već da ovaj proces treba biti dinamičan i agilan. Agilnost ovog procesa označava pravovremene reakcije na sve promjene u poslovanju, te prilagodbu na sve interne i eksterne promjene. Posljednje načelo norme ISO 31000:2009 upravljanje rizicima označava kao kontinuirano poboljšanje svake organizacije.

Okvir norme ISO 31000:2009 odnosi se na učinkovitije upravljanje rizicima kroz primjenu procesa upravljanja rizicima, osiguravanje potpunih i ispravnih izvješća o svim rizicima koji su izvedeni iz procesa upravljanja istima, te osiguravanje da se upravo ta izvješća koriste za daljnje donošenje relevantnih odluka i definiranje odgovornosti na svim razinama svake organizacije. Okvir norme zapravo prikazuje na koji način su sve komponente upravljanja rizicima povezane.

Slika 1 - Prikaz okvira norme ISO 31000:2009 (Prema: PECB, 2015.)

Okvir se sastoji od pet različitih komponenata. Prva komponenta odnosi se na ovlast i predanost procesu upravljanja rizika. Uprava i menadžment svake organizacije treba svojim primjerom pokazati cijelom kolektivu predanost prema kontinuiranom i pravovremenom upravljanju rizicima. Menadžment i uprava moraju zajedničkim snagama definirati politiku upravljanja rizicima, ciljeve upravljanja rizicima, osigurati zakonsku i regulatornu usklađenost, osigurati raspodjelu svih potrebnih i postojećih resursa za upravljanje rizicima te prikazati sve pozitivne ishode upravljanja rizicima cjelokupnom kolektivu. Iduća komponenta odnosi se na dizajniranje okvira za upravljanje rizicima koji se mora definirati prije same implementacije. Ova komponenta trebala bi sadržavati razumijevanje same organizacije, uspostavu politike za upravljanje rizicima, osiguravanje svih odgovornih i kompetentnih zaposlenika za upravljanje rizicima, integriranje procesa upravljanja rizicima u sve organizacijske procese, alokaciju resursa te uspostavu pravilne interne i eksterne komunikacije, kojom će se zatim i na pravilan način komunicirati i izraditi izvještaji. Treća komponenta odnosi se na implementaciju okvira i procesa upravljanja rizicima. Nakon same implementacije potrebno je nadgledati i na neki način recenzirati okvir kako bi se osigurala učinkovitost samog upravljanja rizicima. Organizacija bi u ovom koraku trebala mjeriti uspješnost upravljanja rizicima, ali i određeni napredak, zatim razmotriti je li došlo do kakvih promjena u poslovanju i poslovnom okruženju, te u skladu s time pregledati je li okvir upravljanja rizicima i dalje aktualan i učinkovit. Obzirom na rezultate ovog koraka, javlja se sljedeća komponenta, odnosno kontinuirano poboljšanje samog okvira.

Proces upravljanja rizicima posljednja je komponenta ili klauzula norme ISO 31000:2009. Norma ISO 31000:2009 naglašava kako uspjeh upravljanja rizicima uvelike ovisi o učinkovitosti samog menadžmenta, te kako bi proces upravljanja rizicima zapravo trebao biti sastavni dio menadžmenta svake organizacije, na neki način ukorijenjen u kulturu i praksu svake organizacije, te prilagođen, odnosno prilagodljiv svim poslovnim procesima svake organizacije. Proces upravljanja rizicima prema ovoj normi sastoji se od nekoliko komponenata.



Slika 2 - Prikaz procesa upravljanja rizicima prema normi ISO 31000:2009 (Prema: PECB, 2015.)

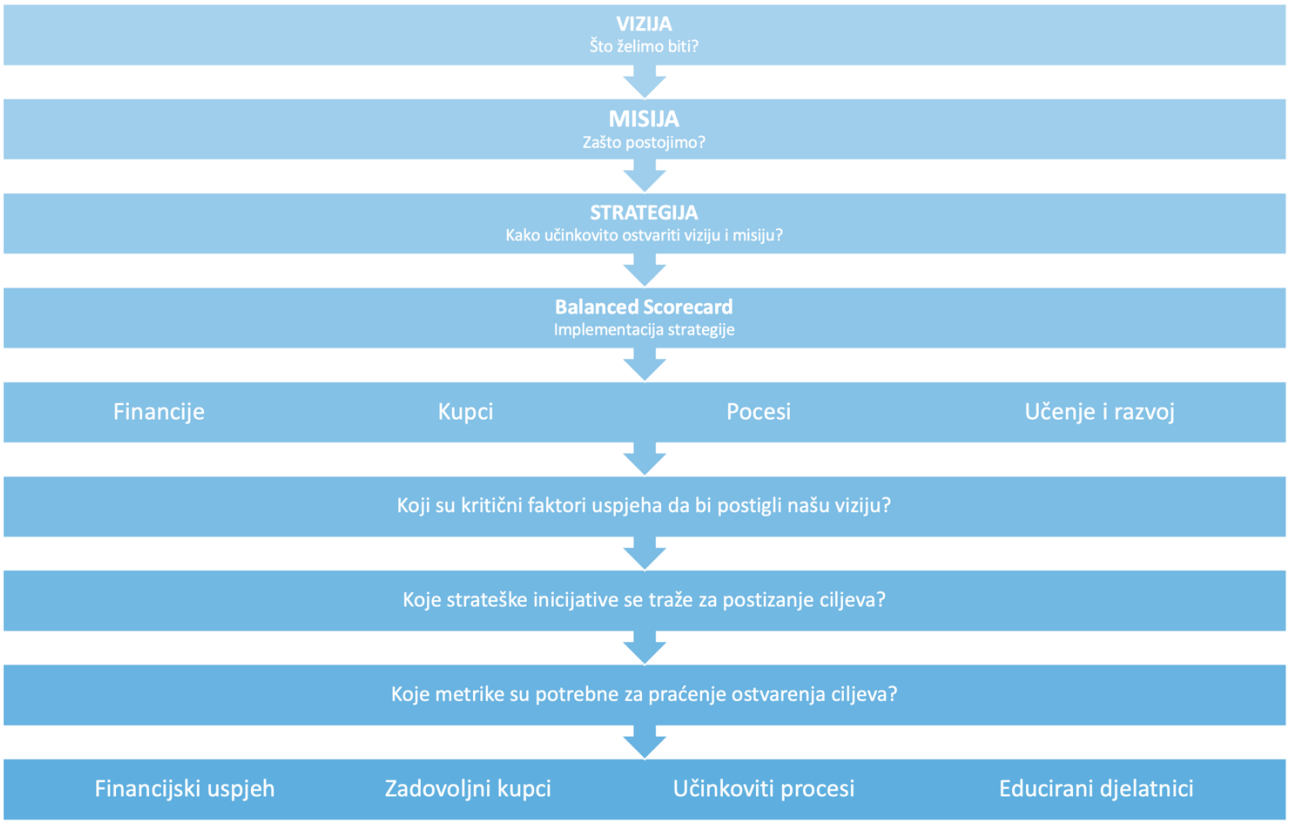
Prva komponenta odnosi se na procjenu rizika, kao cjelovit proces identifikacije, analize te evaluacije rizika. Komponenta utvrđivanja konteksta odnosi se na definiranje ciljeva, svih internih i eksternih parametara koji bi se trebali uzeti u obzir prilikom upravljanja rizicima, te na definiranje kriterija te opsega rizika. U tom lancu procesa, posljednja komponenta odnosi se na tretiranje rizika, odnosno na sve opcije koje bi se trebale sagledati nakon procjene rizika, sve očekivane troškove koje bi implementacija mogla donijeti, te benefite svake od opcija. Komponenta komunikacije i savjetovanja odnosi se na komunikaciju sa internim i eksternim *stakeholderima*, koja je veoma bitna i trebala bi se odvijati dvosmjerno u svakoj fazi procesa upravljanja rizicima. Kontrola i evaluacija posljednja je komponenta, koja se odnosi na provjeru i ocjenu procesa upravljanja rizicima, te eventualna modificiranja prema trenutnim potrebama poslovanja. [8]

4. Balanced Scorecard metoda

Balanced scorecard metoda je koju su kreirali profesor računovodstva na Sveučilištu Harvard, Robert Kaplan, i konzuntant David Norton. Početkom 90-ih njih su dvojica počela istraživanje o metodama mjerenja učinka iz razloga što se počelo vjerovati kako za uspješnost poduzeća više nisu ključni samo financijski pokazatelji. Kaplan i Norton, zajedno sa svojim suradnicima, vjerovali su kako fokusiranje isključivo na financijske pokazatelje utječe na učinkovitost stvaranja novih i dodanih vrijednosti u poduzeću. Nakon određenog vremena i razmatranja nekoliko različitih rješenja, odlučili su se za ideju *Balanced scorecard* koja objedinjava četiri perspektive – klijenti, poslovni procesi, zaposlenici i dioničari. S vremenom su organizacije počele prihvaćati *Balanced scorecard* kao metodu kojom provode svoju strategiju u djelo kroz navedene čimbenike.

Balanced scorecard metoda može se definirati kao skup mjera koje se mogu kvantificirati, a proizlaze iz strategije neke organizacije ili poduzeća. Kompleksnost *Balanced scorecarda* ogleda se u tri načina definiranja metode, odnosno može se tumačiti kao komunikacijski alat, sustav mjerenja ili sustav strateškog upravljanja organizacijom. *Balanced scorecard* svaku organizaciju gleda kroz četiri perspektive, upravo iz razloga što samo jedan čimbenik nije dovoljan za mjerenje napretka, ili nazadovanja, organizacije. Kroz perspektivu klijenta analiziraju se odgovori na pitanja tko su ciljani klijenti, što oni očekuju od organizacije, te koja je dodana vrijednost koju organizacija može pružiti svojim klijentima. Svako ovo pitanje organizacijama koje analiziraju poslovanje kroz perspektivu klijenata, to predstavlja prilično velik izazov. Nakon određivanja ciljane skupine klijenata, određuje se pristup dodanoj vrijednosti i klijentima – operativna izvrsnost, vodstvo u proizvodu i prisnost s klijentima. Operativna izvrsnost odnosi se na praktičnost i nisku cijenu proizvoda ili usluge u odnosu na konkurenciju. Pristup vodstva u proizvodu odnosi se na konstantno inoviranje, poboljšavanje postojećih proizvoda i ponudu najboljih proizvoda na tržištu. Prisnost s klijentima treći je pristup u kojem se organizacija fokusira na lojalnost svojih klijenata, odnosno izgradnju dugoročnih odnosa. Druga perspektiva odnosi se na unutarnje poslovne procese organizacije te određivanje krucijalnih poslovnih procesa koji trebaju biti na najvišem nivou kako bi se organizacija nastavila razvijati. Ponekad je iz ove perspektive vidljivo kako je neke poslovne procese bolje kreirati iznova, a ne poboljšavati postojeće, kako bi se zadovoljila očekivanja i klijenata i dioničara. Perspektiva učenja i rasta zaposlenika u *Balanced scorecardu* pokazuje se kao svojevrsni pokretač ostalih perspektiva. Zaposlenici su temelj cijele organizacije, a upravo to naglašava ova perspektiva, koja u fokus stavlja ne samo vještine zaposlenika, dostupnost određenih informacija, već i zadovoljstvo zaposlenika i njihovu mogućnost napredovanja. Iako su zaposlenici pokretači svega ostalog, organizacije uglavnom tu

perspektivu ostavljaju za kraj i razvijaju na kraju, ukoliko uopće u potpunosti razvijaju, što je definitivno pogrešno. Posljednja perspektiva, za mnoge i najvažnija, jest financijska perspektiva, kao što je i za očekivati u svijetu profita. U financijskoj perspektivi uglavnom se promatraju klasični financijski pokazatelji kao što su profitabilnost, solventnost, iskorištavanje postojeće imovine, ulaganja, isplativost istih i slično.



Slika 3 - Prevođenje misije/vizije/strategije u strateške rezultate (Prema: Kozina M., 2017.)

Ova metoda naziva se i metodom uravnoteženih ciljeva, s obzirom na to da se kroz četiri perspektive razvijaju i postižu strateški ciljevi. Balanced Scorecard metoda na neki način prevodi i ocrtava misiju, viziju, strategiju i vrijednosti svakog poduzeća.

Slika 4 - Prikaz sadržaja Balanced Scorecarda (Prema: Niven, 2007.)

Misija označava svrhu svake organizacije, odnosno zašto određena organizacija ili poduzeće zapravo postoji. Misija je nešto, što se za razliku od strategije i svih ciljeva poduzeća, nikada uistinu ne ispunjava, što bi značilo da je misija svojevrsna nit vodilja. Promjene u organizaciji ne donosi misija, već bi ih trebala nadahnuti, gurati organizaciju prema naprijed i poticati pozitivan rast organizacije. Vizija, strategija i planovi mijenjaju se sukladno trendovima u poslovanju, dok bi misija trebala definirana na način da traje i da postaje temeljem organizacije na kojima će se donositi sve važne buduće odluke. Bez obzira na struku i industriju, misija bi trebala biti definirana na način da je razumije svatko tko čita. Osim lakog razumijevanja, važno je da bude i pamtljiva, da dopire ne samo do zaposlenika, već i do klijenata i krajnjih korisnika, kako bi svi zajedno pojedinu organizaciju gurali prema naprijed.

Obzirom na brzinu promjena u trenutnom poslovanju, konkurentska prednost proizlazi iz mnoštva različitih faktora. Svaku organizaciju vode neka bezvremenska načela, koja zapravo predstavljaju vrijednosti pojedine organizacije. Vrijednosti se ne očituju samo kroz uvjerenja unutar organizacije i internu suradnju zaposlenika, već i kroz svakodnevno ponašanje zaposlenika prema svim vanjskim suradnicima. Vrlo često vrijednosti koje postaje u organizaciji, predstavljaju čvrsta uvjerenja osnivača ili direktora, kao što roditelji imaju velik utjecaj na svoju djecu, tako i osnivači poduzeća imaju velik utjecaj na samo poduzeće.

Na temelju misije i vrijednosti poduzeća, odnosno onoga zašto pojedina organizacija postoji i vodećih načela, kreira se vizija poduzeća. Vizija poduzeća predstavlja budućnost organizacije i sve ono što organizacija želi postići u navedenom vremenskom periodu. Bitno je da opisi vizije ne bude apstraktan, već da što jasnije i detaljnije prikazuje sliku željenog *TO-BE*

stanja. Elementi vizije, koji su najčešće obuhvaćeni, su željeni opseg poslovnih aktivnosti, kako će na poduzeće gledati sve zainteresirane strane (i interne i eksterne, klijenti, zaposlenici, suradnici…), područja vodstva, kompetencije i vrijednosti u koje se vjeruje. Jedna od karakteristika svake uspješne vizije jest sažetost. Najbolja vizija ona je koja momentalno privlači pažnju svakog tko je čita, što bi značilo da su često one najjednostavnije upravo i najsnažnije. Vizija je svojevrstan slogan poduzeća za budućnost. Mnogo interesnih skupina surađuje u poslovanju, radu i napretku poduzeća, pa je bitno da vizijom budu zadovoljni svi – uprava, zaposlenici, klijenti, krajnji korisnici, investitori, dioničari… Kao što je već prethodno navedeno, važno je da vizija bude u skladu sa misijom i vrijednostima, a osim toga, treba biti povjerljiva i izvediva. Posljednja karakteristika uspješne vizije jest nadahnuće.

Posljednji aspekt Balanced Scorecarda nekog poduzeća jest strategija. Strategija je pojam koji se prilično teško definira u poslovnom svijetu, pa tako neki strategiju vide kao plan (ili planove) na nekoj višoj razini koje kreira i donosi menadžment, nekima je strategija jednaka najboljim praksama, dok neki smatraju kako su to veoma specifične i detaljne aktivnosti koje poduzeće poduzima kako bi ostvarilo željenu budućnost. [6]

4.1. Primjer izrade strateške mape Balanced Scorecard alatom

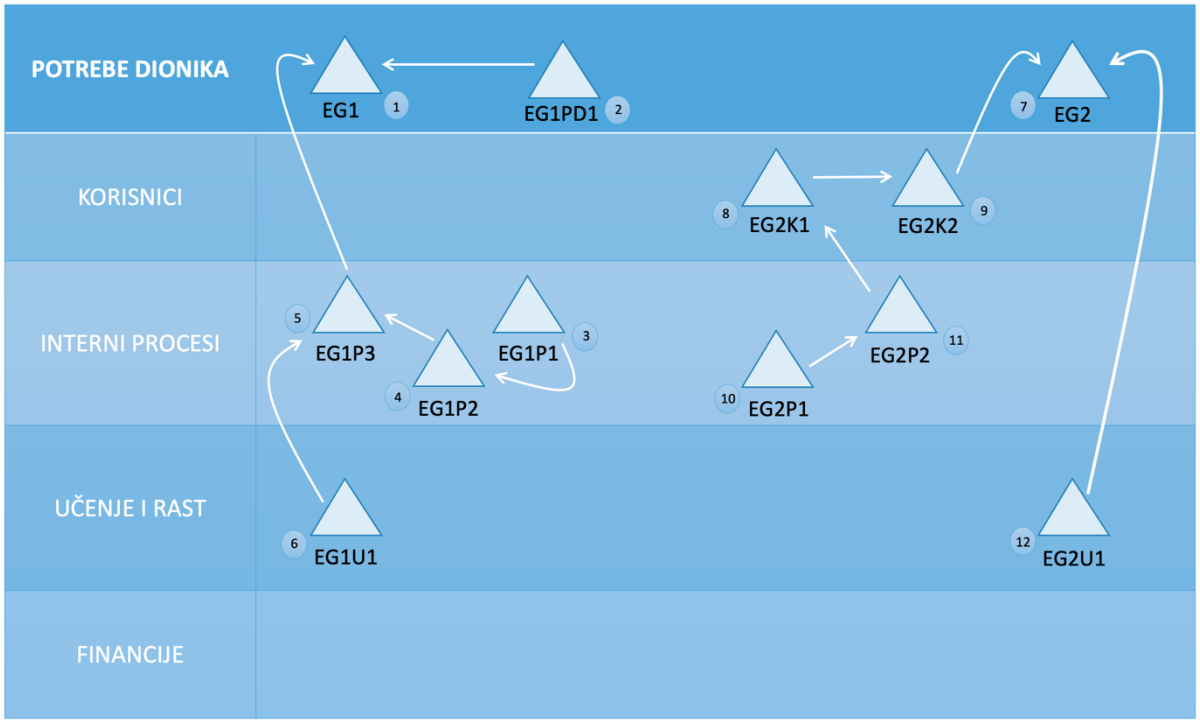
Kao što je već nebrojeno puta navedeno, Balanced Scorecard je vrlo primjenjiv alat, neovisno o veličini ili vrsti organizacije, struci te industriji. Za izradu vlastitog primjera strateške mape i određivanja strateških ciljeva alatom Balanced Scorecard, odabrala sam neprofitnu organizaciju VI. osnovnu školu Varaždin. VI. osnovna škola Varaždin jedna je od sedam gradskih škola grada Varaždina, osnovana 2. rujna 1967. godine pod prvotnim imenom „8. maj“. Škola je u usporedbi sa ostalim gradskim školama prilično velika, te u školskoj godini 2020./2021. broji 104 zaposlenika, od čega je 36 učitelja predmetne nastave, 16 učitelja razredne nastave, 8 učitelja u produženom boravku, 4 stručna suradnika, 4 pripravnika i 31 ostali zaposlenik. Važno je naglasiti kako među zaposlenima nema nestručnih učitelja. Škola ima 32 razredna odjela i 772 učenika, školsku knjižnicu i kuhinju, dvije sportske dvorane i igrališta te šest specijaliziranih učionica. Kroz razne izvannastavne aktivnosti i natjecanja, škola nastoji svojim učenicima pružiti što više raznovrsnih znanja i iskustava, te nadopuniti formalno obrazovanje. Škola konstantno sudjeluje u međunarodnim, te Erasmus projektima, sa školama diljem Europe. Osim ulaganja u učenike, škola ulaže i u svoje zaposlenike, kroz stalna napredovanja, aktivnosti i *job shadowinge*.

Zbog velikog broja učenika i stalnog rasta, škola se nadograđivala već nekoliko puta, kako bi se stvorili adekvatni uvjeti za rad. U posljednjem nadograđivanju napravljena je velika

nova sportska dvorana, knjižnica, te uz opće, nekoliko specijaliziranih učionica za informatiku, kemiju i biologiju.

U trenutnim izvanrednim okolnostima, škola se, kao cjelina, odlučila za rad u virtualnim učionicama kreiranim u Microsoft Teams platformi, kako bi se što bolje savladali nastavni sadržaji obrađivani tijekom nastave na daljinu. Učenici koji se nalaze u samoizolaciji, u kontaktnu nastavu mogli su se uključivati u realnom vremenu kako bi pratili nastavu te ne bi bili na gubitku.

Prilikom kreiranja ove strateške mape pronašla sam misiju – „Programi i aktivnosti kreativne, individualizirane i istraživačke nastave koji potiču partnerske odnose s roditeljima i doprinose razvoju kompetencija učenika.“ i viziju – „Škola i roditelji zajedno uvažavajući različitosti razvijaju kreativnost, odgovornost i ekološku svijest na putu usvajanja znanja i pripreme za svladavanje životnih izazova. Strateški ciljevi koje sam pronašla kroz suradnju sa zaposlenicima VI. osnovne škole Varaždin su „unaprijediti načine učenja i poučavanja“ te „unaprijediti organizaciju nastave“. Ova dva strateška cilja vrlo su generalizirana stoga sam ih odlučila detaljnije razraditi.



Slika 5 - Prikaz izgleda strateške mape za odabranu organizaciju (Izvor: autorica)

Obzirom na to da se radi o neprofitnoj organizaciji, dodana je još jedna perspektiva – misija, odnosno potrebe dionika. Svaka perspektiva sastoji se od ciljeva i njihovih metrika. Ciljevi su povezani strelicama kako bi se stekao dojam koji cilj dalje utječe na koji. Na prethodnoj slici trokutići predstavljaju strateške ciljeve, dok su metrike označene plavim kružićima. U tablici br. 1 objašnjeni su strateški ciljevi, dok su u tablici br. 2 pojašnjene oznake i nazivi svih metrika,

te načini mjerenja. Strateški ciljevi označeni su oznakom **EG** (engl. enterprise goals), dok nastavak oznake pokazuje za koju su perspektivu vezani (u – učenje i rast, p – poslovni procesi, m – potrebe dionika (misija), k – korisnici). IT ciljevi označeni su oznakom **IT.**

Tablica 1 - Prikaz oznake cilja i pojašnjenje svakog strateškog cilja odabrane organizacije (Izvor: autorica)

Oznaka cilja	Strateški cilj organizacije
EG1	Unaprijediti načine učenja i poučavanja.
EG1U1	Napredovanje i zadržavanje stručnog kadra.
EG1P1	Omogućiti učenicima rad u modernim i opremljenim učionicama u svim područjima.
EG1P2	Proširenje ideja, uviđanje novih načina rada.
EG1P3	Omogućavanje kvalitetnijih uvjeta rada, posvećivanje učenicima kao pojedincima i zadržavanje stručnog kadra koji će napredovati i olakšati rad učenicima (bez stalnih promjena učitelja).
EG1PD1	Olakšavanje teškoća učenika uz pomoć stručne službe (psihologa, logopeda, rehabilitatora…).
EG2	Unaprijediti organizaciju nastave.
EG2U1	Zadržavanje stručnog kadra među učiteljima i zapošljavanje stručnog kadra u stručnoj službi kako bi se olakšala organizacija nastave i smanjilo opterećenje.
EG2P1	Nadogradnja škole kako bi se stvorili kapaciteti za organizaciju i izvođenje nastave za sve razredne odjele s početkom u isto vrijeme (jednosmjenska nastava u punom smislu riječi).
EG2P2	Organizacija cjelodnevne nastave.

EG2K1	Organizacija nastave na način da učenici svoje aktivnosti mogu ostvarivati na "jednom mjestu".
EG2K2	Povećanje broja izbornih i izvannastavnih aktivnosti kako bi se smanjio broj učenika koji ne pohađaju iste.

Tablica 2 - Prikaz metrika strateških ciljeva organizacije i pojašnjenje istih (Izvor: autorica)

Oznaka metrike	Naziv metrike	Način mjerenja
1	Unaprjeđenje načina učenja i poučavanja	Određivanje odnosa prosječnih ocjena za učitelje i predmete u odnosu na prošlu školsku godinu
2	Rad s učenicima s teškoćama	Broj sati rada s učenicima s teškoćama u odnosu na prošlu školsku godinu
3	Broj moderniziranih kabineta za nastavu	Broj opremljenih kabineta za nastavu u odnosu na prošlu školsku godinu
4	Pohađanje edukacija o nekonvencionalnim načinima rada	Broj provedenih edukacija u odnosu na prošlu školsku godinu
5	Broj učenika u razrednim odjelima	Smanjenje broja učenika u razrednim odjelima u odnosu na prošlu školsku godinu
6	Omogućavanje napredovanja učitelja u zvanje mentor/savjetnik/viši savjetnik	Broj novounaprjeđenih učitelja u viši stupanj zvanja
7	Unaprjeđenje organizacije nastave	Smanjenje broja sati nestručnih zamjena i prekovremenih sati
8	Povećanje broja sportskih i umjetničkih aktivnosti u organizaciji škole	Broj različitih izbornih i izvannastavnih aktivnosti u odnosu na prošlu školsku godinu

9	Povećanje broja izbornih i izvannastavnih aktivnosti za "svačiji ukus"	Broj učenika koji pohađa izborne ili izvan nastavne aktivnosti
10	Izvođenje nastave u jednoj smjeni za sve razredne odjele	Broj razrednih odjela u jednoj smjeni u odnosu na prošlu školsku godinu
11	Organiziranje cjelodnevne nastave	Broj faktora koji teži prema cjelodnevnoj nastavi u odnosu na prošlu školsku godinu
12	Omogućavanje rada učitelja u jednoj smjeni	Broj radnih dana u tjednu, u jednoj smjeni, u odnosu na prošlu školsku godinu

Tablica 3 - Prikaz IT ciljeva organizacije i njihovih oznaka (Izvor: autorica)

Oznaka cilja	IT cilj organizacije
IT1	Povećanje broja suradnji sa školama.
IT2	Povećanje broja suradnji sa poduzećima i obrtnicima.
IT3	Povećanje broja učenika uključenih u projekte.
IT4	Kvalitetno izvođenje nastave na daljinu.
IT5	Prihvaćanje digitaliziranih i interaktivnih materijala
IT6	Poboljšanje IT infrastrukture
IT7	Povećanje broja digitaliziranih materijala za nastavu
IT8	Stvaranje pametne učionice na otvorenom
IT9	Uvođenje alata za organizaciju nastave i kreiranje rasporeda
IT10	Veće korištenje sredstava iz EU fondova
IT11	Smanjenje vremena pripremanja za nastavu kroz korištenje digitalnih materijala
IT12	Edukacija svih zaposlenika

4.2. IT Balanced Scorecard

IT Balanced Scorecard, moglo bi se reći, podvrsta je klasične metode Balanced Scorecard. S vremenom, glavni direktori za informacijsku tehnologiju unutar poduzeća, odnosno CIO, shvatili su kako nije dovoljno upravljati samo IT-em unutar poduzeća, već kako je vrlo bitno IT strategiju integrirati unutar poslovne strategije. Svaki segment poslovanja uvelike je ovisan o tehnologiji, te se često povlači paralela između intelektualnog kapitala i tehnologije; intelektualni kapital je na neki način gorivo i pokretač za razvoj moderne tehnologije, a moderna tehnologija motor je koji pokreće ne samo pojedina poduzeća, već cijele industrije da napreduju silovitom brzinom. Sve je to vrlo lako reći, no kao što treba obratiti pažnju na pravilnu usmjerenost i iskorištavanje ljudskog kapitala, isto tako treba obratiti pažnju na vezu između tehnologije i strategije, odnosno na koji način doprinos informatičke tehnologije koristi u provođenju strategije poduzeća i ostvarenju strateških ciljeva.

Nakon temeljitog istraživanja o integraciji IT strategije u poslovnu strategiju i proučavanja mnoštva strateških mapa i rezultata, zaključak istraživanja jest da su najuspješnije strateške mape dijelile šest strukturalnih atributa:

- jednostavnost prezentacije strateške mape
- eksplicitna poveznica sa IT strategijom
- obvezivanje uprave
- definirane metrike prema standardima pojedinog poduzeća
- detaljne analize
- upravljanje troškovima (plaće, investicije…).

Jednostavnost strateške mape ogleda se u opisivanju iste kroz desetak metrika, ali u netehničkom vokabularu, kako bi strateška mapa bila razumljiva svakome tko ju čita. Strateška mapa isto tako mora biti usklađena sa planiranjem IT strategije, te mora sudjelovati u praćenju napretka u ostvarivanju IT ciljeva. Eksplicitna poveznica poslovne i IT strategije isto tako znači i povezanost IT i poslovnih menadžera, koji moraju zajedno raditi na stvaranju strateških mapa, definiranju ciljeva, te provođenju strategija. Definirane metrike prema standardu poduzeća u procesu kontrolinga i revizije olakšavaju posao. Ukoliko su sve metrike definirane kako treba, tada se u revizijskom dijelu više prostora ostavlja za fokus na same odluke, a ne na ponovnu raspravu oko metrika. Nakon definiranja metrika, važne su i detaljne analize koje pokazuju promjene u trendovima na tržištu, te pružaju bolji pogled na ključne elemente. Upravljanje troškovima također je bitna stavka, jer se na kraju krajeva usklađuje sa rezultatima provođenja strategije i ostvarivanja ciljeva, na temelju strateške mape.

Šest strukturalnih atributa jedan je aspekt IT Balanced Scorecarda. Drugi aspekt odnosi se na metrike koje su podijeljene u pet ključnih kategorija:

- financijske performanse
- izvedba projekata
- operativne performanse
- upravljanje ljudskim kapitalom
- zadovoljstvo korisnika.

Sve ove metrike u kontekstu Balanced Scorecarda zapravo pojašnjavaju same sebe. Osim navedenih pet metrika, pri izradi IT Balanced Scorecarda, dodane su još dvije metrike:

- informacijska sigurnost
- inicijative poduzeća.

Metrika koja se odnosi na informacijsku sigurnost prati napore u otklanjanju sigurnosnih ranjivosti, te praćenje politike i certificiranja. Primjeri ove metrike su postotak zaposlenika koji prolazi kroz treninge i tečajeve vezane uz informacijsku sigurnost, ali i postotak vanjskih suradnika i partnera s kojima se suradnja odvija u skladu sa sigurnosnom politikom i standardima poduzeća. Što se tiče inicijativa poduzeća, najbolji stručnjaci i praktičar za Balanced Scorecard naglašavaju kako su inicijative u IT-u od velike strateške važnosti za poduzeća. Primjer ove metrike jest postotak koraka poslovnih procesa koji potporu pronalaze u tehnologiji i korištenju IT-a.

Kao rezultat svih ovih istraživanja, za uspjeh koji se ogleda iz kreiranja strateške mape, integracije IT i poslovne strategije, te korištenja Balanced Scorecarda u postizanju ciljeva, profiltriralo se sljedećih šest kriterija:

- isporuka svakog novo dogovorenog segmenta na vrijeme i u okvirima budžeta
- isporuka svake nove funkcionalnosti prema ugovoru
- održavanje visokog standarda performansi sustava
- smanjenje oslanjanja na *legacy* sustave
- povećanje korisničkog zadovoljstva
- održavanje zadovoljstva zaposlenika.

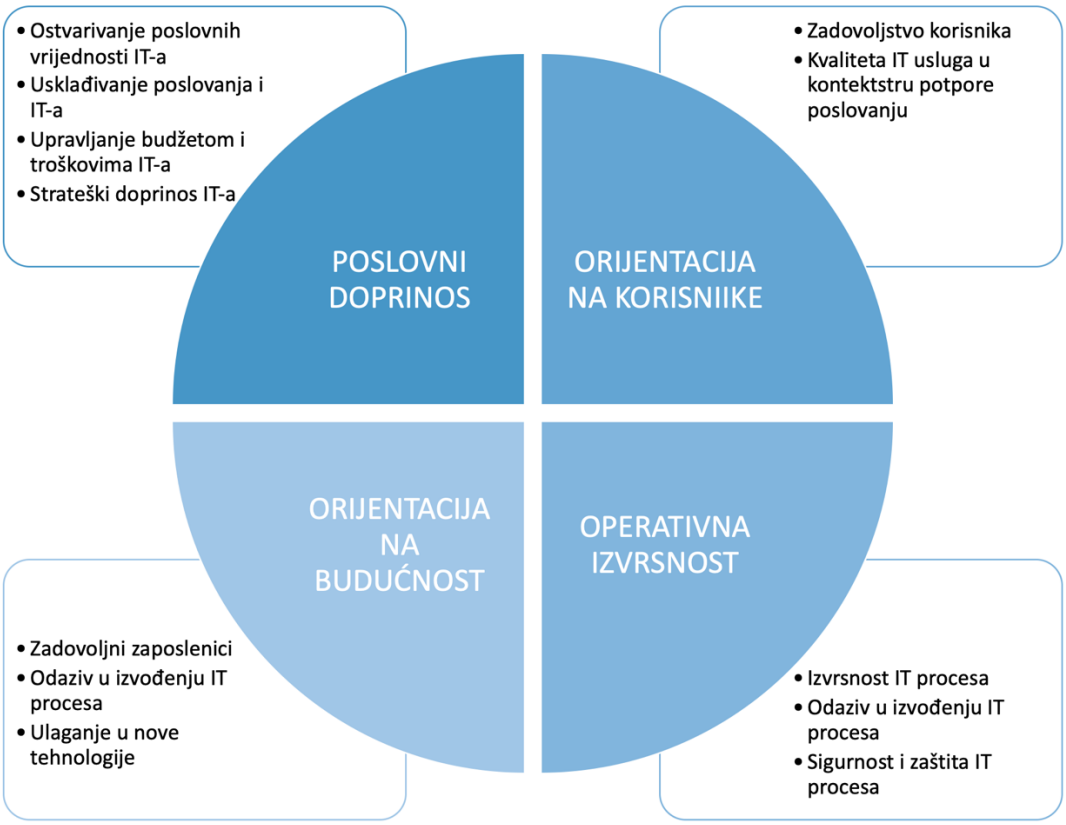
Još jedna veoma bitna stvar jest pomicanje IT-a iz okvira pružatelja usluga u okvir strateškog partnera. Ukoliko se gleda u okviru pružatelja usluga, informacijska tehnologija pomaže u učinkovitosti poduzeća, odvojiva je od poslovanja, trošak je koji se treba kontrolirati, IT menadžeri smatraju se isključivo tehničkim ekspertima, a budžeti vezani uz IT određuju se i vode prema nekim eksternim okvirima. Ukoliko se IT stavi u okvir strateškog partnera tada iz faktora koji samo pomaže u učinkovitosti poduzeća, prelazi u itekako bitan faktor u rastu ne

samo poslovanja, već cijelog poduzeća, postaje neodvojiv od poslovanja, više nije vidljiv kao trošak koji se treba kontrolirati, već kao investicija kojom se upravlja, a IT menadžeri od isključivo tehničkih stručnjaka postaju stručnjaci koji mogu rješavati poslovne probleme. Budžeti vezani uz IT više ne ovise o eksternim okvirima, već se vode prema poslovnoj strategiji poduzeća. [2][4]

4.2.1. Van Grembergenov IT Balanced Scorecard model

Van Grembergenov model jedan je od najpoznatijih modela IT Balanced Scorecarda. Model se sastoji od četiri kvadranta – orijentacija na korisnike, poslovni doprinos, operativnu izvrsnost i orijentaciju na budućnost. Orijentacija na korisnike postavlja pitanje na koji način korisnici vide IT odjel poduzeća, misija ovog kvadranta je biti preferirani isporučitelj informacijskih sustava, dok su ciljevi povećanje zadovoljstva korisnika, postizanje određene razine partnerstva s korisnicima, te postajanje preferiranog isporučitelja svih informacijskih proizvoda i usluga. Kvadrant poslovni doprinos postavlja pitanja kako poslovni menadžment unutar poduzeća vidi IT odjel, dok je misija ovog kvadranta isporuka poslovne vrijednosti IT-a. Ciljevi poslovnog doprinosa su ostvarivanje poslovne vrijednosti IT projekata, kontrola svih IT troškova, te isporuka novih poslovnih vrijednosti. Kvadrant operativne izvrsnosti postavlja pitanje koliko su zapravo IT procesi unutar poduzeća učinkoviti i adekvatni. Misija i ciljevi koji se ovdje javljaju, odnose se na isporuku učinkovitih i adekvatnih IT sustava i usluga. Posljednji kvadrant odnosi se na orijentaciju na budućnost gdje se postavlja pitanje u kojoj je mjeri IT pripremljen da u budućnosti može zadovoljiti potrebe poduzeća, te odgovoriti na promjene trendova koji će se javiti. Misija se odnosi na stvaranje mnoštva prilika za zadovoljavanje budućih zahtjeva i svladavanje izazova, dok su ciljevi orijentirani na educiranje i stručnost IT djelatnika, te istraživanje mogućih nadolazećih tehnologija.

Strateški ciljevi koji se javljaju kroz sve četiri perspektive IT BSC strateške mape moraju se na neki način mjeriti.



Slika 6 - Prikaz strateških ciljeva unutar perspektiva IT BSC strateške mape (Prema: Kozina M., 2017.)

Za svaki od navedenih strateških ciljeva postoji određena vrsta metrike, ili pak više njih, kojom se zatim može odrediti uspješnost definiranog cilja. Strateški cilj ostvarivanja poslovnih vrijednosti IT-a, ne odnosi se samo na kvantitativnu, već i na kvalitativnu dobit IT-a, a može se mjeriti analizom vrijednosti, povratom ulaganja ili ROI (engl. *Return on investment*), te kvalitetom izvođenja poslovnih procesa podržanih IT uslugama. Cilj usklađivanja poslovanja i IT-a najbolje se mjeri kvalitetom samog operativnog plana te planiranja ulaganja i troškova, odnosno kreiranjem budžeta. Nastavno na usklađenost poslovanja i IT-a te planiranja budžeta, cilj koji se odnosi na upravljanje troškovima IT-a, mjeri se kroz odnos stvarnih i planiranih troškova, dok se cilj strateškog doprinosa IT-a mjeri kroz postotak ispunjenih i ostvarenih strateških ciljeva. Sljedeća perspektiva odnosi se na orijentiranost na korisnike te su glavni ciljevi zadovoljstvo korisnika te kvaliteta IT usluga u kontekstu potpore poslovanju. Zadovoljstvo korisnika mjeri se kroz razna istraživanja i anketiranja, kvalitete usluge, ali i pristupačnosti usluge korisnicima. Kvaliteta IT usluge u kontekstu potpore poslovanju mjeri se kroz prosječno vrijeme odziva, raspoloživost IT usluge, ali i kroz sve funkcionalnosti koje usluga nudi svojim ključnim korisnicima. Perspektiva operativne izvrsnosti uglavnom se ogleda u IT procesima kroz ciljeve izvrsnosti, odaziva u izvođenju te osiguravanju sigurnosti i zaštite IT procesa. Izvrsnost IT procesa mjeri se kroz zrelost istih, učestalosti pojave incidenata, te

kroz kvalitetu i troškove izvođenja IT procesa. Odaziv u izvođenju IT procesa mjeri se kroz vrijeme trajanja izvođenja pojedinog IT procesa, dok se sigurnost i zaštita IT procesa provjeravaju kroz izvješća o reviziji sigurnosti. Posljednja perspektiva odnosi se na orijentaciju na budućnost te ciljeve zadovoljstva zaposlenika, ulaganja u nove razvojne tehnologije, ali i odaziv u izvođenju IT procesa, te se može primijetiti da se ovaj cilj dijeli sa perspektivom operativne izvrsnosti. Zadovoljstvo zaposlenika, također se kao i zadovoljstvo korisnika, mjeri putem anketa, ali kroz osobni napredak i viziju zaposlenika u poduzeću. Ulaganje u nove razvojne tehnologije mjeri se kroz kvantitativnu metriku, odnosno kroz troškove ulaganja, dok je metrika za cilj odaziva u izvođenju IT procesa, jednaka kao i u prethodnoj perspektivi. [2]

5. CobiT

CobiT je jedan od okvira i normi koji informatiku gledaju kao sredstvo povezivanja poslovanja. Osim informatike kao sredstvo povezivanja poslovanja, CobiT, jednako kao i IT Balanced Scorecard informatiku vidi kao strateški resurs poslovanja. CobiT (engl. *Control Objectives for Information and Related Technology*) okvir je koji se koristi za korporativno upravljanje informatikom. Ovaj okvir nastao je 1992. godine, te je prvenstveno bio namijenjen za provedbu poslovnih aktivnosti i ostvarivanja ciljeva kako bi ih zapravo informatički dio poslovanja mogao podržati. CobiT je namijenjen velikom broju korisnika, te je primjenjiv u svim strukama i industrijama. CobiT određuje i opisuje informatičke procese, koja svrstava u određena područja, definira obaveze i područja odgovornosti, određuje ciljeve nadzora i kontrole, te ciljeve i metrike uspješnosti informatičkih procesa. Od samog razvoja ovog okvira, konstantno se nadograđivao, tako da je trenutno aktualna verzija 5 CobiT-a, odnosno CobiT 5. CobiT 1 naglasak je stavljao na reviziju, CobiT 2 na kontrolu, CobiT 3 na upravljanje, odnosno na mendažment, a CobiT 4 na korporativno upravljanje. CobiT 5 organizacijama i poduzećima koja koriste ovaj okvir omogućuje uravnoteženo korištenje resursa, ostvarivanje koristi, te optimizaciju rizika, a sve to uz značajno poboljšanje poslovnih rezultata i sve veće podržavanje poslovanja od strane informatike.

Pod pojmom CobiT 5 ne podrazumijeva se samo okvir, već metodologija, koja sadrži dvije vrste preporuka, jedna za korporativno upravljanje informatikom i druga za operativno upravljanje informatikom. Broj informatičkih procesa je povećan, te postoji čak 300 veoma detaljnih kontrola koje se dijele u pet kategorije:

- procjena, smjernice i nadzor (engl. *Evaluate, Direct and Monitor, EDM*)
- usklađivanje, planiranje i organizacija informatike (engl. *Align, Plan and Orrganize, APO*)
- izgradnja, akvizija i implementacija informacijskog sustava (engl. *Build, Aquire and Implement, BAI*)
- isporuka, usluge i potpora radu informacijskog sustava (engl. *Deliver, Service and Support, DSS*)
- nadzor, provjera i procjena (engl. *Monitor, Evaluate and Assess, MEA*)

U nastavku diplomskog rada i u istraživanju, koriste se procesi iz kategorije korporativnog upravljanja informatikom (*EDM*), procesi iz kategorije operativnog upravljanja informatikom (*APO*) te iz kategorije koja obuhvaća izgradnju, akviziciju i implementaciju informacijskog sustava (*BAI*).

Cijela IT industrija rapidno raste i vrlo brzo se mijenja. Kako bi se u informatičkom odjelu, nekog poslovnog sustava odredile sve potrebe i želje dionika, tada je upravo to praćenje promjena i trendova određena polazišna točka. Svako poduzeće ima svoje specifične ciljeve, CobiT 5 jedan je od načina identificiranja ciljeva na najvišoj razini, ali i kaskadiranja na operativne ciljeve. [7][10]

Slika 7 - Prikaz određivanja i kaskadiranja ciljeva prema okviru CobiT 5 (Prema: Spremić M., 2017.)

CobiT 5 sastoji se od pet različitih principa koji se koriste kako bi se u poduzećima mogla stvoriti i održati ravnoteža, a ovi se principi mogu primijeniti na bilo koju vrstu poduzeća, bez obzira na starost, veličinu, struku ili industriju. Glavni principi su:

- Princip 1: Zadovoljavanje potreba dionika
- Princip 2: Pokrivanje cijelog poduzeća
- Princip 3: Primjena jedinstvenog integriranog okvira
- Princip 4: Omogućavanje holističkog pristupa
- Princip 5: Odvajanje vodstva od menadžmenta

Trenutno se naglasak stavlja na Princip 1: Zadovoljavanje potreba dionika. Ovaj princip fokus stavlja na upravljanje, pregovaranje te donošenje odluka o svim, često veoma različitim, željama, zahtjevima i potrebama dionika. Princip 1 na neki način osigurava da kada se god donose odluke o bilo kakvim benefitima, korištenju resursa ili pak procjene rizika, u obzir se moraju uzeti potrebe dionika.

6. Istraživanje

Istraživanje za potrebe diplomskog rada napravljeno je na primjeru neprofitne organizacije, VI. osnovne škole u Varaždinu. Za istraživanje je prije svega bila potrebna iznimno dobra suradnja sa zaposlenicima kako bi se mogao dobiti uvid u sve potrebne podatke za izradu istraživanja.

6.1. Protokol istraživanja

Kako bi se istraživanje moglo uspješno odraditi, za početak je najbitnije kreirati protokol istraživanja čiji se vizualni prikaz nalazi na slici 8.

Slika 8 - Prikaz protokola istraživanja (Izvor: autorica)

Nakon kreiranja protokola istraživanja i stupanja u kontakt sa zaposlenicima (učiteljima i stručnom službom), potrebno je bilo proučiti sve dane dokumente koji se povezuju sa strateškim ciljevima organizacije, te misije i vizije organizacije. U poglavlju Balanced Scorecard prikazana je strateška mapa napravljena na temelju dokumentacije te razgovora sa zaposlenicima. Nakon popisa strateških ciljeva te razrađene strateške mape, potrebno je bilo definirati i IT ciljeve. Sve zahtjeve i potrebe dionika važno je povezati, odnosno mapirati, sa strateškim ciljevima, dok je potom strateške ciljeve važno povezati sa IT ciljevima organizacije. Prilikom povezivanja ključno je ciljeve podijeliti prema prethodno navedenim BSC perspektivama. Nakon što su svi ciljevi međusobno povezani, istraživanje se nastavlja uz pomoć CobiT 5 okvira, te su IT ciljevi organizacije povezani sa IT procesima prema CobiT 5 okviru. Povezivanje sa IT procesima CobiT 5 okvira bitno je za nastavak istraživanja, odnosno identifikaciju prijetnji. Nakon što su kroz razgovor sa zaposlenicima identificirane prijetnje, određena je i vjerojatnost da se neka od njih dogodi, te koliki su razmjeri posljedica svake pojedine prijetnje. Razina svakog rizika i način tretiranja istih, određen je kroz omjer vjerojatnosti dao se pojedina prijetnja ostvari, te posljedica koje će nanijeti. Tretiranje rizika označava postupke kojima se prijetnje nastoje ublažiti ili izbjeći u potpunosti. Posljednje potpoglavlje bavi se protumjerama, odnosno postupcima za tretiranje rizika, te prijedlogom poboljšanja.

6.2. Standardizirani ciljevi i procesi okvira CobiT 5

Kao što je bilo navedeno u samom poglavlju broj 5, pod temom CobiT 5, ovaj okvir sadrži standardizirane ciljeve i procese. Ciljevi se dijele na strateške i IT ciljeve, te svakih postoji 17 što je prikazano u idućim tablicama.

Tablica 4 - Prikaz strateških ciljeva prema okviru CobiT 5 (Prema: ISACA, 2012.)

BSC perspektiva	Redni broj	Strateški cilj prema CobiT 5
Financije	1.	Vrijednost poslovnih ulaganja od strane dionika
	2.	Portfolio konkurentnih proizvoda i usluga
	3.	Upravljanje poslovnim rizicima – zaštita imovine
	4.	Usklađenost sa eksternim zakonima i propisima
	5.	Financijska transparentnost
Korisnici	6.	Kultura proizvoda i usluga orijentiranih na korisnike
	7.	Kontinuitet i dostupnost usluga
	8.	Agilni odgovor na promjenjivo poslovno okruženje
	9.	Donošenje strateških odluka zasnovanih na informacijama
	10.	Optimizacija troškova pružanja usluga
Interni procesi	11.	Optimizacija funkcionalnosti poslovnih procesa
	12.	Optimizacija troškova poslovnih procesa
	13.	Upravljanje programima za promjenu poslovanja i poslovnih procesa
	14.	Operativna produktivnost i produktivnost zaposlenika
	15.	Usklađenost sa internim pravilima
Učenje i rast	16.	Vješti i motivirani zaposlenici
	17.	Kultura inoviranja proizvoda, usluga i poslovanja

Tablica 5 - Prikaz IT ciljeva prema okviru CobiT 5 (Prema: ISACA, 2012)

BSC perspektiva	Redni broj	IT cilj prema CobiT 5
Financije	1.	Usklađivanje IT i poslovne strategije
	2.	Usklađenost IT-a i poslovne strategije sa eksternim zakonima i propisima
	3.	Predanost izvršnog menadžmenta za donošenje odluka vezanih uz IT
	4.	Upravljanje poslovnim rizikom koji je povezan s IT-om
	5.	Ostvarene koristi od portfelja ulaganja i usluga temeljenih na IT-u
	6.	Transparentnost IT troškova, koristi i rizika
Korisnici	7.	Isporuka IT usluga u skladu s poslovnim zahtjevima
	8.	Odgovarajuća uporaba aplikacija, informacijskih i tehnoloških rješenja
Interni procesi	9.	IT agilnost
	10.	Sigurnost informacija i infrastrukture
	11.	Optimizacija IT imovine i resursa
	12.	Omogućavanje i podrška poslovnim procesima kroz integraciju aplikacija i tehnologije u poslovne procese
	13.	Isporuka programa koji donose benefite, na vrijeme, u okviru proračuna, te koji ispunjavaju zahtjeve i standarde kvalitete
	14.	Dostupnost pouzdanih i korisnih informacija za donošenje odluka
	15.	Usklađenost IT-a sa internim pravilima
Učenje i rast	16.	Sposoban i motiviran cjelokupni kadar
	17.	Znanje, stručnost i inicijatiiva za poslovne inovacije

Osim standardiziranih ciljeva, prema CobiT 5 okviru, postoje i standardizirani procesi koji se svrstavaju u pet različitih kategorija. Svih pet kategorija u poglavlju pod brojem 5. pojašnjeno je i navedeno sa punim nazivom, dok se u tablici pod brojem 6 nalaze procesi koji se svrstavaju u svaku kategoriju, te skraćeni nazivi svih kategorija (eng. **EDM** – Evaluate, Direct, Monitor; **APO** – Align, Plan, Organise; **BAI** – Build, Acquire, Implement; **DSS** – Delivery, Service, Support; **MEA** – Monitor, Evaluate, Assess).

Tablica 6 - Prikaz procesa svrstanih u kategorije prema okviru CobiT 5 (Prema: Krakar Z. i suradnici, 2014)

Kategorija	Oznaka	Proces prema CobiT 5
EDM	EDM01	Izrada i održavanje postavki korporativnog radnog okvira
	EDM02	Osiguranje i isporuka koristi
	EDM03	Osiguranje optimizacije upravljanja rizicima
	EDM04	Osiguranje optimizacije upravljanja resursima
	EDM05	Osiguranje transparentnosti dionicima
APO	APO01	Upravljanje radnim okvirom korporativnog upravljanja
	APO02	Upravljanje strategijom
	APO03	Upravljanje arhitekturom poslovnog subjekta
	APO04	Upravljanje inovacijama
	APO05	Upravljanje portfeljem
	APO06	Upravljanje proračunom i troškovima
	APO07	Upravljanje ljudskim potencijalima
	APO08	Upravljanje odnosima
	APO09	Upravljanje ugovorima o pružanju usluga
	APO10	Upravljanje dobavljačima
	APO11	Upravljanje kvalitetom
	APO12	Upravljanje rizicima
	APO13	Upravljanje sigurnošću
BAI	BAI01	Upravljanje programima i projektima
	BAI02	Upravljanje definicijom zahtjeva

	BAI03	Upravljanje identifikacijom rješenja i izgradnjom
	BAI04	Upravljanje raspoloživošću i kapacitetom
	BAI05	Upravljanje omogućavanjem organizacijskih promjena
	BAI06	Upravljanje promjenama
	BAI07	Upravljanje prihvaćanjem promjenama i prijelaznim rješenjima
	BAI08	Uparvljanje znanjem
	BAI09	Upravljanje imovinom
	BAI10	Upravljanje konfiguracijama
DSS	DSS01	Upravljanje operacijama
	DSS02	Upravljanje zahtjevima za uslugama i incidentima
	DSS03	Upravljanje problemima
	DSS04	Upravljanje neprekidnošću poslovanja
	DSS05	Upravljanje uslugama sigurnosti
	DSS06	Upravljanje kontrolama poslovnih procesa
MEA	MEA01	Nadzor, vrednovanje i procjena performansi i sukladnosti
	MEA02	Nadzor, vrednovanje i procjena sustava internih kontrola
	MEA03	Nadzor, vrednovanje i procjena usklađenosti s eksternim zahtjevima

6.3. Provedeno istraživanje

U nastavku potpoglavlja, kroz sve tablice, slijedi prikaz provedenog istraživanja u neprofitnoj organizaciji VI. osnovna škola Varaždin. Istraživanje je provedeno u suradnji sa stručnom službom organizacije, nastavnicima i informatičarima. U prethodnim poglavljima prikazani su strateški ciljevi, IT ciljevi, te izvedena strateška mapa, dok su u nastavku prikazani IT benefiti za svaki strateški cilj, IT ciljevi su smješteni u IT BSC perspektive, te povezani sa strateškim ciljevima. Nakon tablice br. 9 u kojoj su IT ciljevi povezani sa strateškim, prikazano je povezivanje IT ciljeva sa procesima CobiT 5 okvira, te su na temelju tog povezivanja identificirane prijetnje. U tablici br. 13 prikazana je razina svakog pojedinog rizika, te protumjere za ublažavanje ili potpuno izbjegavanje pojedinih rizika. Svi podaci koji su korišteni u istraživanju, te svi izvedeni strateški i IT ciljevi organizacije, zajedno sa identificiranim rizicima,

dobiveni su kao rezultat provedenih intervjua te proučavanih CobiT 5 standarda, odnosno standardiziranih poslovnih i IT ciljeva, te procesa iz CobiT 5 okvira.

Tablica 7 - Prikaz IT benefita za svaki strateški cilj organizacije (Izvor: autorica)

BSC perspektiva	Strateški cilj organizacije	IT benefit
Potrebe dionika	EG1. Unaprijediti načine učenja i poučavanja.	Povećanje informatičke pismenosti. Mogućnost stvaranja generacije budućnosti.
	EG2. Unaprijediti organizaciju nastave.	Skraćivanje vremena pripreme za nastavu. Proširenje *poola* stručnih i nestručnih zamjena
Korisnici	EG2K1. Organizacija nastave na način da učenici svoje aktivnosti mogu ostvarivati na "jednom mjestu".	Poticanje rada kroz različite alate i platforme.
	EG2K2. Povećanje broja izbornih i izvannastavnih aktivnosti kako bi se smanjio broj učenika koji ne pohađaju iste.	Omogućavanje interaktivnih izbornih i izvannastavnih aktivnosti kroz platforme koje se koriste u nastavi – Microsoft Teams
Interni procesi	EG1P1. Omogućiti učenicima rad u modernim i opremljenim učionicama u svim područjima.	Poticanje rada i učenja kroz različite alate i platforme.

		Povećanje interesa za zanimanja budućnosti. Ostvarivanje međunarodnih suradnji i job shadowing.
	EG1P2. Proširenje ideja, uviđanje novih načina rada.	Ostvarivanje međunarodnih suradnji i job shadowing.
	EG1P3. Omogućavanje kvalitetnijih uvjeta rada, posvećivanje učenicima kao pojedincima i zadržavanje stručnog kadra koji će napredovati i olakšati rad učenicima (bez stalnih promjena učitelja).	Održavanje virtualnih edukacija (i za učitelje i za učenike). Korištenje energije iz obnovljivih izvora.
	EG2P1. Nadogradnja škole kako bi se stvorili kapaciteti za organizaciju i izvođenje nastave za sve razredne odjele s početkom u isto vrijeme (jednosmjenska nastava u punom smislu riječi).	Ostvarivanje većeg povrata od ulaganja.
	EG2P2. Organizacija cjelodnevne nastave.	Smanjenje opterećenja učenika van nastave.
Učenje i rast	EG1U1. Napredovanje i zadržavanje stručnog kadra.	Ostvarivanje međunarodnih suradnji, job shadowing, virtualne edukacije.

		Rad u modernom i pametnom okruženju.
	EG2U1. Zadržavanje stručnog kadra među učiteljima i zapošljavanje stručnog kadra u stručnoj službi kako bi se olakšala organizacija nastave i smanjilo opterećenje.	

Tablica 8 - Prikaz smještanja IT ciljeva organizacije prema IT BSC perspektivama (Izvor: autorica)

IT BSC perspektiva	IT cilj organizacije
Izvedba projekata (potpora IT-a poslovanju)	IT1. Povećanje broja suradnji sa školama
	IT2. Povećanje broja suradnji sa poduzećima i obrtnicima.
	IT3. Povećanje broja učenika uključenih u projekte
Zadovoljstvo korisnika	IT4. Kvalitetno izvođenje nastave na daljinu.
	IT5. Prihvaćanje digitaliziranih i interaktivnih materijala
Operativne performanse i IT procesi	IT6. Poboljšanje IT infrastrukture.
	IT7. Povećanje broja digitaliziranih materijala za nastavu.
	IT8. Stvaranje pametne učionice na otvorenom.
	IT9. Uvođenje alata za organizaciju nastave i kreiranje rasporeda.

	IT10. Veće korištenje sredstava iz EU fondova.
Upravljanje ljudskim kapitalom	IT11. Smanjenje vremena pripremanja za nastavu kroz korištenje digitalnih materijala.
	IT12. Edukacija svih zaposlenika.

Tablica 9 - Prikaz mapiranja IT ciljeva organizacije sa strateškim ciljevima organizacije (Izvor: autorica)

IT cilj organizacije	Mapiranje IT ciljeva organizacije sa strateškim ciljevima organizacije			
	Potrebe dionika	**Korisnici**	**Interni procesi**	**Učenje i rast**
IT1. Povećanje broja suradnji sa školama	EG1. Unaprijediti načine učenja i poučavanja.		EG1P2. Proširenje ideja, uviđanje novih načina rada.	
IT2. Povećanje broja suradnji sa poduzećima i obrtnicima.	EG1. Unaprijediti načine učenja i poučavanja.		EG1P2. Proširenje ideja, uviđanje novih načina rada.	
IT3. Povećanje broja učenika uključenih u projekte	EG1. Unaprijediti načine učenja i poučavanja.	EG2K1. Organizacija nastave na način da učenici svoje aktivnosti		

		mogu ostvarivati na "jednom mjestu". F2K2. Povećanje broja izbornih i izvannastavnih aktivnosti kako bi se smanjio broj učenika koji ne pohađaju iste.		
IT4. Kvalitetno izvođenje nastave na daljinu.	EG1. Unaprijediti načine učenja i poučavanja.			
IT5. Prihvaćanje digitaliziranih i interaktivnih materijala	EG1. Unaprijediti načine učenja i poučavanja.		EGP2. Proširenje ideja, uviđanje novih načina rada.	
IT6. Poboljšanje IT infrastrukture.	EG1. Unaprijediti načine učenja i poučavanja.		EG1P1. Omogućiti učenicima rad u modernim i opremljenim učionicama u svim područjima.	

IT7. Povećanje broja digitaliziranih materijala za nastavu.	EG1. Unaprijediti načine učenja i poučavanja.	FEGK2. Povećanje broja izbornih i izvannastavnih aktivnosti kako bi se smanjio broj učenika koji ne pohađaju iste.	EG1P2. Proširenje ideja, uviđanje novih načina rada.	
IT8. Stvaranje pametne učionice na otvorenom.	EG1. Unaprijediti načine učenja i poučavanja.		EG1P1. Omogućiti učenicima rad u modernim i opremljenim učionicama u svim područjima. EG1P3. Omogućavanje kvalitetnijih uvjeta rada, posvećivanje učenicima kao pojedincima i zadržavanje stručnog kadra koji će napredovati i olakšati rad učenicima (bez stalnih promjena učitelja).	EG1U1. Napredovanje i zadržavanje stručnog kadra.

IT9. Uvođenje alata za organizaciju nastave i kreiranje rasporeda.	EG2. Unaprijediti organizaciju nastave			
IT10. Veće korištenje sredstava iz EU fondova.	EG1. Unaprijediti načine učenja i poučavanja.		EG1P1. Omogućiti učenicima rad u modernim i opremljenim učionicama u svim područjima.	EG1U1. Napredovanje i zadržavanje stručnog kadra.
IT11. Smanjenje vremena pripremanja za nastavu kroz korištenje digitalnih materijala.				EG2U1. Zadržavanje stručnog kadra među učiteljima i zapošljavanje stručnog kadra u stručnoj službi kako bi se olakšala organizacija nastave i smanjilo opterećenje.
IT12. Edukacija svih zaposlenika.			EG1P2. Proširenje ideja, uviđanje novih načina rada.	EG1U1. Napredovanje i zadržavanje stručnog kadra.

Tablica 10 - Prikaz mapiranja CobiT 5 IT procesa sa IT ciljevima organizacije (Izvor: autorica)

Cobit5 IT proces	Utjecaj na IT cilj organizacije
EDM2**: osiguravanje koristi za poslovanje**	IT1. Povećanje broja suradnji sa školama. IT2. Povećanje broja suradnji sa poduzećima i obrtnicima. IT9. Uvođenje alata za organizaciju nastave i kreiranje rasporeda. IT10. Veće korištenje sredstava iz EU fondova. IT12. Edukacija svih zaposlenika.
APO3**: definiranje informacijske arhitekture**	IT6. Poboljšanje IT infrastrukture.
APO6**: upravljanje budžetom i troškovima**	IT10. Veće korištenje sredstava iz EU fondova.
APO7**: upravljanje ljudskim resursima**	IT11. Smanjenje vremena pripremanja za nastavu kroz korištenje digitalnih materijala. IT12. Edukacija svih zaposlenika.
APO11**: upravljanje kvalitetom**	IT4. Kvalitetno izvođenje nastave na daljinu. IT11. Smanjenje vremena pripremanja za nastavu IT12. Edukacija svih zaposlenika.
BAI1**: upravljanje programima i projektima**	IT1. Povećanje broja suradnji sa školama.

	IT2. Povećanje broja suradnji sa poduzećima i obrtnicima. IT3. Povećanje broja učenika uključenih u projekte.
BAI6**: upravljanje promjenama**	IT7. Povećanje broja digitalnih materijala za nastavu. IT8. Stvaranje pametne učionice na otvorenom. IT9. Uvođenje alata za organizaciju nastave i kreiranje rasporeda.
BAI7**: upravljanje prijelazima i prihvaćanje promjena**	IT5. Prihvaćanje digitaliziranih i interaktivnih materijala. IT12. Edukacija svih zaposlenika
BAI8**: upravljanje znanjem**	IT12. Edukacija svih zaposlenika.

Tablica 11 - Prikaz identificiranih prijetnji za pojedini CobiT 5 proces (Izvor: autorica)

CobiT 5 IT proces	Identificirane prijetnje
EDM2: **osiguravanje koristi za poslovanje**	1. Nedovoljna količina materijalnih sredstava za ostvarivanje svih ciljeva 2. Nedovoljna podrška Ministarstva znanosti i obrazovanja Republike Hrvatske 3. Nedovoljan broj realiziranih projekata

	4. Preopterećenje nastavnog kadra
APO3: **definiranje informacijske arhitekture**	1. Rapidan razvoj tehnologije i potrebne opreme 2. Prevelik broj slabije opremljenih obrazovnih ustanova 3. Minimalna količina materijalnih sredstava za održavanje informacijske infrastrukture
APO6: **upravljanje budžetom i troškovima**	1. Nedovoljno sudjelovanje u projektima koji povećavaju novčana sredstva, zbog premalog interesa učitelja 2. Nedostatak znanja i edukacija za pisanje dokumentacije EU projekata
APO7: **upravljanje ljudskim resursima**	1. Nedefiniranost potrebnih IT znanja i vještina za rad 2. Premalen obujam formalnih edukacija za povećanje IT znanja i vještina 3. Nedostatak nadzora znanja i vještina 4. Nedostatak konstantne verifikacije potrebnih IT znanja i vještina
APO11: **upravljanje kvalitetom**	1. Nedefiniranost standarda kvalitete na razini svih obrazovnih ustanova 2. Nedostatak sustava za upravljanje kvalitetom

	3. Premalena količina znanja koju učenici nose u daljnje obrazovanje
BAI1: **upravljanje programima i projektima**	1. Nedostatak materijalnih sredstava za sudjelovanje dovoljnog broja učenika i djelatnika na projektima 2. Neusklađenost sa Nacionalnim kurikulumom
BAI6: **upravljanje promjenama**	1. Upitna kvaliteta projektne dokumentacije 2. Povezanost učitelja s pojedinim izdavačkim kućama 3. Uvođenje nekvalitetnih ili prividno kvalitetnih alata i materijala 4. Nedovoljna educiranost učitelja
BAI7: **upravljanje prijelazima i prihvaćanje promjena**	1. Nedovoljna educiranost učitelja 2. Nezainteresiranost učitelja koja proizlazi iz potplaćenosti i preopterećenosti 3. Nedovoljna podrška Ministarstva znanosti i obrazovanja Republike Hrvatske 4. Premalo organiziranih formalnih edukacija od strane Ministarstva znanosti i obrazovanja Republike Hrvatske
BAI8: **upravljanje znanjem**	1. Nezainteresiranost učitelja koja proizlazi iz potplaćenosti i preopterećenosti

	2. Premalno organiziranih formalnih edukacija od strane Ministarstva znanosti i obrazobanja Republike Hrvatske

Tablica 12 - Prikaz odnosa vjerojatnosti događaja pojedine prijetnje te posljedice koja se nanosi (Izvor: autorica)

		Vjerojatnost događaja		
		Mala (1)	Srednja (2)	Velika (3)
Posljedice rizika	Mala (1)	1	2	3
	Srednja (2)	2	4	6
	Velika (3)	3	6	9
	Vrlo velika (4)	4	8	12

Tablica 13 - Prikaz razine pojedinih rizika prema CobiT 5 procesima (Izvor: autorica)

CobiT 5 IT proces	**Vjerojatnost događaja prijetnje**	**Posljedice pojedine prijetnje**	**Razina rizika i način tretiranja**
EDM2: **osiguravanje koristi za poslovanje**	Srednja (2)	Velika (3)	**Srednja** (6) Mjera: veća financijska podrška Ministarstva znanosti i obrazovanja Republike

			Hrvatske te Vlade Republike Hrvatske
APO3: **definiranje informacijske arhitekture**	Velika (3)	Vrlo velika (4)	**Velika** (12) Mjera: ulazak većeg broja škola u CARNET-ov projekt e-Škole; delegiranje dijela održavanja informacijske infrastrukture na zaposleni kadar
APO6: **upravljanje budžetom i troškovima**	Velika (3)	Vrlo velika (4)	**Velika** (12) Mjera: dodatna financiranja učitelja kroz bonuse i nagrade; plaćene edukacije o pisanju EU projektne dokumentacije
APO7: **upravljanje ljudskim resursima**	Velika (3)	Velika (3)	**Velika** (9) Mjera: definiranje formalnog dokumenta na razini svih obrazovnih ustanova Republike Hrvatske u kojem se

			navode sva potrebna IT znanja i vještine potrebna za rad
APO11: **upravljanje kvalitetom**	Srednja (2)	Srednja (2)	**Srednja** (4) Mjera: suradnja sa Nacionalnim centrom za vanjsko vrednovanje i Agencijom za odgoj i orazovanje u kreiranju testiranja te u kreiranju formalnog okvira za praćenje upravljanja kvalitetom na razini svih obrazovnih ustanova Republike Hrvatske
BAI1: **upravljanje programima i projektima**	Srednja (2)	Mala (1)	**Mala** (2) Mjera: veća podrška Ministarstva znanosti i obrazovanja Republike Hrvatske te ostalih nadležnih tijela

BAI6: **upravljanje promjenama**	Mala (1)	Mala (1)	**Mala** (1) Mjera: povećanje broja edukacija za zaposlene djelatnike, te promjene u nastavnom planu i programu Učiteljskog fakulteta.
BAI7: **upravljanje prijelazima i prihvaćanje promjena**	Velika (3)	Vrlo velika (4)	**Velika** (12) Mjera: veća podrška Ministarstva znanosti i obrazovanja Republike Hrvatske te ostalih nadležnih tijela
BAI8: **upravljanje znanjem**	Srednja (2)	Vrlo velika (4)	**Velika** (8) Mjera: veća podrška Ministarstva znanosti i obrazovanja Republike Hrvatske te ostalih nadležnih tijela

6.4. Prijedlog poboljšanja

Posljednji dio istraživanja odnosi se na definiranje mjera, odnosno postupaka kojima se rizici na određeni način tretiraju, te samim time i ublažavaju ili pak čak u potpunosti otklanjaju i izbjegavaju. U istraživanju je identificirano pet rizika koji su izuzetno problematični, te je razina tih rizika velika, što znači da su i vjerojatnost da dođe do tog rizika, ali i posljedice iznimno teške. Procesi prema CobiT 5 okviru u kojima se pojavljuju veliki rizici su: **APO03** – definiranje informacijske arhitekture, **APO06** – upravljanje budžetom i troškovima, **APO07** – upravljanje ljudskim resursima, **BAI07** – upravljanje prijelazima i prihvaćanje promjena i **BAI08** – upravljanje znanjem. Prema provedenom istraživanju i zaključcima diplomskog rada, rizike povezane sa procesima **APO07** i **BAI08**, smjestila bih u perspektivu učenja i rasta prema BSC. Rizik vezan uz proces **APO06** smjestila bih u perspektivu financija, dok bi rizike povezane sa procesima **APO03** i **BAI07** smjestila u perspektivu internih procesa prema BSC.

Glavnina rizika čija je razina velika kao mjeru za ublažavanje zapravo bi trebala veću podršku nadležnih tijela, počevši od Agencije za odgoj i obrazovanje, Nacionalnog centra za vanjsko vrednovanje, Ministarstva znanosti i obrazovanja Republike Hrvatske, ali i Vlade Republike Hrvatske. Ovakva vrsta protumjera generalno je najbitnija za cjelokupni obrazovni sustav Republike Hrvatske, te se vrlo često odnosi na nešto što sama organizacija ne može samostalno kontrolirati.

7. Zaključak

Dinamičnost je glavna karakteristika današnjeg poslovanja, no dinamičnost se nerijetko ogleda u koje kakvim prijetnjama i rizicima koji se javljaju. Upravljanje rizicima relativno je novi pristup u poslovanju, no iznimno bitan. Upravljanje rizicima trudi se pronaći najslabije karike u svakom sustavu, odnosno organizaciji ili poduzeću, ali i kreirati protumjere koje će pomoći u očuvanje imovine svake organizacije ili poduzeća. Posljednja krucijalna točka upravljanja rizicima jest granica uspješnog poslovanja poduzeća, ili pak barem održivog poslovanja. Sam pristup upravljanja rizicima pruža svojevrsni uvid u razmjer gubitaka, određivanja vjerojatnosti pojedinih prijetnji, te mjera i aktivnosti kojima bi se rizici mogli umanjiti ili čak izbjeći. Korporativno upravljanje rizicima podpojam je upravljanja rizicima, a odnosi se na upravljačke strukture i procese unutar poslovnih sustava, što u krajnjoj liniji znači da je to određeni skup mehanizama koji zajedno osiguravaju povrat ulaganja, ali na način koji ne ugrožava održivost organizacije. Korporativno upravljanje informatičkim rizicima važan je pojam u poslovanju zbog sve veće upotrebe digitalnih tehnologija, a omogućuje određeni stupanj informatičke sigurnosti. Informatički rizici nisu problem isključivo tehnološke prirode, već su problem koji je važno sagledati s korporativne razine. Važan korak pri upravljanju rizicima je određivanje protumjera kojima se ublažavaju posljedice, ili pak u potpunosti eliminiraju rizici.

Balanced Scorecard metoda je koja se uglavnom koristi za pregled uspješnosti neke organizacije ili poduzeća, a ogleda se u tome što u fokus ne stavlja isključivo financijske pokazatelje, kao mnoštvo drugih metoda. Osim pregleda uspješnosti poslovanja, ova se metoda može koristiti i u upravljanju IT rizicima. Za prikaz korištenja Balanced Scorecard na stvarnom primjeru, odabrana je neprofitna organizacija, odnosno VI. osnovna škola Varaždin. Kroz suradnju sa zaposlenicima škole, definirani su strateški ciljevi, te samim time i strateška mapa, zatim su definirani IT ciljevi koji su se povezali sa strateškim ciljevima. Nakon povezivanja strateških i IT ciljeva, te smještanja u ispravne perspektive Balanced Scorecarda, IT ciljevi povezali su se sa IT procesima CobiT 5 okvira i definirane su moguće prijetnje. Za svaku prijetnju određena je vjerojatnost nastanka iste, te posljedice koje može nanijeti. Nakon sagledavanja vjerojatnosti i posljedica svake pojedine prijetnje, definirana je ne samo razina rizika, već i način tretiranja, odnosno mjera za ublažavanje ili izbjegavanje rizika.

Popis literature

[1] ISACA (2012) COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT, dostupno 27.08.2021. na https://www.oo2.fr/sites/default/files/document/pdf/cobit-5_res_eng_1012.pdf

[2] Keyes J. (2005) *Aligning IT with Corporate Strategy – Implementing the IT Balanced Scorecard*, Auerbach Publications

[3] KnowledgeHut (28.08.2019.) *Top Principles of COBIIT 5 Foundation – IT Security*, dostupno 15.06.2021. na https://www.knowledgehut.com/blog/security/top-principles-cobit-5-foundation-security

[4] Kozina M. (2017) *Neki aspekti IT menadžmenta u uvjetima digitalne ekonomije*, Fakultet organizacije i informatike, Sveučilište u Zagrebu, Zrinski d.d., Čakovec

[5] Krakar Z. i suradnici (2014) Korporativna informacijska sigurnost, Fakultet organizacije i informatike, Sveučilište u Zagrebu

[6] Niven P. (2007) *Balanced Scorecard: Korak po korak*, Poslovni dnevnik, Zagreb

[7] Panian, Spremić i suradnici (2007) *Korporativno upravljanje i revizija informacijskih sustava*, Tiskara Zelina

[8] PECB (Lachapelle E., Hundozi B.) (2015) *ISO 31000 Risk Management – Principles and Guidelines,* dostupno 18.06.2021. na https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines

[9] Spremić M. (2017) *Digitalna transformacija poslovanja*, Sveučilište u Zagrebu, Ekonomski fakultet, Sveučilišna tiskara d.o.o. Zagreb

[10] Spremić M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilište u Zagrebu, Ekonomski fakultet, Sveučilišna tiskara d.o.o., Zagreb

[11] Tipurić D. i suradnici (2008) *Korporativno upravljanje*, Sinergija nakladništvo, Zagreb

[12] Zaposlenici VI. osnovne škole Varaždin

Popis slika

Popis tablica